

**REGULATING THE MASS DATAVEILLANCE CAPABILITIES OF PSYCHOPATHIC
CORPORATIONS**

LAURA GARCIA VARGAS

Thesis submitted to the University of Ottawa
in partial Fulfillment of the requirements for the
PhD in Law

Faculty of Law
University of Ottawa

© Laura Garcia Vargas, Ottawa, Canada, 2025

Table of Content

List of Abbreviations	vi
Abstract	viii
Acknowledgments	x
Dedication	xi
Chapter I. Introduction	1
I. Surveillance and Corporations	4
II. Structure of the Thesis	9
Chapter II. Literature Review and Methodology	13
I. Previous Literature on Privacy and Location Technologies	14
A. Privacy Concerns and Proposed Solutions	15
1) Privacy Concerns	15
2) Proposed Solutions	19
(a) Giving Individuals More Control Over Their Data	19
(b) Minimizing the Risks Associated with Collected Data	22
(c) Privacy by Design (PbD)	25
B. Specific Critiques of Data Protection Regulation	27
1) Location Data and Data Protection Regulations	27
2) Data Protection Regulation and Privacy Issues	29
II. Law, Technology, and Society	33
A. Law, Regulation, and Technology	35
B. Analyzing the Adequacy of a Regulatory Framework	40
III. Conclusions	44
Chapter III. Surveillance and Privacy in the International Human Rights Framework	46
I. Brief History of Surveillance and Technologies	51
A. Digital Technologies and Surveillance	55
B. Location Technologies and Surveillance	61
1) Realtime Tracking and Future Locations	62
2) Infer Details About Lifestyles	64
3) Geo-Relational Analysis	65
II. Privacy and Technologies in the International Human Rights Framework	68
A. Privacy and Data Banks: Information Privacy	77
III. International Human Rights Framework and Government-Led Surveillance	80
A. Mass Interception Regimes	82
B. Metadata and Mandatory Data Retention Regimes	91
C. Geolocation Surveillance Practices	96
IV. Conclusion	100
Chapter IV. Corporate Mass Dataveillance	102
I. Corporations as Psychopathic Institutions	105
A. Pathological Traitst of Corporations	109
B. The Psychopathic Personality of Corporations With Data-Driven Business Models	111

1) Manipulation of the Privacy Discourse	116
2) Internal Manipulative Behaviours	119
II. Case Examples: Uber Technologies Inc. and Meta Platforms Inc.	123
A. Uber Technologies Inc. (Uber Inc.)	125
B. Meta Platforms Inc. (Meta Inc)	129
C. The Psychopathic Personality of Uber Inc and Meta Inc	131
1) Irresponsibility	132
2) Superficial Relationships	134
3) Refusal to Take Responsibility	137
4) Lack of Empathy	139
5) Asocial Behaviour	146
6) Building and Maintaining a Deceptive “good neighbour” Image	149
III. Mass Dataveillance Systems as a Facet of Corporate Pathology: The Example of Location Dataveillance	156
A. From Human Mobility to Digital Movement Records	159
1) Localization Techniques	160
2) Identification Methods	162
3) Movement Records	164
4) Location Data as Business Assets	166
B. Corporate Dataveillance Systems and Surveillance Capitalism	168
1) Surveillance Capitalism and Traditional Capitalism	169
2) Source of Profit (Predictions Products)	170
3) Economic Imperatives	173
(a) Extraction Imperative: Expanding Behavioural Surplus	174
(b) Prediction Imperative: Enhancing Predictive Capabilities	176
(i) Economies of Scope: Expanding the Reach of Dataveillance	176
(ii) Economics of Action: Shaping User Behaviour	178
C. Risks of Corporate Mass Dataveillance Systems	181
IV. Conclusions	188
Chapter V. Regulation of Corporate Dataveillance Practices and International Human Rights Framework	191
I. States’ Duty to Regulate Corporate Mass Dataveillance and Data Protection Regulations	194
A. Assumption 1: Data Must Be (Are) Collected and Processed by Corporations	199
1) Beginning of Data Protection Regulations	201
2) Modernization Efforts: 2010–2023	206
B. Assumption 2: Corporations are Benevolent	212
1) Carry Out Data Protection Impact Assessments (DPIAs)	214
2) Choosing the Legal Ground	216
3) Integrate Privacy by Design (PbD) into their technologies, products, and Services	224
4) Fines as Deterrents of Deviant Behaviour	227
II. International Human Rights, Corporations, and Surveillance	230
A. Corporate Human Rights Responsibilities and Their Pathological Personality	231
B. B-Tech Analysis of the UNGPs	234
C. Enhancing the “Good Neighbour” Image: Corporations as Protectors	237
D. UN Perspective on Corporate Data Practices	239
III. Conclusions	243

Chapter VI. Regulating Corporate Dataveillance in the Face of Socio-technical Change	245
I. The Need for a New Regulatory Framework	251
A. Regulatory Rationales: Democratic Oversight and Protecting Rights	252
B. Regulatory Goal and Target	256
1) Regulatory Goal	257
2) Regulatory Object	259
3) Regulatory Subject	264
II. Limiting Corporate Dataveillance: Essential Features	266
A. Regulating Self-Interest Corporate Purpose and Limiting How to Pursuit their Purpose	267
1) Corporate Purpose: Broadening the Scope Beyond Self-Interested Profit Generation	269
2) Corporate Duties: Limiting How Corporations Can Generate Profit	274
(a) Duty to Limit Revenue Streams	279
(b) Reporting and Regulatory Review	284
(i) Detail Revenue Reporting	285
(ii) Mapping of Data to Revenue Streams	286
(c) What This Means for Corporations	286
(i) Meta Platforms Inc. (Meta Inc.)	289
(ii) Uber Technologies Inc (Uber Inc.)	293
(iii) Stellantis N. V.	296
(iv) H&M Hennes & Mauritz AB (H&M Group)	301
(d) Enforcement of the Duty	306
B. Consequences to Corporations' Own Existence: Mandatory Dissolution	308
1) Triggering the Dissolution of a Corporation	311
2) Dissolution Process and Alternatives.	315
C. Adoption of the Proposed Framework	318
III. Limits and Possible Critiques of the Proposed Framework	324
IV. Conclusions	328
Chapter VII. Conclusions	331
I. Summary and Contributions	333
II. Limits and Further Research	338
Bibliography 342	
Legislation: Canada	342
Legislation: EU	342
Legislation: OtherOther Countries	343
Legislation: Regional and International Human Rights Treaties	343
Jurisprudence: Regional Human Right Courts	344
InterAmerican Court of Justice	344
European Court of Human Rights	344
Jurisprudence: CJEU	345
Jurisprudence: Canada	345
Jurisprudence: USA	345
Secondary Material: European Union Documents	345
Secondary Material: United Nations Documents	348
Secondary Material: Canadian Government Documents	350
Secondary Material: Books	354

Secondary Material: Books Chapters	357
Secondary Material: Journal Articles	365
Secondary Material: Reports	377
Secondary Material: Conference Papers	379
Secondary Material: News Articles	383
Secondary Material: Blogposts	392
Secondary Material: Corporations Documents	393
Meta Platforms Inc	394
SEC Documents	394
Newsroom	394
Uber Technologies Inc	397
SEC Documents	397
Blogposts	397
Newsroom	398
H & M Hennes & Mauritz AB (H&M Group)	399
Stallantis N.V.	400
Secondary Material: Others	401
Secondary Material: Websites	401

List of Abbreviations

APIs	Application Programming Interfaces
CJEU	Court of Justice of the European Union
CBCA	Canada Business Corporation Act
DPIAs	Data Protection Impact Assessments
DPO	Data Protection Officer
ECHR	European Conventions on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
FIPs	Fair Information Principles
GDPR	General Data Protection Regulation [European Union]
GPS	Global Position System
HRC	UN Human Rights Council (UN Charter Body)
CCPR	UN Human Rights Committee (Treaty Body)
IACtHR	InterAmerican Court of Human Rights
ICCPR	International Covenant on Civil and Political Rights
IoT	Internet of Things
Irish DPC	Irish Data Protection Commission
ISPs	Internet Service Providers
LBS	Location Based Services
NSA	National Security Agency [United States of America]
OHCHR	Office of the High Commissioner for Human Rights
OPC	Office of the Privacy Commissioner of Canada
PbD	Privacy-by-Design
PIA	Privacy Impact Assessment
PIPEDA	Personal Information Protection and Electronic Documents Act [Canada]
SDKs	Software Development Kits

SRSG	Special Representative of the Secretary-General on the issue of Human Rights and Transnational Corporations and other Business Enterprises
UN	United Nations
UDHR	Universal Declaration of Human Rights
UNGPs	UN Guiding Principles on Business and Human Right
WP29	Article 29 Data Protection Working Party
WPPJ	Working Party on Police and Justice
WWII	Second World War

Abstract

The increasing prevalence of corporate mass dataveillance poses significant risks to privacy and societal well-being. This thesis examines the effectiveness of existing data protection regulations in addressing these risks in the current socio-technical landscape. It argues that these regulations are inadequate due to their outdated assumptions: the necessity and acceptability of corporate data processing and the benevolent nature of corporations. Drawing on Joel Bakan's theory of the psychopathic personality of corporations, this thesis highlights the misalignment between corporate profit-driven motivations and regulatory objectives, and proposes a new regulatory framework that aims to restrict corporate mass dataveillance by targeting the business models that have incentivized its development and the institutional structures that enable pathological corporate behaviour.

The thesis begins by mapping the current socio-technical landscape, highlighting the now possible capabilities of public and private organizations by technological advances in the generation, collection, and processing of data about individuals and their behaviours. It analyzes the evolution of the right to privacy within the international human rights framework, particularly its application to government surveillance, before shifting the focus of the analysis to corporations as central actors in the data economy and how this framework applies to them.

Using Uber Technologies Inc. and Meta Platforms Inc. as examples of corporations with data-driven business models, it illustrates how these corporations exhibit psychopathic tendencies consistent with Bakan's theory, including an obsession with profit, a lack of concern for others, and a propensity for breaking legal rules. The thesis then discusses corporate mass dataveillance systems as a manifestation of this psychopathic personality, highlighting the economic model of surveillance capitalism, in which these corporations operate, and the risks and harms posed by

their extensive data collection and processing practices: such as undermining democratic institutions, interfering with the right to privacy, and facilitating behavioural manipulation. This socio-economic ecosystem, driven by a logic of data accumulation, has propelled the expansion of dataveillance technologies and influenced the design of products and services to maximize corporate profits at the expense of individual rights and societal well-being.

With this landscape in mind, the thesis analyzes the adequacy of data protection regulations, exemplified by the GDPR and PIPEDA, in addressing corporate mass dataveillance. It identifies two key shortcomings: their failure to question the necessity of corporate data processing, and their flawed assumption of corporate empathy. These limitations render these regulations inadequate to limit corporate mass dataveillance and inadequate to protect human rights and society from the risks and harms dataveillance creates.

To address these gaps, I propose a new regulatory framework aimed at restricting corporate mass dataveillance. The framework targets the business models that have incentivized the development of corporate mass dataveillance and the institutional structures that enable pathological corporate behaviour. Specifically, it introduces a new and broader corporate purpose to create value for the benefit of society, a new duty to limit revenues from behavioural data surpluses, and imposes existential consequences on corporations that fail to do so. Under this duty, corporations must ensure their business models do not derive revenues from the sale of technologies, products, or services that either facilitate, are based on, or are informed or improved by the collection or processing of behavioural data surpluses.

The thesis concludes by emphasizing the need for an interdisciplinary approach to effectively regulate corporate mass dataveillance and limit corporate power, thereby protecting democratic values and individual rights.

Acknowledgments

This thesis is the culmination of a long journey—one filled with books, articles, notebooks, post-its, and endless cups of tea. It has been a journey of joy, discovery, reflection, and frustration. The intersection of technology, society, regulation, and corporate actors has been a fascinating and emotional topic to explore. Reading and writing about this intersection has made me passionate, hopeful, angry, and desperate—sometimes all at the same time.

Throughout this journey, I have been fortunate to have incredible people by my side, to whom I am deeply grateful.

Firstly, to my parents—thank you for your constant concern as I completed my PhD, even though I did not always seem to appreciate it, I know it was your way of showing care and support.

To my husband—thank you for your unwavering support and patience throughout this process, and for always been there to listen as I rode the emotional rollercoaster, ranted about the world and society, and questioned where we were headed.

To Chica—thank you for so many “Bees” conversations, for your constant support, and for always being there to bounce ideas off.

To my supervisor—thank you for your time and support throughout this journey. Your guidance and input not only made this thesis possible, but also helped me grow as a researcher and writer.

To my committee members—thank you for choosing to be part of this journey. Your time, feedback, insightful ideas, and words of encouragement were invaluable.

To all of those that made Ottawa feel like home:

To my family—thank you for all the good times: the trips, the outdoor adventures, the roasts, the movie nights, the BBQs, and most of all, for always making sure I was alright.

To those fantastic people that I meet in UOttawa—thank you for our “Wednesday is the new Friday” gatherings, the good company, and of course the fries, nachos, and beer.

To everyone in the writing group—our sessions exploring Ottawa’s coffee spots kept me on track and your encouragement was invaluable.

And last but not least, to the Edgelands team—your support and community provided a much-needed space to breathe and reflect.

Dedication

For a future where technological innovation is driven by the well-being of society,
not corporate profit.

Chapter I. Introduction

In the early 2000s, utilizing US Supreme Court Justice Louis Brandeis' characterization of corporations as Frankenstein monsters,¹ Joel Bakan contended that, similar to how Dr. Frankenstein created his monster, governments are responsible for the creation of corporations. However, much like the monster, once these corporations came into existence, they posed a danger of overpowering their creators.²

He argued that corporations hold immense power over individuals' lives, influencing what they consume, watch, wear, work, and do. Individuals are inevitably immersed in corporations' cultural influence, symbols, and beliefs. Similar to how the church and monarchy were viewed in the past, they presented themselves as infallible and omnipotent, showcasing their power through grand buildings and elaborate displays. Moreover, they increasingly wield control over government decisions and areas of society traditionally considered to be part of the public sphere.³

He posited that corporations possess psychopathic qualities as they are solely focussed on their own self-interest and lack authentic care for others. Their primary objective is to maximize profits without considering the consequences.⁴ As pathological institutions, they pose a significant threat due to the substantial power they wield over individuals and societies.

¹ *Luis K Liggett Co et al v Lee, Comptroller et al*, 288 U.S. 517, (1933) cited in Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power*, ebook ed (Toronto: Penguin Group, 2009) at 166.

² Bakan, *The Corporation*, *supra* note 1.

³ Bakan, *The Corporation*, *supra* note 1 at 9.

⁴ Bakan, *The Corporation*, *supra* note 1 at 57.

Twenty years later, Bakan asserted that corporations continued to govern people's lives, and that they remained a psychopathic institution, but more charming.⁵ Corporations have used this charm to persuade governments to free them from regulations designed to protect the public interest and individuals' well-being, claiming that they can be trusted to self-regulate. As governments step back from governing, corporations seize greater control, and society transform into one "that no longer *has* corporations but that *is* corporate."⁶

Over the course of those twenty years, certain traditional corporations, such as those in the oil and gas industry and banking sector, continued to grow and gain both economic and political power. Additionally, a new sector emerged and gained significance: the information industry, which deals with the generation, collection, processing, and trading of data on individuals, their behaviours, and their surroundings.

Corporations in the information industry are responsible for developing technologies and services that individuals use on a daily basis. This includes determining the type and amount of data generated, where they are processed, the accuracy and precision of the data, the identifiers linked to them, and the algorithms used to process them. By prioritizing certain functionalities, these corporations embed certain values into their technologies,⁷ giving them significant power. Considering the pathological personality of corporations, the design of these technologies is primarily driven by one goal: profit.

⁵ Joel Bakan, *The New Corporation: How "Good" Corporations are Bad for Democracy*, ebook ed (Canada: Allen Lane, 2020).

⁶ Bakan, *New Corporation*, *supra* note 5 at 8.

⁷ The design of certain architectural structure or physical arrangements can have an explicit or implicit political purpose. See e.g., Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, (Chicago: The University of Chicago Press, 1989) at ch 2; Lawrence Lessig, *Code: Version 2.0*, (New York: Basic Books, 2006) at 341.

In an economic system that rewards the generation, collection, and processing of data for profit-making purposes and thrives on the pathological behaviours of corporations, the design of these technologies will be optimized to continuously collect and generate vast amounts of data. While acknowledging the benefits of these technologies to society and individuals, it is undeniable that the way corporations have designed and used these technologies has resulted in a series of mass dataveillance systems.

The term *mass dataveillance system* refers to technological systems that collect, process, and organize data about individuals and their behaviours on a continuous and systematic basis, with the aim of providing organizations with a basis for action towards those individuals.⁸ The data operations of companies such as Google, Meta, and Uber, among others, fit this definition, as they provide a series of digital technologies and services to individuals that allow them to collect a vast amount of data about their users. These companies then use their own proprietary algorithms to process these data and make correlations, which provide valuable insights that are used to offer personalized content, information, and access to services through the same platform initially used by individuals.

Companies have been processing data on individuals to sort them into predefined categories to make commercial decisions for a long time. What has changed in recent years is the amount of data that companies have access to, the granularity of that data, and the improvement in algorithmic techniques to sort, score, and make automated decisions based on that data. For instance, before the widespread availability of location data, individuals were profiled based on their residential area.⁹ Now, with the advent of digital location technologies and the increased

⁸ See James B Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, (New York: Oxford University Press, 2007) at 14.

⁹ See e.g., Mark Monmonier, *Spying with Maps: Surveillance Technologies and the Future of Privacy*, (Chicago: University of Chicago Press, 2002) at ch 9; Oscar H Gandy, *The Panoptic Sort: A Political Economy of Personal*

availability of location data, geographic profiles have evolved beyond static information to include dynamic insights into individuals' daily movements such as their preferred areas and locations in the city.¹⁰ This enhanced data collection has enabled advanced algorithmic systems to categorize individuals into various groups—such as outdoor enthusiasts, religious individuals, LGBTIQ+ individuals, and government employees—based on the places they visit.

I. Surveillance and Corporations

Surveillance is a practice that has been recognized by academics, NGOs, and international human rights systems as invasive, prone to abuse of power, and a threat to individuals' human rights.¹¹ Digital technologies have radically changed this practice because they enable the easy generation, collection, and processing of vast amounts of data on individuals and their behaviours.¹² Initially, the capability to survey individuals was mostly reserved for governments, as they were the only organizations with the institutional and resource capacity to do so; however, this is no longer the case.

Today corporations have not only acquired the capability to implement extensive mass dataveillance systems, but have also found it extremely profitable to do so.¹³ This shift in

Information, (Boulder, Colorado: Westview, 1993) at 87; Jon Goss, “‘We Know Who You Are and We Know Where You Live’: The Instrumental Rationality of Geodemographic Systems” (1995) 71:2 *Economic Geography* 171.

¹⁰ See e.g., Alex “Sandy” Pentland, “Society’s Nervous System: Building Effective Government, Energy, and Public Health Systems” (2012) 45:1 *Computer* 31 at 32. (“The proliferation of GPS-enabled devices makes it possible to leap beyond demographics to directly measure human behaviour. Where do people eat, work and hang out? What routes do they travel?”)

For detail explanation of the difference between traditional geodemographics and the use of the location data generated and collected by technologies see Harrison Smith, “Metrics, Locations, and Lift: Mobile Location Analytics and the Production of Second-Order Geodemographics” (2019) 22:8 *Information, Communication & Society* 1044.

¹¹ This will be further developed on Chapter III, *below*.

¹² This will be further developed on Chapter III-I.A, *below*.

¹³ This will be further developed on Chapter IV-III, *below*.

surveillance capabilities from governments to corporations has significant implications. While government-led mass surveillance systems and practices are generally prohibited under international human rights law because of their interference with the right to privacy of individuals,¹⁴ corporate surveillance practices have not received the same level of scrutiny. Despite being recognized by academics and NGOs, corporate surveillance practices have not been a prominent concern within this legal framework.

In the international human rights system, for example, surveillance is primarily associated with government activities, whereas corporate practices are generally understood in terms of the flow of information and data processing. However, at their core, corporations, whose business models are data-dependent, do not simply process data; they implement and maintain mass dataveillance systems that allow them to constantly generate and collect an extensive amount of data about individuals' behaviours and surroundings. Furthermore, these companies have the same (or even more) power over the lives of individuals than states, and they are abusing it in the name of profit.¹⁵

Under Article 2(2) of the International Covenant on Civil and Political Rights (ICCPR), states have a responsibility to implement regulatory frameworks that protect individuals from

¹⁴ It has also been recognized that these practices constitute an interference with the rights of freedom of opinion and expression, and free assembly See e.g., UN, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by Frank La Rue, HRC, 23th Sess, UN Doc A/HRC/23/40 (2013); UN, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, by Martin Scheinin, HRC, 13th Sess, UN Doc A/HRC/13/37 (2009); UN Special Rapporteur on Freedom of Opinion and Expression et al, "Joint Declaration on Freedom of Expression and Responses to Conflict Situations" (4 May 2015) online: <oas.org> [<https://web.archive.org/web/20231220114722/https://www.oas.org/en/iachr/expression/showarticle.asp?artID=987&IID=1>].

¹⁵ See e.g., Zeynep Tufekci, "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency" (2015) 13 *Colorado Technology Law Journal* 203; Rule, *Privacy in Peril*, *supra* note 8; Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*, (Cambridge, UK: Cambridge University Press, 2021). [Waldman, *Industry Unbound*].

interference with their rights by both state and private actors.¹⁶ As part of this obligation, many states have established data protection frameworks to oversee corporations' data collection and processing practices.¹⁷ However, the rapidly evolving digital landscape requires regular evaluation of these frameworks to ensure their continued effectiveness. According to Lyria Bennet Moses, it is crucial to periodically assess the effectiveness of laws and regulations to ensure their relevance and alignment with the sociotechnical landscape that they aim to govern.¹⁸ This assessment is particularly important in the context of data protection, given the rapid advances in technology and the increasing complexity of data practices.

Considering the context described above, this thesis seeks to evaluate whether existing data protection frameworks are sufficient to regulate and monitor corporate data practices in the current sociotechnical landscape, and therefore adequate for states to fulfil their ICCPR obligations, or whether a new framework is required instead. To guide this analysis, this thesis uses location dataveillance systems as concrete examples of the current sociotechnical landscape.

Location dataveillance systems and the location data they generate are particularly relevant for four reasons. First, location data are collected without the active involvement of individuals. This differs from, for example, social media data, as the latter (usually) requires individuals not

¹⁶ *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976). [ICCPR]

¹⁷ For a list of international standards for the processing of personal data see OHCHR, *The Right to Privacy in the Digital Age*, HRC, 39th Sess, UN Doc A/HRC/39/29 (2018) at para 28; UNCTAD, "Data Protection and Privacy Legislation Worldwide" (last visited 11 October 2021) online: <[unctad.org](http://web.archive.org/web/20231220111334/https://unctad.org/page/data-protection-and-privacy-legislation-worldwide)> [http://web.archive.org/web/20231220111334/https://unctad.org/page/data-protection-and-privacy-legislation-worldwide].

¹⁸ Bennet Moses theory will be developed in Chapter II, *below*.

See also Lyria Bennett Moses, "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target" (2013) 5:1 *Law, Innovation and Technology* 1 at 11.

only to create an account, but also to interact with certain content (i.e., read, like, or share).¹⁹ Second, the widespread use of digital technologies, such as smartphones and wearables, makes location dataveillance systems indiscriminate, as corporations can collect location data from anyone using these devices.²⁰ Third, location data are highly versatile and profitable.²¹ Corporations can combine them with other datasets to enrich user profiles with geographic details, or use location data alone to infer individuals' lifestyles. This versatility enables corporations to profit from these data through at least two sources: digital advertising and the sale of pooled location data. This second category opens up the revenue streams beyond online advertising, to government agencies, businesses, researchers, journalists, and others who are interested in buying these data.²² Finally, the growing market for location data demonstrates an increasing incentive for corporations to collect and generate such data.²³

¹⁹ See e.g., Zeynep Tufekci, "As the Pirates Become CEOs: The Closing of the Open Internet" (2016) 145:1 *Daedalus* 65 at 65–78.

On this point it is important to highlight that an individual may not actively participate in social media, but nevertheless information about them may be posted by others there.

²⁰ See e.g., Agnieszka Leszczynski, "Geoprivacy" in Rob Kitchin, Tracey P Lauriault & Matthew W Wilson, eds, *Understanding Spatial Media* (London: SAGE Publications, 2017) 235.

²¹ See e.g. Mark N Gasson et al, "Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones" (2011) 41:2 *IEEE Transactions on Systems, Man, and Cybernetics, Part C* 251; Michael Herrmann et al, "Privacy in Location-Based Services: An Interdisciplinary Approach" (2016) 13:2 *SCRIPTed* 144; Daniel Ashbrook & Thad Starner, "Using GPS to Learn Significant Locations and Predict Movement Across Multiple Users" (2003) 7 *Personal and Ubiquitous Computing* 275.

²² See e.g., Roger Clarke & Marcus Wigan, "You are Where You've Been: the Privacy Implications of Location and Tracking Technologies" (2011) 5:3–4 *Journal of Location Based Services* 138 at 150.

²³ See e.g., Ryan Dezember, "Your Smartphone's Location Data Is Worth Big Money to Wall Street", *Wall Street Journal* (2 November 2018), online: <wsj.com> [<http://web.archive.org/web/20210624215349/https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260>]; Jon Keegan & Alfred Ng, "There's a Multibillion-Dollar Market for Your Phone's Location Data", *The Markup* (30 September 2021), online: <themarkup.org> [<http://web.archive.org/web/20211001105321/https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>]; Joseph Cox, "CBP Bought 'Global' Location Data from Weather and Game Apps", (6 October 2020), online: <vice.com> [<http://web.archive.org/web/20230329193633/https://www.vice.com/en/article/n7wakg/cbp-dhs-location-data-venntel-apps>].

This thesis builds upon the existing literature that acknowledges the inadequacies of data protection as a means of curbing corporate surveillance powers and protecting the privacy of individuals and society.²⁴ Extending this literature, this thesis incorporates Bakan's theory to offer a fresh perspective on data protection frameworks, emphasizing the need for regulators to consider the psychological personality of corporations. This consideration is crucial given the power that corporations wield in the design, marketing, and use of digital technologies that individuals use in their daily lives and that grant these corporations dataveillance capabilities.

Using Bakan's theory, this thesis highlights the inherent misalignment between corporate interests and the regulatory objectives of data protection regulation. It argues that existing data protection frameworks are not adequate, not only because they are based on privacy as consent and control, but also because they are based on two outdated assumptions about the sociotechnical landscape they aim to regulate. First, these frameworks assume that it is necessary for corporations to collect and process data about individuals, making it difficult to analyze and question the necessity and proportionality of corporate dataveillance systems. Second, they assume that corporations are benevolent entities capable of changing their behaviour to comply with regulations and protect the rights of their users, even when doing so would negatively affect their profits, overlooking the pathological nature of the entities they seek to regulate.

Given the inadequacy of existing data protection frameworks to regulate corporate mass dataveillance and mitigate its risks to privacy and other human rights, this thesis proposes a new regulatory framework. This framework aims to constraint corporate mass dataveillance by targeting corporation's primary driver: profit. To achieve this, it seeks to limit business models that

²⁴ See e.g., Valerie Steeves, "Now You See Me: Privacy, Technology, and Autonomy in the Digital Age" in Gordon DiGiacomo, ed, *Human Rights: Current Issues and Controversies* (Toronto: University of Toronto Press, 2016) 461; Waldman, *Industry Unbound*, *supra* note 15; Neil M Richards & Woodrow Hartzog, "Privacy's Constitutional Moment" (2020) 61 Boston College Law Review 1687.

rely on the collection and processing of behavioural data surpluses, as the profitability of such data is the driving force behind the development and deployment of mass dataveillance systems. In addition, the framework aims to address the root causes of corporate misconduct by modifying some of the institutional structures that enable the pathological corporate behaviour. By regulating both the profit incentives and the structural features that enable harmful practices, this framework aims to effectively reduce the risks posed by corporate mass dataveillance.

While this proposed framework offers a legal perspective on the regulation of corporate mass dataveillance, effective regulation requires a multifaceted and interdisciplinary approach. Addressing the complexities of corporate dataveillance requires an approach that incorporates the insights and expertise of professionals from fields such as sociology, information studies, economics, engineering, and the active participation of civil society. Moreover, the regulation of corporate dataveillance is only one aspect of the broader challenge of addressing corporate power over democratic institutions and societies. Comprehensive reform is essential to limit and regulate corporate influence and address its potentially harmful tendencies in order to protect the values and rights that underpin a democratic society.

II. Structure of the Thesis

The remainder of this thesis is organized into six chapters. Chapter II reviews the relevant literature on the subject and outlines the methodology of this thesis, which focusses on the relationship between law, technology, and society. Specifically, this thesis uses the analytical lenses proposed by Bennett Moses to assess the effectiveness of regulatory frameworks in addressing the challenges posed by a rapidly evolving sociotechnical landscape.

Chapter III focusses on the international human rights framework and its application to government surveillance practices. It begins by discussing how technological advancements have

transformed government-led surveillance from the Second World War to the present. It then examines the development and evolution of the right to privacy within the international human rights framework, and analyzes how this framework has been applied to evaluate government-led mass surveillance systems and location-based surveillance practices.

Chapter IV shifts the focus to corporations as key players in the current sociotechnical system. The chapter begins by introducing Bakan's theory of corporations as psychopathic institutions, and examines how corporation such as Uber Technologies Inc (Uber Inc) and Meta Platforms Inc (Meta Inc), adhere to this concept. These corporations, which offer location-based services (LBS), rely on business models driven by extensive data collection, processing, and analysis. The chapter demonstrates that these corporations exhibit psychopathic tendencies consistent with Bakan's framework. The chapter concludes by discussing mass dataveillance systems as a manifestation of this psychopathic personality. It examines the economic system in which these corporations operate, how this influences the design and marketing of technologies, and the risks posed by these systems.

Chapter V turns back to international human rights framework, focussing on the responsibility of states under Article 2(2) of the ICCPR to establish regulatory frameworks that protect individuals from interference with their rights by both state and private actors, including corporations. As many states have implemented data protection frameworks to fulfil part of this responsibility regarding corporate data processing operations, this chapter examines the effectiveness of data protection regulations in addressing corporate mass dataveillance. The chapter uses the GDPR and PIPEDA as examples. The GDPR for its global significance and influence as a European Union regulation, and PIPEDA as an example of a national framework governing data processing in commercial activities within Canada.

The argument of this chapter is that current data protection frameworks are outdated, as their regulatory goals and assumptions do not consider the current sociotechnical landscape. These frameworks were established to foster trust and promote a data-based economy. They were enacted on the premise that the collection and processing of data about individuals and their behaviours by corporations is necessary to advance the data-based economy. However, the regulation of corporate dataveillance capabilities becomes challenging when it is assumed that the generation and processing of data on individuals are an acceptable practice. Additionally, these frameworks assume that corporations, as key players in the economy, modify their behaviour to comply with regulations and safeguard their users' rights, even if they negatively impact their profits. This assumption disregards the pathological nature of corporations and their self-interest motivations.

Chapter VI addresses the limits of data protection by proposing a regulatory framework to constrain the mass dataveillance capabilities of corporations. This framework aims to reform existing corporate law to limit both the business models and the pathological personality of corporations that derive revenue from technologies, products, or services that either facilitate, are based on, or are enhanced by the collection or processing of behavioural data surpluses.

The framework targets two key aspects of the institutional nature of corporations that contribute to their pathological behaviour. The first is the combination of three elements: a corporate purpose narrowly focussed on profit, a duty requiring directors to prioritize profit maximization, and an internal legal structure with minimal constraints on how these goals can be achieved. The second is the absence of meaningful consequences for corporate non-compliance, which reduces legal compliance to a mere cost-benefit analysis.

Taking these two aspects into account, the proposed framework has two main features. First, it redefines corporate purpose by broadening the corporate mission beyond profit

maximization and introducing a duty to limit revenue streams derived from behavioural data surpluses. As explained in more detail in Chapter IV, “behavioural data surpluses” refer to data generated by an individual’s interactions with technology that goes beyond what it is necessary to improve that technology, service, or product. These changes are designed to refocus corporate purpose and set clear limits on acceptable revenue generation practices. Second, the framework introduces mandatory corporate dissolution for non-compliance. This measure ensures that corporations face existential consequences for illegal or harmful activities, reinforcing the principle that governments, which grant corporations the right to exist and operate, can revoke that right when corporations endanger society.

Chapter VII concludes by summarizing the main argument of this thesis, highlighting its significance and contributions, and explaining its limitations. Additionally, it outlines questions for future research.

Chapter II. Literature Review and Methodology

A growing number of businesses revolve around the generation, collection, and processing data. With technological advances such as Artificial Intelligence (AI) and Big Data, the generation and collection of data about people's everyday activities are becoming increasingly essential to many industries. Corporations analyze data such as shopping preferences, political views, health data, and location to predict patterns, understand behaviours, and target people with personalized advertising, information, and services.²⁵;

In this growing landscape of data-driven transactions, location data has emerged as a critical component. These data enable commercial data analysts to distinguish between real human users and bots designed to generate automated content and responses on social media. From a business perspective, the integration of location data into online activity offers significant value to advertisers and marketers, who are among the primary actors involved in user profiling. Location and movement data serves as a reliable indicator of an individual's presence online, reinforcing the identification of a real person behind digital interactions.²⁶

The introduction of faster electronic communications standards, such as 5G mobile networks, has further accelerated this trend. These standards enable the transmission of larger volumes of data at a higher speed, including real-time data, and have fuelled the spread of internet-connected devices. While these innovations enhance the functionality of technologies and improve the consumer experience, they have also enabled corporations to collect vast amounts of detailed

²⁵ See e.g., Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, (Los Angeles: SAGE, 2014) at 119–123; European Commission, *A European Strategy for Data*, COM(2020) 66 final (19 February 2020) CELEX:52020DC0066.

²⁶ See e.g., Yves-Alexandre de Montjoye et al, "Unique in the Crowd: The Privacy Bounds of Human Mobility" (2013) 3:1376 *Nature* 1.

data about their users.²⁷ Notably, in this data-driven market model, communication and data exchange between stakeholders occurs on a global scale, amplifying both opportunities and challenges.

This chapter will review the relevant literature and outline the methodology of this thesis. It is divided into two main parts. The first part reviews the existing literature on digital technologies, privacy, and data protection, with a particular focus on location technologies as concrete examples of the current socio-technical landscape. Recognizing the interdisciplinary nature of this topic, this review draws from a variety of fields, including law, geography, social sciences, computer science, and engineering. The second part outlines the law, technology, and society methodology used in this thesis. In particular, it explains how the analytical lens proposed by Bennett Moses is used to assess the effectiveness of data protection regulation in addressing the challenges posed by a rapidly evolving socio-technical landscape.

I. Previous Literature on Privacy and Location Technologies

The intersection of location technologies and privacy has been studied extensively in a variety of disciplines, including law, geography, engineering, and computer science, and by a variety of stakeholders, including academics, regulatory bodies, interdisciplinary groups, and industry groups. This part categorizes the relevant literature into two parts: (1) privacy concerns

²⁷ See e.g., Mohsen Attaran, “The Impact of 5G on the Evolution of Intelligent Automation and Industry Digitization” (2023) 14:5 *Journal of Ambient Intelligence and Humanized Computing* 5977; Mitrabinda Khuntia, Debabrata Singh & Sipra Sahoo, “Impact of Internet of Things (IoT) on 5G”(Paper delivered at the 1st International Conference on Intelligent and Cloud Computing, Bhubaneswar, India, December 20, 2019) in Debahuti Mishra et al, eds, *ICICC 2019* (Singapore: Springer, 2021) 125, DOI:<10.1007/978-981-15-6202-0_14>; McKinsey & Company, “What is 5G technology?” (7 October 2022) online: <mckinsey.com> [<http://web.archive.org/web/20231112053416/https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-5g>].

raised by location technologies and proposed solutions, and (2) criticisms of data protection legislation as an adequate solution to address privacy issues.

A. Privacy Concerns and Proposed Solutions

This subsection summarizes the first group of relevant literature: privacy issues associated with location technologies, and explores the solutions proposed in the literature to address them. This literature is important for this research because it provides a multidisciplinary perspective on the challenges posed by location technologies and explores the potential solutions and their limitations. It also highlights the shortcomings of existing regulatory frameworks, such as the reliance on technological tools to protect individuals' location data. For instance, anonymity remains a commonly proposed measure to mitigate the risks associated with personal data, allowing organizations to use such data more freely. While this approach may be effective for some types of personal data, advances in computing power are increasingly challenging its reliability in the case of location data.²⁸

1) Privacy Concerns

The main concern identified in the literature is the ability of location technologies to reveal and increase the visibility of individual behavioural patterns,²⁹ enabling the creation of detailed movement profiles. The location data generated and collected by these technologies allows

²⁸ See Section 2.b, *below*, for more on this topic.

²⁹ See Roger Clarke, "Person Location and Person Tracking: Technologies, Risks and Policy Implications" (2001) 14:2 *Information Technology & People* 206; F Bonchi et al, "Privacy in Spatiotemporal Data Mining" in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 297; John Krumm, "A Survey of Computational Location Privacy" (2009) 13 *Pers Ubiquit Comput* 391; Maria Luisa Damiani, "Privacy Enhancing Techniques for the Protection of Mobility Patterns in LBS: Research Issues and Trends" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2012) 223.

organizations to reconstruct the movements of individuals across space and time,³⁰ revealing sensitive details about an individual's lifestyle based on information inferred from the places they visit³¹ and their travel patterns.³² Advances in computing power, data storage capacity, and analytical algorithms have exacerbated these concerns, making it easier for organizations to

³⁰ See Eleni Kosta et al, "Legal Considerations on Privacy-Enhancing Location Based Services Using PRIME Technology" (2008) 24 Computer Law & Security Review 139; de Montjoye et al, "Unique in the Crowd", *supra* note 26; Office of the Privacy Commissioner of Canada, *Location Technologies: Mobility, Surveillance and Privacy*, by David Lyon, Stephen Marmura & Pasha Peroff, Contributions Program (Ottawa: OPC, 2005).

³¹ See WP29, *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices*, 811/11/EN WP 185 (2011); Jorge R Cuellar, "Location Information Privacy" in Behcet Sarikaya, ed, *Geographic Location in the Internet* (New York: Springer, 2002) 179; Mark Monmonier, "The Internet, Cartographic Surveillance, and Locational Privacy" in Michael Peterson, ed, *Maps and the Internet* (Pergamon, 2003) 97; Robert P Minch, "Privacy Issues in Location-Aware Mobile Devices" (Paper delivered at the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, January 5-8, 2004) in Ralph H. Sprague, ed, *Proceedings HICSS 2004* (California: IEEE, 2004) 1, DOI:<10.1109/HICSS.2004.1265320>; D Pedreschi et al, "Privacy Protection: Regulations and Technologies, Opportunities and Threats" in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 101; V S Verykios, M L Damiani & A Gkoulalas-Divanis, "Privacy and Security in Spatiotemporal Data and Trajectories" in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 213; Michael Decker, "Location Privacy-An Overview" (Paper delivered at the 7th International Conference on Mobile Business, Barcelona, July 7-8, 2008) in Silvia Ceballos, ed, *Proceedings ICMB 2008* (California: IEEE, 2008) 221, DOI:<10.1109/ICMB.2008.14>; Mark Burdon, "Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws" 2010:1 Journal of Law, Technology and Policy 1; Anna Monreale et al, "C-Safety: A Framework for the Anonymization of Semantic Trajectories" (2011) 4:2 Transactions on Data Privacy 73; Sébastien Gambs, Marc-Olivier Killijian & Miguel Núñez del Prado Cortez, "Show Me How You Move and I Will Tell You Who You Are" (Paper delivered at the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, San Jose, CA, November 2, 2010) in Maria Luisa Damiani & Yucel Saygin, eds, *Spring'10* (New York: ACM, 2010) 34, DOI:<10.1145/1868470.1868479>; Anna Monreale et al, "Privacy-Preserving Distributed Movement Data Aggregation" in Danny Vandenbroucke, Bénédicte Bucher & Joep Cromptvoets, eds, *Geographic Information Science at the Heart of Europe* (Cham: Springer, 2013) 225; de Montjoye et al, "Unique in the Crowd", *supra* note 26; Chao Lee, Yunchuan Guo & Lihua Yin, "A Framework of Evaluation Location Privacy in Mobile Network" (2013) 17 Procedia Computer Science 879; Katina Michael & Roger Clarke, "Location and Tracking of Mobile Devices: Überveillance Stalks the Streets" (2013) 29 Computer Law & Security Review 216; ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, (California: ACLU, 2010) online: <aclunc.org> [http://web.archive.org/web/20220126145214/https://www.aclunc.org/sites/default/files/asset_upload_file183_9627.pdf]; Jeffrey H Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future" (1995) 11 Computer & High Technology Law Journal 27; Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places" (2000) 50:3 University of Toronto Law Journal 305.

³² Minch, "Privacy Issues in Location-Aware Mobile Devices", *supra* note 31; Delphine Christin & Matthias Hollick, "Roadmap for Privacy Protection in Mobile Sensing Applications" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2012) 203.

classify individuals into algorithmically defined groups, which are often used as the basis for discriminatory practices.³³

Other issues identified arise from the expected and unexpected uses of location technologies and location data.³⁴ For example, easy access to such data poses two major risks: it creates risks to personal safety and increases the risk of tracking turning into intrusive surveillance.

First, knowing people's whereabouts opens the door to new ways of intruding on their privacy,³⁵ creating risks to their personal safety,³⁶ and potentially leading to unforeseen negative consequences, such as stalking.³⁷ It also increases the scope for politically damaging and personally embarrassing disclosures, blackmail, and extortion.³⁸

Second, by enabling the tracking of individuals' everyday activities and movements,³⁹ location technologies enable various organizations such as corporations and governments (and

³³ See e.g., Kitchin, *Data Revolution*, *supra* note 25 at 175–78; David Murakami Wood, “Spatial Profiling, Sorting and Prediction” in Rob Kitchin, Tracey P Lauriault & Matthew W Wilson, eds, *Understanding Spatial Media* (London: SAGE Publications, 2017) 225; Gandy, *Panoptic Sort*, *supra* note 9; Linnet Taylor, “Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World” in Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds, *Group Privacy: New Challenges of Data Technologies* (Cham: Springer International, 2017) 13.

³⁴ See e.g., Office of the Privacy Commissioner of Canada, *Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices*, (consultation paper) (Ottawa: OPC, 2008) at 9; Monmonier, “Internet, Cartographic Surveillance, and Location Privacy”, *supra* note 31.

³⁵ See Monreale et al, “C-safety”, *supra* note 31.

³⁶ Minch, “Privacy Issues in Location-Aware Mobile Devices”, *supra* note 31; Lee, Guo & Yin, “Framework of Evaluation Location Privacy in Mobile Network”, *supra* note 31; William A Herbert, “No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?” (2006) 2:2 *I/S: A Journal of Law and Policy for the Information Society* 409; Institute for Law and Justice, *Privacy in the Information Age: A Guide for Sharing Crime Maps and Spatial Data*, by Julie Wartell & J Thomas McEwen, NCJ 188739 (Washington, DC: US Department of Justice, 2001) online: <ojp.gov> [<http://web.archive.org/web/20231219151816/https://www.ojp.gov/pdffiles1/nij/188739.pdf>]; Reza Shokri et al, “Quantifying Location Privacy”(Paper delivered at the 2011 IEEE Symposium on Security and Privacy, Oakland, CA, May 22-25, 2011) in Lisa O’Conner, ed, *Proceedings SP 2011* (California: IEEE, 2011) 247, DOI:<10.1109/SP.2011.18>; Linda Ackerman, James Kempf & Toshio Miki, *Wireless Location Privacy: Law and Policy in the US, EU and Japan*, Isoc Member Briefing #15 (Virginia: Internet Society, 2003) online: <isoc.org> [<https://web.archive.org/web/20050117191259/http://www.isoc.org/briefings/015/briefing15.pdf>].

³⁷ See Herbert, “No Direction Home”, *supra* note 36; Anne SY Cheung, “Location Privacy: The Challenges of Mobile Service Devices” (2014) 30 *Computer Law & Security Review* 41.

³⁸ See Clarke, “Person Location and Person Tracking”, *supra* note 29.

³⁹ See John B Morris, “The Elements of Location Tracking and Privacy Protection” in Behcet Sarikaya, ed,

those with access to the data collected) to constantly monitor individuals' activities,⁴⁰ and to store and analyze such data for extended surveillance.⁴¹ These technologies have also made it possible for a single organization to remotely monitor the movements of one or more individuals for an unlimited period of time and to determine their precise location at any given moment.⁴²

The ubiquitous tracking and recording of individuals' movements have also led to a loss of anonymity in everyday activities in public places.⁴³ Anonymity is a fundamental element of what it means to be human and, as such, it is important to preserve it.⁴⁴ The inability to carry out daily activities anonymously can have a chilling effect on the development of individuals and their rights, such as freedom of association.⁴⁵

Geographic Location in the Internet (New York: Kluwer Academic Publishers, 2002) 163; Alastair R Beresford & Frank Stajano, "Location Privacy in Pervasive Computing" (2003) 2:1 IEEE Pervasive Computing 46; Office of the Privacy Commissioner of Canada, *Locational-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risk in Canada*, by Colin J. Bennett & Lori Crowe, Contributions Program 2004-05 (Ottawa: OPC, 2005); Lyon, Marmura & Peroff, *Location Technologies*, *supra* note 30.

⁴⁰ See e.g., April A Otterberg, "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space under the Fourth Amendment" (2005) 46:3 Boston College Law Review 661.

⁴¹ See Michael R Curry, "Digital People, Digital Places: Rethinking Privacy in a World of Geographic Information" (1997) 7:3 Ethics & Behavior 253; Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39.

⁴² See Renée McDonald Hutchins, "Tied Up in Knotts? GPS Technology and the Fourth Amendment" (2007) 55 UCLA Law Review 409.

⁴³ See Moira Paterson, "Surveillance in Public Places: The Regulatory Dilemma" in Normann Witzleb et al, eds, *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge, UK: Cambridge University Press, 2014) 201; Reiman, "Driving to the Panopticon", *supra* note 31; Helen Nissenbaum, "Toward an Approach to Privacy in Public: Challenges of Information Technology" (1997) 7:3 Ethics & Behavior 207.

⁴⁴ See e.g., Carole Lucock & Katie Black, "Anonymity and the Law in Canada" in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy & Identity in a Networked Society* (New York: Oxford University Press, 2009) 465; Joseph Siprut, "Privacy Through Anonymity: An Economic Argument for Expanding the Right of Privacy in Public Places" (2006) 33 Pepperdine Law Review 311; Tjerk Timan, "Conclusion: The Need for Privacy in Public Space" in Tjerk Timan, Bryce C Newell & Bert-Jaap Koops, eds, *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar Publishing, 2017) 269; *R v Spencer*, 2014 SCC 43 at para 71 [*Spencer*].

⁴⁵ See Paton-Simpson, "Protection of Privacy in Public Places", *supra* note 31.

2) Proposed Solutions

The solutions proposed to address the issues raised by location technologies differ not only in their objectives, but also in the instruments proposed to implement them (i.e., law, policy, or technology).⁴⁶ They can be broadly divided into two main groups: solutions that aim to give individuals more control over their data, and solutions that aim to minimize the risks posed by the data collected. In addition to these two groups, this subsection will also examine the literature on privacy by design, as it is proposed as an essential element of privacy protection.

(a) Giving Individuals More Control Over Their Data

The first group of authors advocate empowering individuals to exercise control over their data, but differ on which part of the data chain is more important to exercise control over. For instance, some emphasize the importance of having control over how data are used,⁴⁷ others over

⁴⁶ For a summary of the different methods see Caitlin D Cottrill, “Location Privacy: Who Protects?” (2011) 23:2 URISA 49 at 52.

⁴⁷ See Carlos Rodríguez Casal, “Location and Personal Information for Direct Marketing: Third Generation Killer Application” (2003) 5:2 info 45; Marco Furini, “Users Behavior in Location-Aware Services: Digital Natives versus Digital Immigrants” 2014 *Advances in Human-Computer Interaction* 1; Cheung, “Location Privacy”, *supra* note 37.

what data are collected and how these are collected,⁴⁸ others over how data are disclosed or shared with others,⁴⁹ and others place more emphasis on being able to control access to the data.⁵⁰

Mechanisms to achieve this includes legal measures that grant individuals certain rights over their information, such as data protection regulations,⁵¹ and technological tools that allow users to manage their preferences.⁵² Examples include controls to enable or disable the location tracking feature of the device or service, and dynamic systems where privacy preferences are automatically managed by a third party as individuals move through different locations and interact

⁴⁸ See Morris, “Elements of Location Tracking”, *supra* note 39.

⁴⁹ See Dan Cvrcek et al, “The Value of Location Information: A European-Wide Study”(Paper delivered at the 14th International Workshop on Security Protocols, Cambridge, UK, March 27-29, 2006) in Bruce Christianson et al, eds, *Security Protocols* (Berlin: Springer, 2009) 112, DOI:<10.1007/978-3-642-04904-0_15>; Matt Duckham & Lars Kulik, “Location Privacy and Location-Aware Computing” in Roland Billen, Elsa Joao & David Forrest, eds, *Dynamic and Mobile GIS : Investigating Changes in Space and Time* (Boca Raton: CRC Press, 2006); Verykios, Damiani & Gkoulalas-Divanis, “Spatiotemporal Data and Trajectories”, *supra* note 31; Krumm, “Survey Computational Location Privacy”, *supra* note 29; Gambis, Killijian & Núñez del Prado Cortez, “Show Me How You Move”, *supra* note 31; Shokri et al, “Quantifying Location Privacy”, *supra* note 36; Michael & Clarke, “Location and Tracking of Mobile Devices”, *supra* note 31; Mark J Keith et al, “Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior” (2013) 71:12 International Journal of Human-Computer Studies 1163; Caitlin D Cottrill & Piyushimita “Vonu” Thakuriah, “Privacy in Context: An Evaluation of Policy-Based Approaches to Location Privacy Protection” (2014) 22:2 International Journal of Law and Information Technology 178–207, online: <<http://ijlit.oxfordjournals.org/cgi/doi/10.1093/ijlit/eat014>>; Caitlin D Cottrill & Piyushimita “Vonu” Thakuriah, “Location Privacy Preferences: A Survey-Based Analysis of Consumer Awareness, Trade-Off and Decision-Making” (2015) 56 Transportation Research Part C 132; Christin & Hollick, “Roadmap Privacy Protection”, *supra* note 32; Aran Khanna, “Facebook’s Privacy Incident Response: A Study of Geolocation Sharing on Facebook Messenger” (2015) Technology Science, online: <[techscience.org](http://web.archive.org/web/20231222114452/https://techscience.org/a/2015081101/)> [<http://web.archive.org/web/20231222114452/https://techscience.org/a/2015081101/>].

⁵⁰ See Sarah Elwood & Agnieszka Leszczynski, “Privacy, Reconsidered: New Representations, Data Practices, and the Geoweb” (2011) 42 Geoforum 6; Einar Snekkenes, “Concepts for Personal Location Privacy Policies”(Paper delivered at the 3rd ACM conference on Electronic Commerce, Tampa, FL, October 14-17, 2001) in Michael P. Wellman & Yoav Shoham, eds, *EC’ 01* (New York: ACM, 2001) 48, DOI:<10.1145/501158.501164>; Douglas A Fretty, “Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places” (2011) 16:03 Virginia Journal of Law & Technology 430; Ginger Myles, Adrian Friday & Nigel Davies, “Preserving Privacy in Environments with Location-Based Applications” (2003) 2:1 IEEE Pervasive Computing 56.

⁵¹ Some authors argue that it is important to extend the domain where individuals can exercise such control. See e.g., Roger C Geissler, “Private Eyes Watching You: Google Street View and the Right to an Inviolable Personality” (2012) 63 Hastings Law Journal 897; ACLU of Northern California, *Location-Based Services*, *supra* note 31.

⁵² See e.g., Mark Monmonier, “Geolocation and Locational Privacy: The ‘inside’ Story on Geospatial Tracking” in Katherine J Strandburg & Daniela Stan Raicu, eds, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (New York: Springer, 2005) 75 at 90; Morris, “Elements of Location Tracking”, *supra* note 39.

with different people.⁵³ These solutions emphasize the choice and ability of individuals to set their preferences for their location data.

However, the reliance on individual control has been criticized as too narrow and outdated, particularly in the current socio-technical context.⁵⁴ For example, giving individuals more control over their data does not necessarily prevent organizations from inferring information from other people's data:⁵⁵ if someone shares a picture on social media that includes other people,⁵⁶ or provides their DNA for a genetic test,⁵⁷ organizations can easily use algorithms to analyze the data and infer information about the other people involved—in the first case, the individuals in the picture, and in the second case, members of their family.

Similarly, giving individuals more control over their data does not prevent organizations from placing individuals into algorithmically sorted groups and making inferences about them based on the inferential characteristics of those groups. The use of big data analytics allows organizations to identify patterns and characteristics between individuals, allowing groups to be

⁵³ See e.g., Meg Leta Jones, "The Internet of Other People's Things: Conceptual and Regulatory Challenges" in Tjerk Timan, Bryce C Newell & Bert-Jaap Koops, eds, *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar Publishing, 2017) 242; Sneekenes, "Concepts Location Privacy Policies", *supra* note 50; ACLU of Northern California, *Location-Based Services*, *supra* note 31; Katie Shilton, "Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection" (2009) 52:11 Communications of the ACM 48.

⁵⁴ See e.g., Linnet Taylor, Luciano Floridi & Bart van der Sloot, "Introduction: A New Perspective on Privacy" in Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds, *Group Privacy: New Challenges of Data Technologies* (Cham: Springer International, 2017) 1 at 6.

⁵⁵ Some people refer to this as the network effect. See e.g., Taylor, Floridi & van der Sloot, "Introduction", *supra* note 54 at 9.

Others refer to this as interdependent privacy. See e.g., Mathias Humbert, Benjamin Trubert & Kévin Huguenin, "A Survey on Interdependent Privacy" (2020) 52:6 ACM Computing Surveys 122:1.

⁵⁶ See e.g., Taylor, Floridi & van der Sloot, "Introduction", *supra* note 54 at 9.

⁵⁷ See e.g., danah boyd, "Networked Privacy" (2012) 10:3/4 Surveillance & Society 348–350 at 348.

formed based on similar attributes, and in some cases, the habits and characteristics of a single individual can be used to draw conclusions about an entire group.⁵⁸

(b) Minimizing the Risks Associated with Collected Data

The second group of solutions focusses on minimizing the risks associated with collected location data, either by modifying some or all of the attributes of these data (i.e., identity, position, and time),⁵⁹ or by reducing the volume of data collected. There are four types of location privacy preservation mechanisms (LPPMs): cryptography, shared information reduction, obfuscation, and anonymization.⁶⁰ These solutions have in common that they do not depend on the active participation of the individual in order to work.

Cryptographic mechanisms protect the user's location through encryption,⁶¹ with the aim of providing services without revealing the user's actual location to other users.⁶² The main challenge of these mechanisms is their computational complexity and server cooperation requirements.⁶³

⁵⁸ See e.g., Lanah Kammourieh et al, "Group Privacy in the Age of Big Data" in Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds, *Group Privacy: New Challenges of Data Technologies* (Cham: Springer International, 2017) 37 at 38–43; Michele Loi & Markus Christen, "Two Concepts of Group Privacy" (2020) 33:2 *Philosophy & Technology* 207–224 at 220; House of Commons, *Submissions on Bill C-27 The Digital Charter Implementation Act*, 44-1 (5 October 2023) (Brief submitted by Jane Bailey, Jacquelyn Burkell, and Brenda McPhail) online: <ourcommons.ca> [<https://web.archive.org/web/20240214183340/https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/R12605252/br-external/Jointly3-e.pdf>] at 5.

⁵⁹ See generally Bo Liu et al, "Location Privacy and Its Applications: A Systematic Study" (2018) 6 *IEEE Access* 17606 at 17611; *A Unified Framework for Location Privacy*, by Reza Shokri, Julien Freudiger & Jean-Pierre Hubaux, EPFL Report 148708 (Switzerland: LCA, EPFL, 2010).

⁶⁰ See Liu et al, "Location Privacy and Its Applications", *supra* note 59 at 17611.

⁶¹ See Liu et al, "Location Privacy and Its Applications", *supra* note 59.

⁶² See e.g., Sergio Mascetti et al, "Anonymity: A Comparison Between the Legal and Computer Science Perspectives" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2012) 85.

⁶³ See Liu et al, "Location Privacy and Its Applications", *supra* note 59 at 17612.

Reducing shared information mechanisms aim to reduce the amount of location data shared with organizations. To do this, some proposals process the data within devices, transmitting only the necessary data,⁶⁴ while others focus on setting limits on data sharing between organizations⁶⁵ and retention periods.⁶⁶

Obfuscation mechanisms reduce the accuracy of the location data by adding dummy locations,⁶⁷ hiding parts of users' trajectories,⁶⁸ or reducing the granularity of the data.⁶⁹ One of the limitations identified is that these mechanisms are at the expense of the user experience.⁷⁰

⁶⁴ See e.g., Bart Jacobs & Wiebren de Jonge, "Privacy-Friendly Electronic Traffic Pricing via Commits" (Paper delivered at the 5th International Workshop, Formal Aspects in Security and Trust, Malaga, Spain, October 9-10, 2008) in Pierpaolo Degano, Joshua Guttman & Fabio Martenelli, eds, *Formal Aspects in Security and Trust* (Berlin: Springer, 2009) 143, DOI:<10.1007/978-3-642-01465-9_10> (proposing not to send car journeys are not to a central server for a fee computation but to keep on the on-board computer, and only transmit aggregated data just every few times a month for billing); Bart Jacobs, "Architecture is Politics: Security and Privacy Issues in Transport and Beyond" in Serge Gutwirth, Yves Poulet & Paul De Hert, eds, *Data Protection in a Profiled World* (Dordrecht: Springer, 2010) 289 (proposing a decentralized system where there is an in-context data storage); Melissa Gaughan, *Privacy in the Smart City: Implications of Sensor Network Design, Law, and Policy for Locational Privacy* (Master of Urban Planning, University of Washington, 2016) [unpublished] (processing the data inside the device before it is sent).

⁶⁵ See Information and Privacy Commissioner Ontario, *Redesigning IP Geolocation Privacy by Design and Online Targeted Advertising*, by Ann Cavoukian, (Toronto: IPC-ON, 2010). This is also the regulatory approach of the California regulation (limiting the information that is sent) see *The California Consumer Privacy Act of 2018*, c 735, 2018 Cal SB 1121 [CCPA].

⁶⁶ See Clarke & Wigan, "You are Where You've Been", *supra* note 22; *Personal Information Protection and Electronic Documents Act*, SC 2000, c5 [PIPEDA] at sch 1. section 4.5; Office of the Privacy Commissioner of Canada, "Personal Information Retention and Disposal: Principles and Best Practices" (17 June 2014) online: <https://www.priv.gc.ca/en/privacy-topics/safeguarding-personal-information/gd_rd_201406/>; EU, *Regulation of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC*, [2016] OJ, L 119/1 [GDPR] at art 17, recital 39; EU, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*, [2002] OJ, L 201/37 [ePrivacy Directive] at art 26, recital 39.

⁶⁷ See Shokri, Freudiger & Hubaux, *Unified Framework for Location Privacy*, *supra* note 59.

⁶⁸ See *Unified Framework for Location Privacy*, *supra* note 59.

⁶⁹ See Liu et al, "Location Privacy and Its Applications", *supra* note 59 at 17612.

⁷⁰ See Liu et al, "Location Privacy and Its Applications", *supra* note 59 at 17613.

Anonymization as an LPPM⁷¹ breaks the link between the identity of the individual and the location data using trusted third party providers.⁷² Two models of anonymity are “*k*-anonymity” and “mix zones.”

K-anonymity hides information among similar anonymous users,⁷³ while mix zones are unregistered geographic regions where users’ identities are mixed.⁷⁴ One of the recognized limitations of these mechanisms is that the movement patterns are unique to an individual,⁷⁵ allowing potential re-identification from an anonymized dataset,⁷⁶ predicting an individual’s location at a given time or day,⁷⁷ and identifying the location of someone’s home, work,⁷⁸ or

⁷¹ For a comparison between anonymity from a legal and computer science perspective see Mascetti et al, “Anonymity”, *supra* note 62.

⁷² See Liu et al, “Location Privacy and Its Applications”, *supra* note 59 at 17612; Seda Gürses & Bettina Berendt, “PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm” in Serge Gutwirth, Yves Poullet & Paul De Hert, eds, *Data Protection in a Profiled World* (Dordrecht: Springer, 2010) 301 at 309; Cuellar, “Location Information Privacy”, *supra* note 31; Karen P Tang et al, “Putting People in Their Place: An Anonymous and Privacy-Sensitive Approach to Collecting Sensed Data in Location-Based Applications”(Paper delivered at the SIGCHI conference on Human Factors in Computing Systems, Montreal, QC, April 22-27, 2006) in Rebecca Grinter, Thomas Rodden & Paul Aoki, eds, *CHI’ 06* (New York: ACM, 2006) 93, DOI:<10.1145/1124772.1124788>.

⁷³ See Liu et al, “Location Privacy and Its Applications”, *supra* note 59 at 17612.

⁷⁴ See Alastair R Beresford & Frank Stajano, “Mix Zones: User Privacy in Location-Aware Services”(Paper delivered at the IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, FL, March 14-17, 2004) in Bob Werner, ed, *Proceedings PerCom 2004* (California: IEEE, 2004) 127, DOI:<10.1109/PERCOMW.2004.1276918> at 128.

⁷⁵ See de Montjoye et al, “Unique in the Crowd”, *supra* note 26; Luca Rossi, James Walker & Mirco Musolesi, “Spatio-Temporal Techniques for User Identification by Means of GPS Mobility Data” (2015) 4 EPJ Data Science 11.

⁷⁶ See e.g., Chris YT Ma et al, “Privacy Vulnerability of Published Anonymous Mobility Traces”(Paper delivered at the 16th Annual International Conference on Mobile Computing and Networking, Chicago, September 20-24, 2010) in Nitin Vaidya, Suman Banerjee & Dina Katabi, eds, *MobiCom’ 10* (New York: ACM, 2010) 185, DOI:<10.1145/1859995.1860017>; Rossi, Walker & Musolesi, “User Identification by GPS Mobility Data”, *supra* note 75.

⁷⁷ See e.g., Chaoming Song et al, “Limits of Predictability in Human Mobility” (2010) 327 Science 1018 at 1021; Galini Tsoukaneri et al, “On the Inference of User Paths from Anonymized Mobility Data”(Paper delivered at the 1st IEEE European Symposium on Security and Privacy, Saarbrücken, Germany, March 21-24, 2006) in Lisa O’Conner, ed, *Proceedings Euro S&P 2016* (California: IEEE, 2016) 199, DOI:<10.1109/EuroSP.2016.25>.

⁷⁸ See e.g., Philippe Golle & Kurt Partridge, “On the Anonymity of Home/Work Location Pairs”(Paper delivered at the 7th International Conference on Pervasive Computing, Nara, Japan, May 11-14, 2009) in Hideyuki Tokuda et al, eds, *Pervasive Computing* (Verlag: Springer, 2009) 390, DOI:<10.1007/978-3-642-01516-8_26>; John Krumm, “Inference Attacks on Location Tracks”(Paper delivered at the 5th International Conference on Pervasive

frequently visited places.⁷⁹ For example, studies have shown that it is possible to identify individuals from anonymized mobile phone records using minimal spatio-temporal points.⁸⁰

(c) Privacy by Design (PbD)

Other authors have emphasized the importance of implementing privacy measures from the outset, even before the data are generated.⁸¹ This idea of engineering privacy is represented by the concept of Privacy by design (PbD).⁸² This literature emphasizes the importance of incorporating privacy—understood as personal control and choice—from the design stage of

Computing, Toronto, May 13-16) in Anthony LaMarca, Marc Langheinrich & Khai N. Truong, eds, *Pervasive Computing* (Berlin: Springer, 2007) 127, DOI:<10.1007/978-3-540-72037-9_8>.

⁷⁹ See e.g., Ionut Trestian et al, “Measuring Serendipity: Connecting People, Locations and Interests in a Mobile 3G Network”(Paper delivered at the 9th ACM SIGCOMM Conference on Internet Measurement, Chicago, November 4-6, 2009) in Anja Feldmann & Laurent Mathy, eds, *IMC’ 09* (New York: ACM, 2009) 267, DOI:<10.1145/1644893.1644926>.

⁸⁰ See de Montjoye et al, “Unique in the Crowd”, *supra* note 26; Romain Pialat, “GeoTrouveTous: Projet de Réidentification par Géolocalisation” (14 July 2023) online: <linc.cnil.fr> [<http://web.archive.org/web/20231221124813/https://linc.cnil.fr/geotrouvetous-projet-de-reidentification-par-geolocalisation>].

See also Yi Song, Daniel Dahlmeier & Stephane Bressan, “Not So Unique in the Crowd: A Simple and Effective Algorithm for Anonymizing Location Data” (Paper delivered at the PIR@SIGIR, Gold Coast, Australia, 11 July 2014) [unpublished] online: <<https://dblp.org/rec/conf/sigir/SongDB14.html>> (proposing a modification-based anonymization approach to reduce the risk of re-identification. The empirical results showed that there was a decrease of uniqueness in the mobility dataset. However, they concluded that anonymized data couldn’t provide full anonymity so far).

⁸¹ See Information and Privacy Commissioner Ontario, *Privacy by Design: From Rhetoric to Reality* (Toronto: IPC-ON, 2014) online: <ipc.on.ca> [<http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>] at i–ii.

See also Mehrnaz Ataei, Auriol Degbelo & Christian Kray, “Privacy Theory in Practice: Designing a User Interface for Managing Location Privacy on Mobile Devices” (2018) 12:3–4 *Journal of Location Based Services* 141; Katie Shilton, “‘That’s Not An Architecture Problem!’: Techniques and Challenges for Practicing Anticipatory Technology Ethics” (Paper delivered at the iConference 2015, New Port Beach, California, 24 March 2015) [unpublished] online: <<https://hdl.handle.net/2142/73672>> .

⁸² The concept of privacy-by-design was recognized as an essential component of fundamental privacy protection at the International Conference of Data Protection and Privacy Commissioners, and its importance was later reaffirmed by the Privacy Commissioner in Canada see 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (Jerusalem: 2010).

See also Office of the Privacy Commissioner of Canada, *2019-20 Departmental Plan* (Ottawa: OPC, 2019). (“Canada should simultaneously pursue privacy and innovation, and Privacy by Design is an excellent way to achieve both.”)

technology.⁸³ It recognizes that it is not enough to rely on policy and regulation; privacy must be built into the technology itself.⁸⁴ Devices, applications, infrastructure, and business practices need to be designed so that personal control, transparency, data collection limits, and data minimization can be easily exercised throughout the data lifecycle.⁸⁵ PbD solutions range from giving individuals more control over their data to reducing the impact of the data collected.⁸⁶

This thesis agrees with the literature on PbD in that policy and regulation alone are not sufficient and that it is important that devices and services are designed with privacy in mind. However, it differs from this literature in that it seeks regulatory solutions that go beyond the current approach, such as fair information practices, on which PbD is based.

PbD assumes that data are generated, and should be generated.⁸⁷ Therefore, control and transparency are seen as key components for privacy protection. This thesis recognizes the important role that control and transparency play in protecting privacy, they are basic conditions

⁸³ See e.g., Information and Privacy Commissioner of Ontario, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, by Ann Cavoukian & Marilyn Prosch, (Toronto: IPC-ON, 2010); Information and Privacy Commissioner Ontario, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers.*, by Ann Cavoukian, (Toronto: IPC-ON, 2014) online: <ipc.on.ca> [<http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>].

⁸⁴ See e.g., Cavoukian & Prosch, *Roadmap for PbD*, *supra* note 83 at 114–15. See also Michael Veale, Reuben Binns & Jef Ausloos, “When Data Protection by Design and Data Subject Rights Clash” (2018) 8:2 International Data Privacy Law 105 (Explaining how the PETs literature concept of privacy-as-confidentiality, can be in tension with the privacy-as-control defended by the Fair Information Principles and the GDPR).

⁸⁵ See e.g., Cavoukian & Prosch, *Roadmap for PbD*, *supra* note 83; Cavoukian, *PbD in Law, Policy, and Practice*, *supra* note 83.

⁸⁶ See e.g., Information and Privacy Commissioner Ontario, *Privacy and Radical Pragmatism: Change the Paradigm*, by Ann Cavoukian, (white paper) (Toronto: IPC-ON, 2008) at 15–22; Cavoukian & Prosch, *Roadmap for PbD*, *supra* note 83.

⁸⁷ Privacy-by-design is based on the same assumptions that data protection regulation. See Chapter V-I.A, *below*, for more on this topic.

for protecting privacy, but they are not enough in a socio-technical context where corporations set the rules for the design of technologies and where they also define the meaning of privacy.⁸⁸

B. Specific Critiques of Data Protection Regulation

This subsection summarizes the second group of relevant literature: criticisms of data protection legislation as an adequate solution to address privacy issues. This literature can be divided into two main areas of concern: challenges regarding the application of data protection regulations to location data, and the broader adequacy and limitations of these regulations in addressing privacy concerns.

1) Location Data and Data Protection Regulations

The first set of criticisms highlights several challenges associated with the application of data protection regulations to location data. Key issues include the lack of clarity of whether location data constitutes personal information,⁸⁹ the difficulty of determining the sensitivity of such data,⁹⁰ and the challenge of distinguishing between actual and inferred information.⁹¹

⁸⁸ This point is further developed in Chapters IV and V, *below*.

⁸⁹ See e.g., Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39 at 36–38; Geoffrey White, *Off the Grid: Pinpointing Location-Based Technologies and the Law*, (Ottawa: PIAC, 2015) online: <piac.ca> [<http://web.archive.org/web/20231219145416/https://www.piac.ca/research-reports/do-the-watchers-need-more-watching-new-report-asks/>]; Teresa Scassa et al, “Consumer Privacy and Radio Frequency Identification Technology” (2006) 37:2 *Ottawa Law Review* 215; Roba Abbas et al, “Sketching and Validating the Location-Based Services (LBS) Regulatory Framework in Australia” (2013) 29 *Computer Law & Security Review* 576; Future of Identity in the Information Society (No. 507512), *The Legal Framework for Location-Based Services in Europe* (2007) online: <fidis.net> [<https://web.archive.org/web/20231218160143/http://www.fidis.net/resources/fidis-deliverables/mobility-and-identity/d115-the-legal-framework-for-location-based-services-in-europe/doc/9/>].

⁹⁰ See Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39 at 36–38; Abbas et al, “Sketching and Validating LBS”, *supra* note 89 at 585; Future of Identity in the Information Society (No. 507512), *Legal Framework LBS in Europe*, *supra* note 89.

⁹¹ See Teresa Scassa, “Geographical Information as ‘Personal Information’” (2010) 10:2 *Oxford University Commonwealth Law Journal* 185 at 214.

Proposed solutions to these challenges include setting specific guidelines for when location data should be considered personal information,⁹² clarifying what types of inferences should raise data protection concerns,⁹³ and explicitly including location data in the definition of personal information.⁹⁴ This last solution is consistent with the EU's approach in the General Data Protection Regulation (GDPR),⁹⁵ where one of the changes (and improvements) made by the European regulator when replacing the Data Protection Directive with the GDPR, was to include location data in the definition of "personal data".⁹⁶ This inclusion addresses some of the ambiguities that existed prior to the GDPR regarding the status of location data.⁹⁷

Another important criticism identified is the fragmentation of the regulation, particularly in the European context, where both the GDPR (or the previous Data Protection Directive) and the ePrivacy Directive apply to location data. Some authors argue that this dual regime creates confusion and disadvantages for consumers and providers of location-based services (LBS).⁹⁸ In 2019, the European Data Protection Board (EDPB) clarified the interaction between these

⁹² See White, *Off the Grid*, *supra* note 89 at 97.

⁹³ See Scassa, "Geographical Information", *supra* note 91 at 214.

⁹⁴ See White, *Off the Grid*, *supra* note 89 at 97; Abbas et al, "Sketching and Validating LBS", *supra* note 89.

⁹⁵ See *GDPR*, *supra* note 66 at art 4 ("an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as . . . location data.").

This was also the case with the California regulation in the United States See *CCPA*, *supra* note 65 at section 1798.140.(o.1.G) (The definition of personal information includes geolocation data.).

⁹⁶ See *GDPR*, *supra* note 66 at art 4(1).

The modernization efforts that led to the replacement of Directive 95/46/EC with the GDPR are explained in detail in Chapter V-I.A.2, *below*.

⁹⁷ See e.g., Future of Identity in the Information Society (No. 507512), *Legal Framework LBS in Europe*, *supra* note 89.

⁹⁸ See e.g., Colette Cuijpers & Bert-Jaap Koops, "How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services" (2008) 33 *European Law Review* 880; Future of Identity in the Information Society (No. 507512), *Legal Framework LBS in Europe*, *supra* note 89; B van Loenen & J A Zevenbergen, "The Impact of the European Privacy Regime on Location Technology Development" (2007) 1:3 *Journal of Location Based Services* 165.

frameworks, stating that ePrivacy should be understood as the *lex specialis* for the processing of location data in electronic communications, while ensuring that GDPR rights—such as access to information—remain enforceable.⁹⁹

2) Data Protection Regulation and Privacy Issues

The second group of critiques assesses the broader adequacy of data protection regulations in addressing privacy concerns, with particular attention to the limitations of relying on consent and gaps in protecting against systemic privacy risks such as social sorting and discrimination. The following sections focus on the limitations associated with Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) and the GDPR, as these regulations are used to illustrate the data protection framework for the analysis in subsequent chapters.¹⁰⁰

A commonly cited limitation of data protection regulations, such as PIPEDA and GDPR, is their reliance on consent as the primary mechanism for individuals to protect their privacy by exercising control over their data.¹⁰¹ Critics argue that consent is often ineffective because individuals typically lack comprehensive information about how their data will be used and disclosed, face cognitive limitations in assessing the implications of giving consent, and frequently encounter situations where consent is not a meaningful choice.¹⁰² For instance, certain services,

⁹⁹ See generally EDPB, *Opinion 5/2019 on the Interplay Between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities* (2019) at paras 13–16.

¹⁰⁰ These regulations will be further analyzed in Chapter V-I, *below*.

¹⁰¹ For a framework of the different kinds of defects that a consent model can have, see Neil Richards & Woodrow Hartzog, “The Pathologies of Digital Consent” (2019) 96 Washington University Law Review 1461 (they identify three types of problematic consent: unwitting, coerced, and incapacitated).

¹⁰² See e.g., Lyon, Marmura & Peroff, *Location Technologies*, *supra* note 30; Daniel J Solove, “Introduction: Privacy Self-Management and the Consent Dilemma” (2013) 126 Harvard Law Review 1880; Teresa Scassa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 Canadian Journal of Law and Technology 99; Cottrill & “Vonu” Thakuriah, “Location privacy preferences”, *supra* note 49; Alessandro Acquisti & Jens Grossklags, “What Can Behavioral Economics Teach Us About Privacy?” in Alessandro Acquisti et al, eds, *Digital Privacy: Theory, Technologies, and Practices* (New York: Auerbach Publications, 2007) 363.

such as car rental, may require constant location tracking as a condition of use,¹⁰³ while other services, such as location-based applications, will become unusable when location is turned off.¹⁰⁴ In other cases, it is not possible to ask for consent because there is no direct interaction with the organization collecting the data (e.g., third-party data collection in apps, and CCTV surveillance).¹⁰⁵

In a world of ubiquitous computing, it is also impractical to require consent for every instance of data collection.¹⁰⁶ The time and effort required to read the privacy policy of every company with which one interacts would be overwhelming.¹⁰⁷ Some authors argue that although consent has inherent limitations, it cannot be completely abandoned because it promotes autonomy and individual empowerment.¹⁰⁸ Some of these authors suggest improving consent mechanisms

See also Lisa M Austin, “Enough About Me: Why Privacy is About Power, not Consent (or Harm)” in Austin Sarat, ed, *A World without Privacy: What Law Can and Should Do?* (Cambridge: Cambridge University Press, 2014) 131. (She argues that in the face of surveillance as a business model, and in the context of governments' lawful access to data generated and stored by companies, consent to data protection rules provides an illusory protection).

¹⁰³ See Michael R Curry, David J Phillips & Priscilla M Regan, “Emergency Response Systems and the Creeping Legibility of People and Places” (2004) 20:5 *Information Society* 357; Lyon, Marmura & Peroff, *Location Technologies*, *supra* note 30; Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39.

¹⁰⁴ See Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39.

In some of these cases, it is also important to consider liability issues where individuals are able to control when the location is turned on, for example in the case of 9-1-1 services. See e.g., Office of the Privacy Commissioner of Canada, *Surveillance of Mobility*, *supra* note 39.

¹⁰⁵ See Katherine J Strandburg, “Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context” in Julia Lane, Victoria Stodden & Helen Nissenbaum, eds, *Big Data, and the Public Good: Frameworks for Engagement* (Cambridge, UK: Cambridge University Press, 2014) 5 at 85.

¹⁰⁶ See e.g., David J Phillips, “Ubiquitous Computing, Spatiality, and the Construction of Identity: Directions for Policy Response” in Ian Kerr, Valerie M Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* (New York: Oxford University Press, 2009) 303; Teresa Scassa, “A Human Rights-Based Approach to Data Protection in Canada” in Elizabeth Dubois & Florian Martin-Bariteau, eds, *Citizenship in a Connected Canada: A Policy and Research Agenda* (Ottawa: University of Ottawa Press, 2020) 173 at 175.

¹⁰⁷ See e.g., Aleecia M McDonald & Lorrie Faith Cranor, “The Cost of Reading Privacy Policies” (2008) 4:3 *I/S:A Journal of Law and Policy for the Information Society* 540; Tony Vila, Rachel Greenstadt & David Molnar, “Why We Can’t Be Bothered to Read Privacy Policies” in Stephen Lewis & L Jean Camp, eds, *Economics of Information Security* (New York: Kluwer Academic Publishers, 2004) 143.

¹⁰⁸ See e.g., Solove, “Consent Dilemma”, *supra* note 102 (He argues that it is important to keep consent at the core of the privacy protection, but establishing more substantive rules, rethinking the moment when consent is required,

through better education, more transparent communication, and better tools to manage the control individuals have over their data.¹⁰⁹

Beyond issues of consent, critics also emphasize that data protection regulations are ill-equipped to address collective privacy risks, such as social sorting and algorithmic discrimination.¹¹⁰ Traditional data protection regimes focus on an individualized conception of privacy that neglects the broader privacy and equality implications of technological advances such as algorithmically created groups.¹¹¹ For instance, PIPEDA's exemption for aggregated and anonymized data leaves systemic risks, such as discriminatory profiling, unaddressed.¹¹² The same limitation has been identified by some authors in the European context prior to the GDPR.¹¹³

The GDPR introduces some measures to mitigate these risks.¹¹⁴ Article 22 introduces additional safeguards when data are used for automated decision-making and profiling, and grant

and exploring libertarian paternalism approaches); Omer Tene, "Privacy Law's Midlife Crisis: A critical Assessment of the Second Wave of Global Privacy Laws" (2013) 74:6 Ohio State Law Journal 1217 (For him consent should not be removed from the framework because it might become paternalistic and overly rigid. However, based on a cost-benefit analysis, policymakers should make a decision in what situations [or uses] should not consent be required and in which ones it should); Office of the Privacy Commissioner of Canada, *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (Ottawa: OPC, 2017) (Highlights the importance of consent in the development of autonomy, and as such OPC argues that it is important to maintain consent as part of the privacy protection scheme).

¹⁰⁹ See Office of the Privacy Commissioner of Canada, *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act*, by Policy and Research Group, (Ottawa: OPC, 2016) online: <priv.gc.ca> [http://web.archive.org/web/20231219165225/https://www.priv.gc.ca/media/1806/consent_201605_e.pdf]. (Some of the alternatives to consent explained in the report are enhancing consent by improving privacy policies presentation, tagging data with privacy preferences, technology-specific safeguards, and incorporating privacy by design)

¹¹⁰ See e.g., Kammourieh et al, "Group Privacy in the Age of Big Data", *supra* note 58 at 56–57.

¹¹¹ See e.g., *Submissions on Bill C-27*, *supra* note 58.

¹¹² See White, *Off the Grid*, *supra* note 89; Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39; Phillips, "Ubiquitous Computing, Spatiality, and the Construction of Identity", *supra* note 106; Lyon, Marmura & Peroff, *Location Technologies*, *supra* note 30 at 40; Eloïse Gratton, "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising" (2002) 1:3 Canadian Journal of Law and Technology 59.

¹¹³ See e.g., Mireille Hildebrandt, "Profiling: From Data to Knowledge. The Challenges of a Crucial Technology" (2006) 30:9 *Datenschutz und Datensicherheit* 548 at 550; Mireille Hildebrandt, "A Vision of Ambient Law" in Roger Brownsword & Karen Yeung, eds, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (London: Hart Publishing, 2008) 175.

¹¹⁴ There are various provisions in the GDPR that aim "to ensure that profiling and automated individual decision-

individuals certain rights in these cases,¹¹⁵ while Article 9 extends protection to sensitive data categories created by inference.¹¹⁶ This is important in the case of location data, as it could potentially reduce some of the privacy risks created by the possibility of making inferences based on location and movement patterns alone. However, the practical effectiveness of these two provisions remains uncertain, and some of their limitations have already been identified in the literature.¹¹⁷

This thesis agrees with these criticisms, but differs in its proposed solutions. For instance, while many Canadian proposals focus on refining the current regulatory framework—such as improving consent requirements,¹¹⁸ adopting stricter interpretations of PIPEDA’s “appropriate purpose” and “specific purpose” provisions,¹¹⁹ and strengthening the Office of the Privacy Commissioner’s (OPC) enforcement powers¹²⁰—this thesis argues that such adjustments remain

making is not used in ways that have an unjustified impact on individuals’ rights.” WP29, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01 (2018) at 6.

¹¹⁵ *GDPR*, *supra* note 66 at art 22(3) (“the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.”).

¹¹⁶ In this context, the Article 29 Data Protection Working Party (WP29), an independent European Union advisory body on data protection and privacy, acknowledges that profiling “can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data.” WP29, *Automated Decision-Making and Profiling*, *supra* note 114 at 15.

¹¹⁷ For limits of Article 22 see Sandra Wachter, “Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR” (2018) 34 *Computer Law & Security Review* 436; Tal Z Zarsky, “Incompatible: The GDPR in the Age of Big Data” (2017) 47 *Seton Hall Law Review* 995 at 1015–18; Sandra Wachter, Brent Mittelstadt & Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation” (2017) 7:2 *International Data Privacy Law* 76.

For limits of Article 9, see Zarsky, “GDPR in the Age of Big Data”, *supra* note at 1012–15; Lokke Moerel & Corien Prins, “Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things” (2016), online: <papers.ssrn.com> [http://web.archive.org/web/20231222125842/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123] at 11; Lokke Moerel, “GDPR Conundrums: Processing Special Categories of Data” (12 September 2016) online (blog): <iapp.org> [http://web.archive.org/web/20231221153045/https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/].

¹¹⁸ See Scassa & Sattler, “Location-Based Services and Privacy”, *supra* note 102 at 99; Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39.

¹¹⁹ See White, *Off the Grid*, *supra* note 89 at 97.

¹²⁰ See Scassa & Sattler, “Location-Based Services and Privacy”, *supra* note 102 at 99.

insufficient. The characteristics of the current socio-technical landscape, in particular the pervasive dataveillance capabilities of corporations, require a fundamental rethinking of the regulatory framework. Rather than incremental adjustments, there is an urgent need for a legal framework that directly constrains the mass dataveillance systems of corporations and the ecosystems in which they operate. Moreover, this thesis argues that data protection frameworks are inherently flawed in addressing corporate dataveillance because they are based on outdated assumptions about the technological capabilities and personalities of the organizations they seek to regulate.

This part reviewed the existing literature on the intersection of digital technologies, privacy and data protection, with a particular focus on location technologies as concrete examples of the current socio-technical landscape. The following part outlines the law, technology, and society methodology used in this thesis.

II. Law, Technology, and Society

Law and Society scholars understand law as a product of various external influences, as opposed to a closed system with an internal logic.¹²¹ Accordingly, Law and Society scholarship seeks to better understand the social, cultural, political, and economic contexts in which law operates in practice.¹²² Its primary aim is to minimize the gap between “law on the books” and “law in action,” by focussing on how law functions in real-world settings between and among “people, places, histories, and institutions.”¹²³ This approach emphasizes the study of the

¹²¹ See Lynn Mather, “Law and Society” in Robert E Goodin, ed, *The Oxford Handbook of Political Science* (Oxford: Oxford University Press, 2011) 289; The Bridge, “Legal Theory: Law and Society” (last visited 24 February 2017) online: <cyber.harvard.edu> [http://web.archive.org/web/20231221122349/https://cyber.harvard.edu/bridge/LawSociety/essay1.htm].

¹²² See Eve Darian-Smith, *Laws and Societies in Global Contexts: Contemporary Approaches*, (New York: Cambridge University Press, 2013) at 2; The Bridge, “Law and Society”, *supra* note 121; Paul Schiff Berman, ed, *Law and Society Approaches to Cyberspace*, (Hampshire, UK: Ashgate, 2007) at xi.

¹²³ Darian-Smith, *Law and Societies*, *supra* note 122 at 2.

institutional structures, behaviours, people, culture, and meanings that influence how laws are applied in everyday life.¹²⁴

A key characteristic of this scholarship is its expansive understanding of law, seeing it not only in the formal legal sphere but also in social, cultural, economic, linguistic, and ideological spheres.¹²⁵ Because of this broad understanding of the law, Lynn Mather argues, scholars in the field are confronted with the “messy question of how to say anything interesting or disciplined at all if in fact ‘the law is all over.’”¹²⁶ Although scholars do not agree on a single answer, most of them approach their research by identifying specific questions about the creation, maintenance, or development of law, and pursuing answers wherever the inquiry leads. Mather emphasizes the importance of self-awareness in defining the scope of the inquiry and drawing on concepts, methods, or insights from other disciplines.¹²⁷

Another characteristic of this scholarship is that while most Law and Society scholars have been trained in one or another established discipline, they frequently borrow from other disciplines in their research, making this scholarship typically multidisciplinary or interdisciplinary. For this reason, contemporary scholarship in this field, “encompasses a wide range of epistemological perspectives, from the cultural studies approach of law and humanities to empirical legal studies—and everything in between.”¹²⁸ Additionally, this scholarship tends to focus on theory and substantive results, rather than on the “sophistication of the methods or an insistence on the

¹²⁴ See Berman, *Law and Society Cyberspace*, *supra* note 122 at xi.

¹²⁵ See Mather, “Law and Society”, *supra* note 121 at 292.

¹²⁶ Mather, “Law and Society”, *supra* note 121.

¹²⁷ See Mather, “Law and Society”, *supra* note 121.

¹²⁸ Mather, “Law and Society”, *supra* note 121 at 291.

superiority of any particular method.”¹²⁹ For this reason, it has “a ‘big tent’ approach to the issue of methodology.”¹³⁰

This multidisciplinary approach and broad methodological acceptance have enabled Law and Society scholars to explore different areas of research, including regulation.¹³¹ In this area, scholars argue that in order to find the best way to regulate certain issues within a given society, it is necessary to understand not only the production or shaping of law, but also the interaction between law and various parts of society. This thesis focusses specifically on the regulation of technology and corporations as integral parts of society.

A. Law, Regulation, and Technology

Scholars from different disciplines emphasize the importance of understanding and studying technology not as an external or isolated element of society but as an intrinsic part of it.¹³² Science and Technology Studies (STS) scholars, for example, argue that the relationship between technology and society is not black and white, but that technology is both shaped and shaper in society.¹³³ Bijker explains that this scholarship, “starts from the position that social and technical

¹²⁹ Mather, “Law and Society”, *supra* note 121.

¹³⁰ Berman, *Law and Society Cyberspace*, *supra* note 122 at xi.

¹³¹ See e.g., Mather, “Law and Society”, *supra* note 121 at 291.

¹³² See e.g., Wiebe E Bijker & John Law, eds, *Shaping Technology: Building Society: Studies in Sociotechnical Change*, (Cambridge, MA: MIT Press, 1992) at 11; Winner, *The Whale and the Reactor*, *supra* note 7 at 11.

See also Kieran Tranter, “The Law and Technology Enterprise: Uncovering the Template to Legal Scholarship on Technology” (2011) 3:1 Law, Innovation and Technology 31 at 73.

¹³³ In the field of interaction of technology with society, there are another two main theoretical approaches: technological determinist and social constructivism see e.g., Günter Ropohl, “A Critic of Technological Determinism” in Paul T Durbin & Friedrich Rapp, eds, *Philosophy and Technology* (Dordrecht: Reidel, 1983) 83 at 86; Thomas P Hughes, “Technological Momentum” in Merritt Roe Smith & Leo Marx, eds, *Does Technology Drives History? The Dilemma of Technological Determinism* (Cambridge, Mass: MIT Press, 1994) 101 at 106; Arthur Cookfield & Jason Pridmore, “A Synthetic Theory of Law and Technology” (2007) 8:2 Minnesota Journal of Law, Science & Technology 475.

change come together, as a package, and if we want to understand either, then we really have to understand both.”¹³⁴

Under this concept, technologies are tools that individuals use every day that allow them to do certain things (e.g., communicate, move from one point to another, and look for information), but they are not neutral, as they also establish a certain way of living.¹³⁵ They shape people’s conduct at home and work. They affect the health of individuals, the way they consume and interact, and the methods by which they exercise control over one another.¹³⁶

Technologies are designed to solve specific problems or fulfil specific societal goals.¹³⁷ These problems, and whether they are linked to a societal objective, depend on various factors such as legal, political, and economic context (e.g., the existence of incentives, subsidies or other mechanisms that favour certain types of design and technology over others)¹³⁸ and the motivations and objectives of the individuals or organizations responsible for their development.¹³⁹ In the case of corporations responsible for development, marketing, and implementation of some digital technologies their primary interest is likely to be driven by profit rather than the social good.¹⁴⁰

¹³⁴ Wiebe E Bijker & John Law, “General Introduction” in Wiebe E Bijker & John Law, eds, *Shaping Technology/Building Society: Studies in Sociotechnical Change* (Cambridge, Mass.: MIT Press, 1992) 1 at 11.

¹³⁵ In this regard see Winner, *The Whale and the Reactor*, *supra* note 7 at 11 (We do indeed “use” telephones, automobiles, electric lights, and computers in the conventional sense of picking them up and putting them down. But our world soon becomes one in which telephony, automobility, electric lighting, and computing are forms of life in the most powerful sense: life would scarcely be thinkable without them).

¹³⁶ See Bijker & Law, “General Introduction”, *supra* note 134 at 11.

¹³⁷ In this regard, Thomas Parke Hughes explains, “the problems have to do mostly with reordering the physical world in ways considered useful or desirable, at least by those designing or employing a technological system.” Thomas Parke Hughes, “The Evolution of Large Technological Systems” in Wiebe E Bijker, Thomas P Hughes & Trevor Pinch, eds, *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, Mass.: MIT Press, 2012) 45 at 47.

¹³⁸ See e.g., Winner, *The Whale and the Reactor*, *supra* note 7 at ch 4.

¹³⁹ See e.g., Hughes, “Evolution of Large Technological Systems”, *supra* note 137.

¹⁴⁰ This topic will be further developed in Chapter IV, *below*,

An important element in the relationship between technology and society is that, once introduced, technologies can become entrenched in the lives of individuals. After technologies are designed and manufactured, they are introduced to society, where people start buying and using them. Some of these technologies will begin to fulfil certain tasks in their daily lives, and there will come a time when these are so entrenched in society that life without them will become inconceivable.¹⁴¹

In the field of law and technology, scholars such as Kieran Tranter argue that there has been a shift in the way scholars have approached these issues in recent years, moving from a focus on a particular technology that created siloed scholarship to a broad understanding of the relationship between law and technology.¹⁴² This emerging field of “law, technology, and society” draws on the theory and methodology of other social disciplines to provide an understanding of how rules and regulatory models operate at the interface of law and technology.¹⁴³

Building on this interdisciplinary approach, scholars in this field draw on various disciplines, such as regulatory theory and technology studies, to gain a better “understanding of the relationship between law, technology, and culture/society, in order not only to better understand how to regulate technology but also to conceive of technology as regulation.”¹⁴⁴ This broad perspective recognizes the complex interplay between legal frameworks, technological

¹⁴¹ Hughes calls this *momentum*. He explains that as the system becomes larger and more complex, thereby gathering momentum, the system becomes “less shaped by and more the shaper of its environment.” Hughes, “Technological Momentum”, *supra* note 133 at 108. See also Winner, *The Whale and the Reactor*, *supra* note 7.

¹⁴² This is what Tranter calls the “law and technology enterprise” scholarship. Tranter, “Law and Technology Enterprise”, *supra* note 132.

¹⁴³ See Tranter, “Law and Technology Enterprise”, *supra* note 132 at 71. See also Michael Anthony C Dizon, “From Regulating Technologies to Governing Society: Towards a Plural, Social and Interactive Conception of Law” in Heather M Morgan & Ruth Morris, eds, *Moving Forward: Tradition and Transformation* (Newcastle upon Tyne, UK: Cambridge Scholars Publishing, 2012) 115.

¹⁴⁴ Kieran Tranter, “The Laws of Technology and the Technology of Law” (2011) 20:4 Griffith Law Review 753 at 755–56.

advances, and societal dynamics. Recognizing the evolving nature of the field, scholars such as Roger Brownsword, Eloise Scotford, and Karen Yeung have described the field of law, regulation, and technology as an emerging “work-in-progress” that combines the “dynamic activity in the ‘world-to-be-regulated’” and the “technological innovation that puts pressure on traditional legal concepts and transforms the instruments and institutions of the regulatory enterprise itself.”¹⁴⁵

Within this evolving field, scholars have identified two distinct categories of regulation. The first category focusses on technology as a regulator, where scholars have focussed on the use of technology as a regulatory tool, exploring how the design of particular technologies affects moral choices, and questions of the rule of law versus the rule of technology and state responsibility.¹⁴⁶ Bert-Jaap Koops, for instance, argues that it is important to distinguish between technology and technology that is deliberately used as a tool to influence people’s behaviour (normative technology). He recognizes that technology in itself has a regulatory effect on people, limiting and expanding the scope of their behaviour,¹⁴⁷ and that there are cases where technology is used as a substitute for law as a regulatory instrument.¹⁴⁸ This is the idea of “code as law” proposed by Lessig.¹⁴⁹

The second category focusses on the regulation of the technology, which is the main focus of this thesis. Scholars such as Lyria Bennett Moses, Art Cockfield, Roger Brownsword, and

¹⁴⁵ Roger Brownsword, Eloise Scotford & Karen Yeung, “Law, Regulation, and Technology: The Field, Frame, and Focal Questions” in Roger Brownsword, Eloise Scotford & Karen Yeung, eds, *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2016) at 3.

¹⁴⁶ See e.g., Roger Brownsword, “So What Does the World Need Now?: Reflections on Regulating Technologies.” in Roger Brownsword & Karen Yeung, eds, *Regulating Technologies : Legal Futures, Regulatory Frames and Technological Fixes* (London: Hart Publishing, 2008) 23; Lessig, *Code*, *supra* note 7.

¹⁴⁷ See Bert-Jaap Koops, “Criteria for Normative Technology: The Acceptability of ‘Code as Law’ in Light of Democratic and Constitutional Values” in Roger Brownsword & Karen Yeung, eds, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (London: Hart Publishing, 2008) 157 at 158.

¹⁴⁸ See Koops, “Criteria for Normative Technology”, *supra* note 147 at 159.

¹⁴⁹ The other three regulators identified by Lessig are norms, law, and market see Lessig, *Code*, *supra* note 7.

Kieran Tranter have pursued the development of a general theory of law and technology by “seeing connections across technologies and across time.”¹⁵⁰ This approach encompasses questions of risks and harms that arise in specific technological contexts, and appropriate regulatory responses to manage such risks and harms.

Building on these foundations, one of the analytical lenses through which the effectiveness of a regulatory framework can be examined is to focus on the challenges, “for law and regulation in an evolving socio-technical landscape.”¹⁵¹ This perspective argues that focussing solely on how to regulate technology narrow policymakers’ and researchers’ understanding and analysis of technology regulation. Instead, it emphasizes the importance of adapting laws and regulations to socio-technical change,¹⁵² recognizing that it is not always the tools or processes themselves that changes over time.¹⁵³

This thesis adopts Bennett Moses’ analytical framework as a methodology for evaluating data protection regulation to address the risks and harms posed by the socio-technical changes brought about by corporate dataveillance capabilities. As the next subsection will explain, this framework provides a structured approach to understanding the evolving socio-technical landscape, assessing the alignment of existing regulations with contemporary technological realities, and identifying necessary adjustments or new regulatory measures.

¹⁵⁰ Tranter, “Laws of Technology and the Technology of Law”, *supra* note 144 at 756.

For different examples of this “new” approach see generally Griffith Law Review, volume 20, issue 4 (2011), Special Issue: The Laws of Technology and the Technology of Law.

¹⁵¹ Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18 at 10.

Brownsword refers to this as “the challenge of regulatory connection” see Roger Brownsword, *Rights, Regulation, and the Technological Revolution*, (New York: Oxford University Press, 2008) at ch 6.

¹⁵² See Lyria Bennett Moses, “Regulating in the Face of Sociotechnical Change” in Roger Brownsword, Eloise Scotford & Karen Yeung, eds, *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2016) 573 at 574.

¹⁵³ See Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18 at 10.

B. Analyzing the Adequacy of a Regulatory Framework

Bennett Moses noted that while the specific impact of technological change on the law may vary, some general patterns can be observed. The current state of technology determines the actions that corporations can take, the objects they can produce, and the relationships they can establish with their users and customers.¹⁵⁴ As a result, technological change often has an impact on the law, raising questions about the permissibility, prohibition, or encouragement of these developments under existing legal frameworks. These legal issues arise only when new technological capabilities become feasible and require consideration of how they should be treated under existing legal rules, or whether it is necessary to introduce new rules to address them effectively.¹⁵⁵

Through a detailed examination of the publications of Bennett Moses,¹⁵⁶ a methodology for assessing the adequacy of regulatory frameworks in the context of technological change emerges. This thesis adopts this methodology, which consists of four steps:

1. **Identify the current socio-technical landscape.** This step involves mapping the capabilities that digital technologies create for different actors in society, such as corporations, individuals, or governments. For this thesis, the focus will be on the dataveillance capabilities available to corporations, including their ability to systematically generate and process data about individuals and their behaviours, to target information, and to profile individuals and groups.¹⁵⁷

¹⁵⁴ See Lyria Bennett Moses, “Why Have a Theory of Law and Technological Change?” (2007) 8:2 *Minnesota Journal of Law, Science & Technology* 589 at 594.

¹⁵⁵ See Bennett Moses, “Why Have a Theory of Law & Tech Change?”, *supra* note 154.

¹⁵⁶ See Lyria Bennett Moses & Monika Zalnieriute, “Law and Technology in the Dimension of Time” in Sofia Ranchordás & Yaniv Roznai, eds, *Time, Law and Change: An Interdisciplinary Study* (Oxford: Hart Publishing, 2020) 303; Lyria Bennett Moses, “Recurring Dilemmas: The Law’s Race to Keep up with Technological Change” 2007:2 *University of Illinois Journal of Law, Technology & Policy* 239; Bennett Moses, “Why Have a Theory of Law & Tech Change?”, *supra* note 154; Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18; Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152.

¹⁵⁷ See Bennett Moses, “Why Have a Theory of Law & Tech Change?”, *supra* note 154 at 598; Bennett Moses, “Recurring Dilemmas”, *supra* note 156 at 245–46.

2. **Determine whether a regulatory response is warranted.** This involves assessing whether technological capabilities pose risks or harms to individuals or society that warrant regulatory intervention.¹⁵⁸
3. **Analyze the interaction between socio-technical change and existing regulation.** This step examines whether the existing regulations are in line with the realities and assumptions of the current socio-technical landscape.¹⁵⁹ In the case of this thesis, the applicable regulations analyzed are the GDPR and PIPEDA as examples of data protection regulations, which are the legal mechanism that the majority of states have chosen to regulate the processing of personal data by corporations.¹⁶⁰
4. **Propose a recommended regulatory response.** If there is a misalignment, this step involves recommending an appropriate regulatory response, whether through new legislation or changes to existing frameworks, and considering the appropriate regulatory target (i.e., artefacts, activities, or relationships).¹⁶¹

A key aspect of this analysis is a detailed understanding of the socio-technical landscape, which includes not only the technological capabilities that digital technologies create for corporations and the risks and harms that these create to individuals and society, but also the context in which corporations operate.¹⁶²

Corporations are central actors in the development, marketing, and implementation of data-driven technologies, and their motivations are an important factor to consider. For this reason, this thesis examines the corporations through the lens of Joel Bakan's theory of the psychopathic personality of corporations, which characterizes corporations as entities that prioritize profit at the

¹⁵⁸ See Bennett Moses, "Why Have a Theory of Law & Tech Change?", *supra* note 154 at 598; Bennett Moses, "Recurring Dilemmas", *supra* note 156 at 245–46.

¹⁵⁹ See Bennett Moses, "How to Think about Law, Regulation and Tech", *supra* note 18; Brownsword, "So What Does the World Need Now?", *supra* note 146 at 26–30; Brownsword, *Rights, Regulation, and the Technological Revolution*, *supra* note 151 at ch 6.

¹⁶⁰ See Chapter I.I States' Duty to Regulate Corporate Mass Dataveillance and Data Protection Regulations, *below*.

¹⁶¹ See Bennett Moses, "How to Think about Law, Regulation and Tech", *supra* note 18 at 17.

¹⁶² This corresponds to steps 1 and 2 of the methodology.

expense of other values, often to the detriment of individuals and society.¹⁶³ This characterization of corporations has sparked considerable debate and reflection on corporate behaviour and legal obligations.¹⁶⁴ The impact of Bakan's work extends beyond academic circles, as evidenced by the international recognition of his film.¹⁶⁵ This suggests that his ideas resonate with a wider audience. Nevertheless, to the best of my knowledge, this theory has not been applied to analyze the existing regulatory framework for data processing by corporations or to propose a new framework based on such an analysis.

Bakan's theory, based on his books *The Corporation* (2004) and *The New Corporation* (2020) and their accompanying documentaries,¹⁶⁶ critiques the inherent drive of corporations to maximize profits regardless of societal harm. While his early work was broadly critical of corporate behaviour, the relevance of his theory has only grown with the rise of data-driven corporations. In his second book and documentary, released in 2020 and 2022, Bakan addresses the power that these corporations have gained in society and the lives of individuals. He touches briefly on how these corporations use digital technologies to interfere with democracy and human agency through censorship, algorithms, and the control of information.¹⁶⁷ His main focus,

¹⁶³ Bakan's theory of the pathological personality of corporations will be developed in Chapter IV, *below*.

¹⁶⁴ See e.g., Aysegul Tunc, Esra Toplu & Selim Yazici, "Understanding the Behavioral Paradox of the Companies' by Using 'The Corporation' Documentary" (2017) 10:5 International Business Research 169; Michael Haynes, "Rationality, Morality and Joel Bakan's the Corporation" (2007) 3:1 International Journal of Business Governance and Ethics 1–18; Samuel F Mansell, *Capitalism, Corporations and the Social Contract: A Critique of Stakeholder Theory*, (Cambridge: Cambridge University Press, 2013) c 1.

¹⁶⁵ See e.g., Emma Bell, "The Corporation 10 Years On: An Interview and an Audience With Joel Bakan" (2016) 25:3 Journal of Management Inquiry 344.

¹⁶⁶ See Bakan, *The Corporation*, *supra* note 1; Joel Bakan, Mark Achbar & Jennifer Abbott, "The Corporation" (2003) online (Documentary): <thecorporation.com> [<http://web.archive.org/web/20230926133755/https://thecorporation.com/film/>]; Bakan, *New Corporation*, *supra* note 5; Joel Bakan & Jennifer Abbott, "The New Corporation: The Unfortunately Necessary Sequel" (2022) online (Documentary): <thenewcorporation.movie> [<http://web.archive.org/web/20230701111918/https://thenewcorporation.movie/about-the-film/>].

¹⁶⁷ See Bakan, *New Corporation*, *supra* note 5 c 5.

however, is on the challenges that these corporations have created to labour regulations, stripping workers of their rights,¹⁶⁸ and how these corporations present themselves, and their technologies, as solutions to global problems such as inequality, world hunger, water rights, and the issues facing underdeveloped countries.¹⁶⁹

This thesis will complement Bakan's insights into corporate behaviour with Ari Waldman's insights into corporate privacy practices in the information industry and Shoshana Zuboff's taxonomy of the data-based business models.¹⁷⁰ Together, these sources provide a solid foundation for assessing the pathological personality of corporations and its implications for regulatory frameworks.

By incorporating Bakan's theory, this thesis offers a fresh perspective on the analysis of data protection regulations. The framework challenges regulators to consider the pathological personality of corporations and their profit-driven strategies when designing regulatory responses. This perspective highlights the need to critically evaluate data protection regimes as the dominant approach to regulating corporate data processing activities.

To assess whether existing data protection regulations align with the realities and assumptions of the current socio-technical landscape, this thesis will analyze two jurisdictions.¹⁷¹ The European Union (EU) data protection framework will serve as the point of departure, due to its international significance in matters of privacy, surveillance, and data protection, as well as the active jurisprudential roles played by both the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). Particular attention will be given to the General

¹⁶⁸ See Bakan, *New Corporation*, *supra* note 5.

¹⁶⁹ See Bakan, *New Corporation*, *supra* note 5 at 116–17, 121.

¹⁷⁰ See Waldman, *Industry Unbound*, *supra* note 15; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, ebook ed (New York: Public Affairs, 2019).

¹⁷¹ See Chapter I.I States' Duty to Regulate Corporate Mass Dataveillance and Data Protection Regulations, *below*.

Data Protection Regulation (GDPR), as it represents the current data protection framework in force within the EU.

Subsequently, Canada will be examined as an example of a national framework, with a special focus on the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal data protection law. Canada presents an interesting case study because it has ratified the International Covenant on Civil and Political Rights (ICCPR) and maintains a data protection regime that has not undergone significant modernization in recent years. This is noteworthy given the active efforts of the Office of the Privacy Commissioner of Canada (OPC) and ongoing calls for legislative reform to ensure the adequate protection of privacy as a human right.

III. Conclusions

This chapter has provided an overview of the relevant literature and methodology that will guide the analysis in this thesis. The literature review highlighted several key themes. First, it emphasized the growing importance of data, particularly location data, in modern business models and technologies, where such data have become central to the operations and profitability of many corporations. Second, it examined the privacy concerns associated with location technologies, in particular their ability to allow organizations to build detailed movement profiles of individuals, which pose significant risks to personal autonomy and security. Third, it examined proposed solutions to these privacy issues, ranging from giving individuals greater control over their data to implementing technical measures to minimize privacy risks. Finally, it addressed criticism of existing data protection regulations, focussing on their heavy reliance on consent mechanisms and their shortcomings in addressing the systemic privacy risks inherent in data-driven economies.

The methodology section outlined the law, technology, and society approach that will frame the analysis of the thesis. Based on Bennett Moses' analytical framework, this methodology focusses on assessing the adequacy of regulatory responses to socio-technical change. This involves four key steps: (1) identifying the current socio-technical landscape, with a focus on companies' dataveillance capabilities; (2) determining whether regulatory intervention is warranted based on identified risks and harms; (3) analyzing how existing regulations, particularly GDPR and PIPEDA, align with current technological realities; and (4) proposing appropriate regulatory responses to address any misalignment between regulatory goals and the socio-technical context.

To enrich this analysis, this paper will use Bakan's theory of the psychopathic personality of corporations, complemented by Waldman's insights into corporate privacy practices and Zuboff's taxonomy of data-based business models. These theories provide a critical lens for understanding corporate motivations and behaviour in the data-driven economy, highlighting how profit-driven imperatives can undermine societal values and individual rights.

The next chapter begins to map the current socio-technical landscape. It explores how technological advances have transformed government-led surveillance from the Second World War to the present day. The chapter then examines the development of the right to privacy within the international human rights framework, and analyzes how this framework has been applied to evaluate government-led mass surveillance systems and location-based surveillance practices.

Chapter III. Surveillance and Privacy in the International Human Rights Framework

The “struggle for human rights is as old as history itself,”¹⁷² as it deals with timeless questions about the relationship between the individual and society,¹⁷³ and the need to protect the individual from the abuse of power by monarchs, tyrants, or states.¹⁷⁴ Throughout history, different philosophical visions have debated whether human rights derive “from God, from enduring religious principles, from natural law, or from the authority of the state.”¹⁷⁵ These debates form the foundation of today’s international human rights framework.¹⁷⁶

Robertson and Merrills argue that before the Universal Declaration of Human Rights (UDHR), there were three examples of international measures to protect human rights. The first example was at the abolition of slavery in the early nineteenth century, with a series of bilateral and international treaties condemning slavery, ending the slave trade, and agreeing on various measures to suppress it.¹⁷⁷ The second example was the development and agreement of respect for certain rights in times of war. The various principles and agreements that have been developed since 1745¹⁷⁸ were transformed into positive law with the signing of the Geneva Convention of

¹⁷² A H Robertson & J G Merrills, *Human Rights in the World: An Introduction to the Study of the International Protection of Human Rights*, 4th ed (Manchester: Manchester University Press, 1996) at 8.

¹⁷³ See Paul Gordon Lauren, *The Evolution of International Human Rights: Visions Seen*, 3rd ed (Philadelphia: University of Pennsylvania Press, 2011) at 12.

¹⁷⁴ See Robertson & Merrills, *Human Rights in the World*, *supra* note 172 at 8.

¹⁷⁵ Lauren, *Evolution of International Human Rights*, *supra* note 173 at 208.

¹⁷⁶ For a detail discussion of the different philosophical visions see e.g., Robertson & Merrills, *Human Rights in the World*, *supra* note 172; Lauren, *Evolution of International Human Rights*, *supra* note 173.

¹⁷⁷ See Robertson & Merrills, *Human Rights in the World*, *supra* note 172 at 15–17.

¹⁷⁸ See Robertson & Merrills, *Human Rights in the World*, *supra* note 172 at 18.

1864, the founding text of contemporary humanitarian law,¹⁷⁹ in which twelve states undertook “to respect the immunity of military hospitals and their staff, to care for sick and wounded soldiers whatever their nationality, and to respect the emblem of the Red Cross.”¹⁸⁰ The third example was the protection of the new minorities that resulted mainly from the redrawing of borders that were part of the peace settlement in 1919.¹⁸¹ This protection included equality before the law in terms of civil and political rights, freedom of religion, the right to use their own language, and the right to maintain their own educational and religious institutions.¹⁸² These protections were established through special treaties with the allied or newly created states, minority provisions in peace treaties with enemy states, and the declaration of adherence to minority rights as a condition of membership of the League of Nations.¹⁸³

The devastation of the Second World War prompted a global reckoning, as states recognized that “disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind.”¹⁸⁴ In response, members of the newly formed United Nations (UN) sought to articulate a set of fundamental rights that should be respected and protected by all states. To achieve this goal members of the newly formed UN Commission on Human Rights drafted an initial document.¹⁸⁵ This draft was then subject to extensive negotiation and debate

¹⁷⁹ See ICRC, “The 1864 Geneva Convention” (18 August 2013) online (blog): <icrc.org> [<http://web.archive.org/web/20231221120504/https://www.icrc.org/en/doc/resources/documents/treaty/geneva-convention-1864.htm>].

¹⁸⁰ Robertson & Merrills, *Human Rights in the World*, *supra* note 172 at 19.

¹⁸¹ See Robertson & Merrills, *Human Rights in the World*, *supra* note 172 at 20.

¹⁸² See Robertson & Merrills, *Human Rights in the World*, *supra* note 172 at 23.

¹⁸³ See Robertson & Merrills, *Human Rights in the World*, *supra* note 172.

¹⁸⁴ *Universal Declaration of Human Rights*, UNGA, 3rd Sess, UN doc A/810 (1948) GA Res 217A (III) at Preamble. [*UDHR*]

¹⁸⁵ The drafting committee was composed of government representative of Australia, China, Chile, France, Lebanon, United States, United Kingdom, and the Union of Soviet Socialist Republics. See UNCHR, *Letter from the Chairman of the Commission on Human Rights to the President of the Economic and Social Council*, ECOSOC, UN Doc E/383 (1947); UN, “Drafting of the Universal Declaration of Human Rights: Drafting Committee Members”

among more than 50 member states,¹⁸⁶ ultimately culminating in Universal Declaration of Human Rights (UDHR). On 10 December 1948, the UN General Assembly adopted the final version of this landmark document.¹⁸⁷ The recognition of these fundamental rights marked a significant milestone in the protection of human rights.¹⁸⁸ Underscoring the significance of this achievement, the first paragraph of the preamble to the UDHR proclaims that “recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world.”¹⁸⁹

The UDHR became the foundation of international human rights law and inspired the drafting and adoption of subsequent treaties.¹⁹⁰ Among these, the International Covenant on Civil and Political Rights (ICCPR), adopted in 1966 and entering into force in 1976,¹⁹¹ gave greater judicial specificity to some of the rights of the UDHR.¹⁹² By referring to the UDHR, the ICCPR “unequivocally states that human rights are essential matters of international concern, hence no longer reside within the exclusive confines of the domestic jurisdiction of those states parties to

(last visited 22 January 2024) online: <research.un.org>

[<http://web.archive.org/web/20240120024735/https://research.un.org/en/undhr/draftingcommittee>].

¹⁸⁶ See UN, “History of the Declaration” (last visited 29 September 2021) online: <un.org>

[<http://web.archive.org/web/20231220111458/https://www.un.org/en/about-us/udhr/history-of-the-declaration>].

¹⁸⁷ From the 58 UN members at the time, 48 voted in favour, none against, eight abstained. See UN, *Hundred and Eighty-Third Plenary Meeting of the UN General Assembly*, GA, 3rd Sess, UN Doc A(01)/R3 (1948) 183th Mtg at 933.

¹⁸⁸ See Lauren, *Evolution of International Human Rights*, *supra* note 173 at ch 7.

¹⁸⁹ UDHR, *supra* note 184.

¹⁹⁰ See UN, “The Foundation of International Human Rights Law” (last visited 29 September 2021) online: <un.org> [<http://web.archive.org/web/20231220114207/https://www.un.org/en/about-us/udhr/foundation-of-international-human-rights-law>].

¹⁹¹ This was one of two international covenants. The other one was the International Covenant of Economic, Social, and Cultural Rights (ICESCR), which was approved at the same time. See UN, “International Bill of Human Rights: A Brief History, and the Two International Covenants” (last visited 27 November 2024) online: <ohchr.org> [<https://web.archive.org/web/20241121030730/https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights>].

¹⁹² See Lauren, *Evolution of International Human Rights*, *supra* note 173 at 240.

the covenants.”¹⁹³ Notably, the ICCPR was approved by representatives of more than one hundred and fifty states, as opposed to the fifty or so that created the UN, “and thus became all the more remarkable for reflecting the normative values not of a particular group or narrow region of states but of the broader international community and its collective sense of responsibility toward those who suffered abuse.”¹⁹⁴

Building on the UDHR and ICCPR, regional human rights treaties have also been adopted. The European Convention on Human Rights (1950)¹⁹⁵ and the American Convention on Human Rights (1969)¹⁹⁶ are particularly relevant for this thesis. Both treaties established regional court—the European Court of Human Rights (ECtHR)¹⁹⁷ and the Inter-American Court of Human Rights (IACtHR)¹⁹⁸—to hear to complaints of human rights violations by the signatory parties. While both courts have contributed significantly to the development of privacy rights, ECtHR has dealt with more cases related to surveillance and technology. The case law of the IACtHR has largely focussed on physical intrusions on the right to privacy, with exceptions such as *Escher*,¹⁹⁹ *Tristán Donoso*,²⁰⁰ and *CAJAR*.²⁰¹ For this reason, the main focus of the analysis in this thesis is on the case law of the ECtHR, with reference to the IACtHR where relevant.

¹⁹³ Lauren, *Evolution of International Human Rights*, *supra* note 173 at 239.

¹⁹⁴ Lauren, *Evolution of International Human Rights*, *supra* note 173 at 241–42.

¹⁹⁵ *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 (entered into force: 3 September 1953). [ECHR]

¹⁹⁶ *American Convention on Human Rights*, 22 November 1969, OEA Treaty Series No 36 B-12, 1144 UNTS 123 (entered into force: 18 July 1978). [Pact of San Jose]

¹⁹⁷ *ECtHR*, *supra* note 195 at s II.

¹⁹⁸ *Pact of San Jose, Costa Rica*, *supra* note 196 at ch VIII.

¹⁹⁹ *Case of Escher et al (Brazil)* (2009), Inter-Am Ct HR (Ser C) No 200 [*Escher*].

²⁰⁰ *Case of Tristán Donoso (Panama)* (2009), Inter-Am Ct HR (Ser C) 193 [*Donoso*].

²⁰¹ *Case of Members of “José Alvear Restrepo” Lawyers Collective (Colombia)* (2023), Inter-Am Ct HR (Ser C) No 506 [*CAJAR*].

Understanding how these regional courts interpret and apply privacy rights is one part of the picture. Another aspect is how states implement their international human rights obligations at a national level.

In order to have legal force, international human rights treaties need to be incorporated into a state's domestic legal system. There are two main ways in which this can be achieved. In a monist system, also known as "automatic acceptance," treaties become part of domestic law once the state has given final consent to be bound by them through ratification, accession, or succession. In a dualist system, also known as "specific acceptance," specific domestic legislation is enacted to incorporate the treaty after formal consent has been given.²⁰²

Furthermore, with regard to the national implementation and interpretation of the ECHR and ICCPR, Ando notes that a significant difference between the two instruments lies in their respective enforcement mechanisms. While the ECHR has a judicial body capable of issuing binding decisions on states parties, implementation is managed by domestic authorities. In contrast, the ICCPR relies on non-binding outcomes, known as "views" or "concluding observations," which are enforced at the discretion of the states parties.²⁰³

Nevertheless, even when human rights treaties are not directly incorporated into national law and therefore do not immediately create binding legal obligations for a particular state, they still hold significant normative and persuasive value. Such instruments establish international

²⁰² See e.g., Nisuke Ando, "National Implementation and Interpretation" in Dinah Shelton, ed, *The Oxford Handbook of International Human Rights Law* (Oxford, UK: Oxford University Press, 2013) 698 at 702; Christof Heyns & Frans Viljoen, "The Impact of the United Nations Human Rights Treaties on the Domestic Level" (2001) 23:3 Human Rights Quarterly 483 at 490.

Canada, which has a dualist system, has not directly implemented any of the seven core UN human rights treaties into Canadian law. See e.g., Alexander Agnello & Frédéric Mégret, "The Impact of the United Nations Human Rights Treaties on the Domestic Level in Canada" in Christof Heyns, Frans Jacobus Viljoen & Rachel Murray, eds, *The Impact of the United Nations Human Rights Treaties on the Domestic Level: Twenty Years On*, second revised edition ed (Leiden, The Netherlands: Brill, 2024) 156.

²⁰³ Ando, "National Implementation and Interpretation", *supra* note 202 at 699.

standards, exert external pressure, and serve as important references for national courts and legislatures when addressing domestic human rights issues.²⁰⁴

This chapter begins to map the current socio-technical landscape, providing a comprehensive overview of the international human rights framework and its application to government use of technologies for surveillance practices. It is divided into three main parts. Part I focuses on how technological developments have changed state surveillance practices since the Second World War. As this part will explain, after the computer, the latest wave of information and communication technologies, such as the ubiquity of digital devices, mobile, distributed, and cloud computing, the Internet of Things (IoT), and social media, have had an impact on various aspects of social life and societies, including surveillance capabilities.²⁰⁵ Part II focusses on the development and evolution of the right to privacy within the international human rights framework. Finally, Part III discusses mass surveillance systems and location-based surveillance, arguing that these practices violate the right to privacy and other rights under the international human rights framework. This part also considers the safeguards and limitations necessary to ensure compliance with international human rights standards.

I. Brief History of Surveillance and Technologies

As Lyon noted in 1994, “Surveillance is not new.”²⁰⁶ Surveillance, understood as the routine collection and use of data about individuals and their activities, has long been a part of

²⁰⁴ See e.g., Christof Heyns, Frans Jacobus Viljoen & Rachel Murray, eds, *The Impact of the United Nations Human Rights Treaties on the Domestic Level: Twenty Years On*, second revised edition ed (Leiden, The Netherlands: Brill, 2024); Agnello & Frédéric Mégret, “The Impact of the UNHR Treaties on the Domestic Level in Canada”, *supra* note 202 at 163–64.

²⁰⁵ See Gary T Marx, “Coming to Terms: The Kaleidoscope of Privacy and Surveillance” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 32 at 43.

²⁰⁶ David Lyon, *The Electronic Eye: The Rise of Surveillance Society*, (Minneapolis: University of Minnesota Press, 1994) at 22.

society for a long time, even before the existence of computers and digital technologies.²⁰⁷ Since ancient civilizations, such as the Egyptians or Romans, rulers have kept records of the population for various purposes such as military service, immigration, and taxation.²⁰⁸ Later, in England in 1086 the Domesday Book contained a massive collection of facts about people and property.²⁰⁹ In each of these examples, surveillance activities allowed the ruler of the moment to maintain power over the governed populations.²¹⁰

Historically, governments have been the primary actors able to implement and enforce surveillance systems.²¹¹ Surveillance powers and practices have been essential to the functioning of the state,²¹² serving purposes ranging from national security and criminal investigation to the allocation of social benefits. However, as technology continues to change, so too have the nature and implication of surveillance. Early practices relied on human agents, such as spies and informants, to gather information with little technological assistance. Over time, as technology has advanced, governments have acquired new surveillance capabilities.

The Second World War marked a turning point in the history of surveillance, as the harms it enabled served as a catalyst for the adoption of the UDHR and the ECHR, and for the agreement on international principles and rights to limit the power of individual states to prevent these harms

²⁰⁷ See Rule, *Privacy in Peril*, *supra* note 8 at 14. For a history of the concept of surveillance see generally Lyon, *Electronic Eye*, *supra* note 206.

²⁰⁸ See Lyon, *Electronic Eye*, *supra* note 206 at 22.

²⁰⁹ See Lyon, *Electronic Eye*, *supra* note 206 at 22–23.

²¹⁰ See Lyon, *Electronic Eye*, *supra* note 206 at 23.

²¹¹ However, as the next chapter will develop further, today some private corporations have also the capability to deploy and sustain extensive surveillance systems. See Chapter IV, *below*.

²¹² See e.g., Lyon, *Electronic Eye*, *supra* note 206 at 26 (Lyon explained that “surveillance must be seen, sociologically, as a central feature of modernity. Never before have social organizations developed that could so comprehensively touch the routines of ordinary people in everyday life”).

from happening again.²¹³ During this period, the use of surveillance techniques facilitated the identification, discrimination against, targeting, and mistreating of vulnerable groups.

This widespread surveillance during the Second World War took various forms, ranging from traditional methods to more advanced technological approaches. Some of these techniques were traditional informant or community espionage systems enforced by members of the Gestapo and the SS.²¹⁴ Other practices involved the use of technologies that primarily facilitated the identification and classification of individuals.

Edwin Black's research has shown that the German government, under Hitler's leadership, was aided in its quest for racial cleansing by unique punch card tabulators, designed, supplied, and maintained by IBM through its German subsidiary (Dehomag), which allowed them to classify people on the basis of biographical characteristics collected by a census questioner,²¹⁵ such as community, gender, religion, age, mother tongue, number of children, current occupation, and second jobs.²¹⁶ These punch cards were then processed by tabulating machines, which allowed Dehomag to identify members of the Jewish population and sort them according to various characteristics, such as occupation, place of residence, and national origin.²¹⁷ These were then correlated with "information from the land register, community lists, and church authorities to create a fantastic new database. What emerged was a profession-by-profession, city-by-city, and indeed a block-by-block revelation of the Jewish presence."²¹⁸ The same system was then used,

²¹³ See e.g., Lauren, *Evolution of International Human Rights*, *supra* note 173 at 197–98.

²¹⁴ See Claire M Hall, "An Army of Spies? The Gestapo Spy Network 1933–45" (2009) 44:2 *Journal of Contemporary History* 247 at 247–265.

²¹⁵ See Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's most Powerful Corporation*, (New York: Three Rivers Press, 2002) at 56.

²¹⁶ See Black, *IBM and the Holocaust*, *supra* note 215 at 58.

²¹⁷ See Black, *IBM and the Holocaust*, *supra* note 215.

²¹⁸ Black, *IBM and the Holocaust*, *supra* note 215.

among other things, within the various concentration camps to keep track of the prisoners and to help with the logistics of transporting people between camps.²¹⁹

The atrocities of the Second World War highlighted the dangers of unchecked surveillance and led to the creation of international principles and rights aimed at limiting state power to prevent similar abuses.

Since the mid-20th century, state surveillance practices have changed significantly, as the development of information and communication technologies (ICTs) has enhanced the ability of governments to establish sophisticated record keeping facilities, implement advanced systems, and use complex analytical techniques to interpret data. Two key catalysts for this change have been the introduction of computers (and their continuing improvement) and the increasing ubiquity of the Internet (and Internet-connected devices). These developments have exponentially increased the capacity to generate, collect, store, analyze, and share vast amounts of data about individuals.²²⁰ In addition, the falling costs of technology and data storage have removed financial and practical disincentives for conducting surveillance. As a result, states have gained a greater “capability to conduct simultaneous, invasive, targeted, and broad-scale surveillance than ever before.”²²¹

The remainder of this part is divided into two sections. The first section will introduce modern digital surveillance, analyzing its defining features, such as the rise of big data and dataveillance. The second part will focus on the critical role of location technologies as surveillance tools.

²¹⁹ See e.g., Black, *IBM and the Holocaust*, *supra* note 215 at 21, 358.

²²⁰ See e.g., UN, *SR Human Rights and Fundamental Freedoms while Countering Terrorism (2009)*, *supra* note 14 at par 12. See also *Big Brother Watch and Others v the United Kingdom* [GC], No 58170/13 (25 May 2021) [*Big Brother* [GC]].

²²¹ UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14 at par 33.

A. Digital Technologies and Surveillance

Technological advances since the 1950s have reshaped our world and surveillance practices: computing power has increased exponentially, devices have become networked, more and more aspects of daily life are mediated by digital systems, data has become more indexical²²² and machine-readable, and data storage has expanded and become distributed.²²³

These technological advances have reconfigured the production, circulation, and interpretation of data, creating what is known as “big data.”²²⁴ This term was originally used to describe the handling and analysis of massive datasets.²²⁵ Today, although there is no consensus on an academic or industry definition,²²⁶ it is understood that there are seven key characteristics that identify this type of data: volume (consisting of terabytes or petabytes of data), velocity (created in or near real time), variety (being both structured and unstructured),²²⁷ scope (exhaustive, capturing entire populations or systems), granularity (fine-grained in resolution and unique labelling and identification), relationality (enabling the integration of different datasets), and flexibility and scalability (rapid growth and adaptability).²²⁸

²²² “Indexical data are those that enable identification and linking, and include unique identifiers.” Kitchin, *Data Revolution*, *supra* note 25 at 8.

²²³ See Kitchin, *Data Revolution*, *supra* note 25 at 81.

²²⁴ See Kitchin, *Data Revolution*, *supra* note 25 at xv.

See also, David Lyon, “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique” (2014) 1:2 Big Data & Society 1 at 3.

²²⁵ See Kitchin, *Data Revolution*, *supra* note 25 at 67.

²²⁶ See Kitchin, *Data Revolution*, *supra* note 25 at 68.

²²⁷ *Structured data* are those “that can be easily organized, stored and transferred in a defined data model, such as numbers/text set out in a table or relational databases that have a consistent format.” In contrast, *unstructured data* “do not have a defined data model or common identifiable structure.” Kitchin, *Data Revolution*, *supra* note 25 at 5–6.

²²⁸ See Kitchin, *Data Revolution*, *supra* note 25 at 68.

Kitchin suggested that the production of data can be broadly divided into three categories: directed, automated, and volunteered. Directed data are generated by traditional forms of surveillance, where the gaze of the technology is directed at a person or place by a human operator, such as traditional CCTV cameras.²²⁹ Automated data are generated as an inherent, automatic function of digital technologies, with little to no human oversight, such as cellphone location tracking.²³⁰ Volunteered data refers to the data that are willingly provided by individuals, either to benefit from a service, such as social media,²³¹ or to participate in a collective project, such as OpenStreetMap.²³²

While the value of big data derives from the ability to aggregate and analyze these three categories of data,²³³ this thesis focusses specifically on automated data. One of the key features of big data practices is the ability to generate, collect, aggregate, and analyze vast amounts of automated data about people, including the metadata generated as a by-product of using a device or engaging with a service. For instance, as part of their basic functioning, cellphones continuously transmit their location to nearby towers to enable the transmission of calls, text messages, and Internet connectivity.²³⁴ This location data, a form of metadata, is an example of the type of automated data that is central to this thesis.²³⁵

²²⁹ See Kitchin, *Data Revolution*, *supra* note 25 at 87.

²³⁰ See Kitchin, *Data Revolution*, *supra* note 25 at 89.

²³¹ Kitchin, *Data Revolution*, *supra* note 25 at 87.

²³² See Kitchin, *Data Revolution*, *supra* note 25 at 93.

²³³ See Kitchin, *Data Revolution*, *supra* note 25 at 87.

²³⁴ See Electronic Frontier Foundation, “Cell Site Location Information” (4 April 2018) online (PDF): <eff.org> [http://web.archive.org/web/20201024220927/https://www.eff.org/files/2019/03/28/csli_one-pager.pdf].

²³⁵ As it will be discussed below, initially there was a distinction between the protection afforded to metadata and other data. See Part III-B, *below*.

As digital devices have become deeply integrated into the daily lives of individuals and societies, and as these devices not only perform digital processes but also actively produce automated data, either as a primary function, a by-product, or both, there has been a widespread generation and collection of automated data that has significantly reshaped surveillance practices. With the increasing use of digital technologies to generate, collect, and process data, the falling cost of data storage, and advances in automated data analysis, organizations have gained the ability to conduct data-based surveillance and monitor people through the data trails left by their actions and behaviours.

Roger Clark has called this phenomenon “dataveillance.”²³⁶ This is surveillance that is “enacted through the processing and analysis of data records.”²³⁷ Clark distinguishes between two forms of dataveillance: personal and mass. Personal dataveillance targets a specific individual, and there are usually specific reasons for surveillance (investigation or monitoring), such as being a suspect in a criminal investigation. In contrast, mass dataveillance focusses on a (large) group of people and is based on a generalized suspicion that certain, as yet unidentified, members of the group may be of interest. It therefore has little to do with any specific suspicion or transaction.²³⁸

The implications of mass dataveillance go beyond the mere collection of data and affect how individuals are perceived and treated by surveillance organizations. Mass dataveillance is routinely used to identify people who belong to a particular class of interest to the surveillance organization and who therefore qualify for more focussed attention.²³⁹ In these cases, individuals

²³⁶ See Roger A Clarke, “Information Technology and Dataveillance” (1988) 31:5 Communications of the ACM 498 at 499.

²³⁷ Kitchin, *Data Revolution*, *supra* note 25 at 15.

²³⁸ See Clarke, “Dataveillance”, *supra* note 236 at 503.

²³⁹ See Lyon, *Electronic Eye*, *supra* note 206 at 50; Clarke, “Dataveillance”, *supra* note 236 at 499.

do not have to do anything to become subjects of surveillance. Rather, they come under “categorical suspicion” because they possess certain characteristics.²⁴⁰

This categorical approach to surveillance has far-reaching consequences for individuals and society as a whole. James Rule explained that mass dataveillance systems “not only *collect and record* details of personal information,” but they are also “organized to *provide bases for action towards the people concerned*.”²⁴¹ The ability to monitor people through the data they leave behind has also created the possibility of sorting “people into categories, assigning worth or risk, in ways that have real effects on their life chances.”²⁴² In this kind of surveillance, people are put at risk because of the groups or categories they are assigned to, “rather than on the basis of their individual identity and the personal information it generates.”²⁴³ The result is significant power imbalances, and discrimination that is based on categorical distinctions of individuals, rather than on individual “data subjects.”²⁴⁴

Building on this concept of categorical surveillance, Katina Michel and M. G. Michael proposed the even more invasive concept of “Überveillance.”²⁴⁵ This concept refers to the consolidation of multiple sources of surveillance and the integration of an individual’s personal data to continuously track and monitor their identity and location in real time.²⁴⁶ For Michael and

²⁴⁰ See Gary T. Marx, *Undercover: Police Surveillance in America*, (Berkeley: University of California Press, 1988) referenced by Lyon, *Electronic Eye*, *supra* note 206 at 50.

²⁴¹ Rule, *Privacy in Peril*, *supra* note 8 at 14 [Emphasis in original].

²⁴² David Lyon, “Introduction” in David Lyon, ed, *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination* (London: Routledge, 2005) 1 at 1. See also Gandy, *Panoptic Sort*, *supra* note 9.

²⁴³ Colin J Bennett, “In Defence of Privacy: The Concept and the Regime” (2011) 8:4 *Surveillance & Society* 485 at 490.

²⁴⁴ See Bennett, “In Defence of Privacy”, *supra* note 243.

²⁴⁵ See e.g., Katina Michael & MG Michael, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*, (Hershey, USA: IGI Global, 2009) c XV.

²⁴⁶ See Michael & Clarke, “Location and Tracking of Mobile Devices”, *supra* note 31 at 219.

See also Michael & Michael, *From Bar Codes to Chip Implants*, *supra* note 245 at 464.

Michael, the ultimate form of Überveillance involves the use of “under the skin” technology, such as microchip implants, to track individuals. Although the full application of this concept has not yet to be realized, it is relevant because of the widespread use of devices that generate data about individuals, resulting in an exaggerated and almost omnipresent 24/7 electronic surveillance that is constantly with them.²⁴⁷

The shift from traditional surveillance to dataveillance has significant implications for surveillance practices. First, dataveillance, which involves tracking individuals through the data that they leave behind, is far more cost-effective than traditional methods such as physical observation.²⁴⁸ This economic advantage enables the implementation of mass dataveillance systems, which subject a much larger population to surveillance.

Second, the ease of implementation and operation of these systems has fundamentally changed law enforcement strategies. Previously, authorities would identify specific suspects and collect data on them. Now the approach has been reversed: data are first collected and aggregated from multiple sources “*before* determining the full range of their actual and potential uses.”²⁴⁹ In a mass dataveillance system, algorithms and analytics process collected data about individuals and their environment to reconstruct past events and to predict future behaviours, enabling pre-emptive intervention.

Third, as evidenced by Snowden’s revelations in 2015, government surveillance programs have expanded their reach through two key strategies. First, they have increased their reliance on a close collaboration with corporations, leveraging private sector data and infrastructure. Second,

²⁴⁷ See Michael & Michael, *From Bar Codes to Chip Implants*, *supra* note 245 at 464.

²⁴⁸ Michael & Clarke, “Location and Tracking of Mobile Devices”, *supra* note 31 at 219.

²⁴⁹ Lyon, “Surveillance, Snowden, and Big Data”, *supra* note 224 at 4.

See also Ian Kerr & Jessica Earle, “Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy” (2013) 66 Stanford Law Review 65.

they have increasingly exploited the self-recording devices that individuals use in everyday communications and transactions.²⁵⁰ One example of this corporate-government nexus is the implementation of mandatory third-party data retention regulations. Under these regulations, governments require service providers to store metadata about their customers' communications and location for later access by law enforcement and intelligence agencies.²⁵¹ Building on this foundation of stored data, another increasingly common feature of government-led surveillance is mass interception programs that allow for the widespread collection and analysis of individuals' digital communications.²⁵² These programs represent a significant escalation in the breadth and depth of surveillance capabilities, further blurring the lines between personal and mass surveillance.

Dataveillance, as will be explored in depth in the next chapter, is not exclusive to governments but has also become a pervasive corporate strategy.²⁵³ Within this broader category, location dataveillance emerges as a significant subset that will be used as a concrete example of dataveillance in this thesis. The following section explains, why location dataveillance is deeply intrusive. As Michael and Clark note: "Knowing where someone has been, knowing what they are doing right now, and being able to predict where they might go next is a powerful tool for social control and for chilling behaviours."²⁵⁴

²⁵⁰ See e.g., Lyon, "Surveillance, Snowden, and Big Data", *supra* note 224 at 3.

See also OHCHR, *Report on Best Practices and Lessons Learned on How Protecting and Promoting Human Rights Contribute To Preventing and Countering Violent Extremism*, HRC, 33th Sess, UN Doc A/HRC/33/29 (2016) at par 59.

²⁵¹ See e.g., OHCHR, *The Right to Privacy in the Digital Age*, HRC, 27th Sess, UN Doc A/HRC/27/37 (2014) at par 20.

²⁵² This will be further discussed, *below*, at Part III-A.

²⁵³ See Chapter IV, *below*.

²⁵⁴ Michael & Clarke, "Location and Tracking of Mobile Devices", *supra* note 31 at 220.

B. Location Technologies and Surveillance

The use of location technologies exemplifies the shift from traditional surveillance to dataveillance. In the past, monitoring a person's movements meant following them around the city—someone would have to spend their day following them, taking notes and pictures of where they went, at what time, and for how long. With the advent of GPS technology law enforcement could install a GPS transmitter in a suspect's car and retrieve the information collected every few days.²⁵⁵ Subsequently, the proliferation of cellphones streamlined this process for government agencies.

As part of their normal operation, cellphones communicate with (and provide their location to) cell towers for basic functions such as calls, text messages, and Internet connectivity.²⁵⁶ Telecommunications companies use this capability to measure and distribute traffic signals.²⁵⁷ As a result, these companies can locate and track the movements of a single phone across a city or country (wherever they have network coverage).²⁵⁸ For law enforcement agencies, this meant that instead of having to tail someone or install a GPS receiver, they could simply ask the telecom companies for these data.

Given the richness of these data, some countries have introduced legislation requiring the preservation and retention of the metadata for historical surveillance purposes.²⁵⁹ The widespread

²⁵⁵ See e.g., Kevin S Banksto & Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones" (2014) 123 Forum, online: <yalelawjournal.org> [<http://web.archive.org/web/20231222141720/https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones>].

²⁵⁶ See Electronic Frontier Foundation, "CSLI", *supra* note 234.

²⁵⁷ See e.g., Christos Laoudias et al, "A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation" (2018) 20:4 IEEE Communications Surveys Tutorials 3607 at 3607.

²⁵⁸ See Electronic Frontier Foundation, "CSLI", *supra* note 234.

²⁵⁹ See UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14 at par 15.

adoption of technologies with location capabilities, such as smartphones and wearables, has further improved the quality and availability of location data.²⁶⁰

One of the Snowden revelations was the existence of interception programs specifically designed to mine and collect location data by intelligence agencies.²⁶¹ These documents identified location as one of the “primary objectives of data interception because of the kinds of questions it allows agencies to answer.”²⁶² The location data generated by location technologies can be analyzed to determine the location and movements of a device at a particular time and place, and can also be used to predict where it will be. In addition, the analysis of these data can be used to infer things about individuals’ lifestyles and to make connections between individuals. Given the far-reaching implications of location dataveillance systems, it is crucial to examine the capabilities that organizations gain from them. The following paragraphs explain these capabilities, which illustrate why this type of dataveillance is particularly problematic and warrants careful consideration.²⁶³

1) Realtime Tracking and Future Locations

Without the use of the data generated by location technologies, few people can know with certainty a person’s precise location at any given moment of the day. Typically, this kind of

²⁶⁰ See e.g., Herrmann et al, “Privacy in Location-Based Services”, *supra* note 21 at 148; Electronic Frontier Foundation, “CSLI”, *supra* note 234; Laoudias et al, “Survey of Enabling Technologies”, *supra* note 257 at 3607.

²⁶¹ See e.g., “An Excerpted Document from Britain’s Government Communications Headquarters From May 2010” (May 2010) online (PDF): <http://web.archive.org/web/20231219173411/https://www.documentcloud.org/documents/1009661-gchq.html>; “An Excerpted Document From the NSA From May 2010” (May 2010) online (PDF): <http://web.archive.org/web/20231219172950/https://www.documentcloud.org/documents/1009660-nsa.html>.

See also Agnieszka Leszczynski, “Spatial Big Data and Anxieties of Control” (2015) 33:6 *Environ Plan D: Society and Space* 965 at 968–69.

²⁶² Leszczynski, “Spatial Big Data”, *supra* note 261 at 968.

²⁶³ The technical aspects of location dataveillance are described in more detail in Chapter IV-III.A, *below*.

knowledge is limited to people who are in the same place at the same time can therefore see them, or people who know because that person has told them. What has changed with digital location technologies is that they have given organizations the ability to generate, collect, and access multiple sources of location data (e.g., cell tower data, GPS data collected by smartphones or wearables) and, based on this knowledge, to know the precise location of specific devices.²⁶⁴

These data can be used to track the movement or location of a device and visualize it on a map to get a better visual understanding of how a device moves around the city, and the places it visits.²⁶⁵ This visualization can be of historical or real-time data; either way, on any given day, an organization with access to these data can see how a particular device moves along the streets, the stops made, the time spent at each stop, and the routes taken to reach each destination.

These location data can also be used to predict the location of individuals. People's daily routines follow a pattern (e.g., they wake up, go to work, and return home) and follow similar routes every day (e.g., the same bus route or the same highway from home to work).²⁶⁶ Therefore, by having access to the records of past locations and mobility patterns, organizations can use algorithms to predict where people will be in the next hour, or even weeks or years.²⁶⁷

²⁶⁴ See e.g., Gasson et al, "Normality Mining", *supra* note 21.

²⁶⁵ See e.g., Monmonier, *Spying with Maps*, *supra* note 9 (referring to "cartographies of surveillance").

²⁶⁶ This predictability of people's mobility patterns and the places they visit the most also reduces the efficacy of anonymity techniques for location data. See Chapter II-I.A.2.b, *above*

See also, Hui Zang & Jean Bolot, "Anonymization of Location Data Does Not Work: A Large-scale Measurement Study" (Paper delivered at the 17th Annual International Conference on Mobile Computing and Networking, Las Vegas, September 19-23, 2011) in Parameswaran Ramanathan, Thyaga Nandagopal & Brian Neil Levine, eds, *MobiCom' 11* (New York: ACM, 2011) 145, DOI:<10.1145/2030613.2030630>; Dionysis Manousakas et al, "Quantifying Privacy Loss of Human Mobility Graph Topology" (2018) 3 Proceedings on Privacy Enhancing Technologies 5.

²⁶⁷ See Adam Sadilek & John Krumm, "Far Out: Predicting Long-Term Human Mobility" (2021) 26:1 Proceedings of the AAAI Conference on Artificial Intelligence 814; Ashbrook & Starner, "Using GPS to Predict Movement", *supra* note 21.

Similarly, companies can predict what activity we will do next. See e.g., Byoungjip Kim et al, "Agatha: Predicting Daily Activities from Place Visit History for Activity-Aware Mobile Services in Smart Cities" (2015) 11:12 International Journal of Distributed Sensor Networks 1.

2) *Infer Details About Lifestyles*

Places have a social function and meaning;²⁶⁸ knowing where someone is, can indicate what they are doing, and this can be used to make assumptions about a person's lifestyle.²⁶⁹ This is because people's movements do not take place in an abstract space, but in a specific context, with neighbourhoods, streets, and buildings carrying certain socially constructed meanings.²⁷⁰ These meanings can be used to program algorithms to infer additional information about people.

Kitchin and Dodge emphasize this point: "The spatial context is not incidental or inert, it is constitutive and productive—the *where* makes a difference to the *what* that unfolds."²⁷¹ Furthermore, tracking and recording movement are not neutral acts. Human movement "is made meaningful in social and cultural context."²⁷² This means that the trajectory from X to Y and its digital recording is not just a line or a set of points; it carries a meaning determined by the designers who set the parameters of the algorithm designed to analyze the data.

This assigned meaning has far-reaching implications, influencing how individuals and groups are perceived in society and how decisions are made about (and for) them. For example, an algorithm could be programmed to identify people who attend a mosque more than three times a week and categorize them as potential risks.

The use of data to create profiles of individuals and make decisions based on them is not new or exclusive to location technologies.²⁷³ However, location data adds a very detailed spatial

²⁶⁸ See Tim Cresswell, *Place: An Introduction*, 2d ed (Malden, MA: John Wiley & Sons, 2015).

²⁶⁹ See Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39 at 33–34.

²⁷⁰ See Cresswell, *Place*, *supra* note 268.

²⁷¹ Rob Kitchin & Martin Dodge, *Code/Space: Software and Everyday Life*, (Cambridge, MA: The MIT Press, 2011) at 65.

²⁷² Tim Cresswell, "The Production of Mobilities" (2001) 43 *New Formations* 11 at 13.

²⁷³ See generally Mireille Hildebrandt & Serge Gutwirth, eds, *Profiling the European Citizen: Cross-Disciplinary Perspectives*, (Dordrecht: Springer, 2008).

and temporal dimension to the profiling, allowing organizations to make decisions based on criteria such as income, religion, hobbies, and occupations, without having to collect them directly.

This enhanced profiling capability has evolved from methods of categorizing people based on the places where they live.²⁷⁴ The proliferation of digital location technologies has significantly increased the volume and granularity of data available, enabling more detailed and personalized geographic profiles. As Alex “Sandy” Pentland noted, “The Proliferation of GPS-enabled devices makes it possible to leap beyond demographics to directly measure human behaviour. Where do people eat, work, and hang out? What routes do they travel?”²⁷⁵

Modern location-based profiles are not limited to a single source of static data, such as postal codes. Instead, they incorporate dynamic data about people’s movements throughout the day and night, including frequently visited locations and areas they tend to avoid.²⁷⁶ These comprehensive movement data allows for more nuanced groupings of individuals, such as outdoor enthusiasts, religious adherents, members of the LGBTIQ+ community, and government officials.

3) Geo-Relational Analysis

Organizations can use geo-relational analysis algorithms that compare the location data of individuals to infer relationships between them.²⁷⁷ An example of this is the US National Security Agency’s (NSA) “Co-Traveller” program, which used various analytical techniques for bulk

²⁷⁴ See Monmonier, *Spying with Maps*, *supra* note 9 at ch 9; Gandy, *Panoptic Sort*, *supra* note 9 at 87; Goss, “We Know Who You Are and We Know Where You Live”, *supra* note 9.

²⁷⁵ Pentland, “Society’s Nervous System”, *supra* note 10 at 32.

²⁷⁶ For detail explanation of the difference between traditional geodemographics and the use of the location data generated and collected by technologies see Smith, “Metrics, locations, and lift”, *supra* note 10; Pentland, “Society’s Nervous System”, *supra* note 10.

²⁷⁷ See Colin J Bennett et al, eds, *Transparent Lives: Surveillance in Canada*, (Edmonton: AU Press, Athabasca University, 2014) at 95.

processing of cellular network location data to identify (new) targets for surveillance.²⁷⁸ This approach allowed the NSA to identify potential “co-travellers” who might be involved in terrorist activities, based on their mobile devices pinging the same cell towers in the same sequence as known targets.²⁷⁹

However, it is crucial to recognize that location data, regardless of their accuracy, are sensitive and can lead to inferences based on biases and assumptions inherent in algorithms and human interpretation. Simply being in the same locations as known terrorists does not necessarily imply an association with them. Nevertheless, being added as a potential intelligence target can have significant negative consequences for an individual.

While other methods, such as communications records or social network analysis, can establish connections between people, location data provide a more complete picture of an individual’s life and therefore a better picture of their relationships with the people they physically interact with.²⁸⁰ This approach provides a better understanding of relationships, although it may not capture all associative ties, particularly those maintained solely online.

²⁷⁸ See Ashkan Soltani & Barton Gellman, “New Documents Show How the NSA Infers Relationships based on Mobile Location Data”, *Washington Post* (10 December 2013), online: <washingtonpost.com> [http://web.archive.org/web/20180219012613/https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?utm_term=.fc24fe7d991b].

²⁷⁹ See Barton Gellman & Ashkan Soltani, “NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show”, *Washington Post* (12 April 2013), online: <washingtonpost.com> [http://web.archive.org/web/20140131100316/https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html]; “How the NSA is Tracking People Right Now”, *Washington Post* (December 2013), online: <washingtonpost.com> [http://web.archive.org/web/20140125154304/http://apps.washingtonpost.com/g/page/national/how-the-nsa-is-tracking-people-right-now/634/]; Leszczynski, “Spatial Big Data”, *supra* note 261 at 969.

²⁸⁰ See e.g., Nathan Eagle & Alex (Sandy) Pentland, “Reality Mining: Sensing Complex Social Systems” (2006) 10 *Personal and Ubiquitous Computing* 255; Ashbrook & Starner, “Using GPS to Predict Movement”, *supra* note 21; Scott R Peppet, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent” (2014) 93 *Texas Law Review* 85 at 131.

Therefore, the aggregation and analysis of the location data generated and collected by location technologies can be used to “reconstruct individual spatial histories, predict future spatial trajectories,”²⁸¹ infer details about their lifestyles, and, “determine copresence with others based on correlations across locational content streams.”²⁸²

The implications of such extensive location dataveillance go beyond individual privacy concerns. For instance, location dataveillance can lead to other forms of corruption and abuse of power.²⁸³ A system capable of singling out an individual within a given area is technologically similar to one that “creates a list of all people who disagree with a particular political policy, or who have openly voiced concern about a particular leader.”²⁸⁴ This potential for abuse underscores the significant privacy concerns and power that location dataveillance gives to the organization that has access to it.

This part discussed the evolution of surveillance practices, focussing on the transition from traditional methods to modern digital surveillance techniques. It highlighted how technological advances, particularly in computing and the Internet, have dramatically increased the capacity to collect, store, and analyze data. It emphasized the rise of “big data” and “dataveillance,” and explained how these concepts have transformed surveillance capabilities and practices. The following part will focus on the development and evolution of the right to privacy within the academic and international human rights frameworks in light of these technological advances.

²⁸¹ Leszczynski, “Spatial Big Data”, *supra* note 261 at 970.

²⁸² Leszczynski, “Spatial Big Data”, *supra* note 261.

²⁸³ See Lyon, Marmura & Peroff, *Location Technologies*, *supra* note 30.

²⁸⁴ Curry, Phillips & Regan, “Emergency Response Systems and the Creeping Legibility of People and Places”, *supra* note 103 at 43.

II. Privacy and Technologies in the International Human Rights Framework

Privacy is a crucial concept in the context of surveillance and technology. From wiretapping cases²⁸⁵ to the more recent implementation of mass dataveillance programs by national security agencies,²⁸⁶ the right to privacy, recognized in international human rights law, has often been invoked to regulate these practices and limit government abuse of power.²⁸⁷

The concept of privacy has both old and deep roots in human history.²⁸⁸ In the modern context, it was most notably articulated by Warren and Brandeis in their seminal 1890 article “The Right to Privacy,” in which they defended the importance of privacy as an individual right, defined as the right to be left alone.²⁸⁹ Since then, scholars have offered various conceptions of privacy,²⁹⁰

²⁸⁵ The ECtHR and the IACtHR have argued that “tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence.” *Huvig v France*, No 11105/84 (24 April 1990) at par 32 [*Huvig*]. See also *Escher*, *supra* note 199 at par 129.

²⁸⁶ This will be developed in Part III-A., *below*.

²⁸⁷ Other rights that have been invoked to regulate these practices are freedom of opinion and expression, and free assembly. See e.g., UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14; UN Special Rapporteur on Freedom of Opinion and Expression et al, “Joint Declaration on Freedom of Expression and Responses to Conflict Situations”, *supra* note 14; UN, *SR Human Rights and Fundamental Freedoms while Countering Terrorism (2009)*, *supra* note 14.

²⁸⁸ For a history of the concept of privacy see Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, (Ithaca: Cornell University Press, 1997) at ch 1. See also Daniel J Solove, “A Brief History of Information Privacy Law” in Kristen J Mathews, ed, *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (New York: Practising Law Institute, 2006) 1.

²⁸⁹ See Samuel D Warren & Louis D Brandeis, “The Right to Privacy” (1890) 4:5 Harvard Law Review 193 at 193–220.

²⁹⁰ For a summary and explanation of different conceptions, see Daniel J Solove, *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008) at 12–38; DeCew, *In Pursuit of Privacy*, *supra* note 288.

See also Antoinette Rouvroy & Yves Poullet, “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy” in Serge Gutwirth et al, eds, *Reinventing Data Protection?* (Dordrecht: Springer, 2009) 45 (They identified three facets of the concept of privacy: seclusion or the right to opacity, decisional privacy, and individual informational control. They reconciled these theories of privacy arguing that each of them protects self-determination, which is the crucial value behind privacy, from different threats).

including limited access to the self,²⁹¹ secrecy,²⁹² control over personal information,²⁹³ personhood,²⁹⁴ and intimacy.²⁹⁵

Despite this long-standing recognition of the importance of privacy in academia, its formal protection in legal frameworks was initially limited. Prior to the adoption of the UDHR, most constitutions around the globe had similar guarantees for the confidentiality of correspondence and the protection of the sanctity of the home from arbitrary interference by the state.²⁹⁶ However, none of them contained a general guarantee of the right to privacy, or an “umbrella term such as ‘privacy’ or ‘private life.’”²⁹⁷

The inclusion of the right to privacy in Article 12 of the UDHR marked a significant turning point. As Oliver Diggelman and Maria Nicole Cleis have argued, the international guarantee went beyond national guarantees from the outset. Something new was created for which there was no

²⁹¹ See e.g., Ruth Gavison, “Privacy and the Limits of Law” (1980) 89:3 Yale Law Journal 421 at 423 (she argued that privacy “is related to our concern over accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention.”); Anita L Allen, “Coercing Privacy” (1999) 40:3 William and Mary Law Review 723 at 724 (she explained that privacy is obtained “where persons and personal information are, to a degree, inaccessible to others”); James B Rule et al, *The Politics of Privacy*, (Broadway: New American Library, 1980) at 23 (he argued that privacy can be understood as the “restriction of others’ access to information about oneself”).

²⁹² See e.g., Richard A Posner, “The Economics of Privacy” (1981) 71:2 American Economic Review 405 (Privacy as concealment of information).

²⁹³ See e.g., Alan F Westin, “Social and Political Dimensions of Privacy” (2003) 59:2 Journal of Social Issues 431 at 431 (he defined privacy as the “claim of an individual to determine what information about himself or herself should be known to others”); Charles Fried, “Privacy” (1968) 77:3 Yale Law Journal 475 at 482 (“Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves”).

²⁹⁴ See e.g., Edward J Bloustein, “Privacy as an Aspect of Human Dignity. An Answer to Dean Prosser” in Ferdinand D Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, UK: Cambridge University Press, 1984) 156; James Griffin, “The Human Right to Privacy” (2007) 44 San Diego Law Review 267.

²⁹⁵ See e.g., Tom Gerety, “Redefining Privacy” (1977) 12:2 Harvard Civil Rights-Civil Liberties Law Review 233.

²⁹⁶ See UNCHR, Drafting Committee, *International Bill of Rights Documented Outline. Part I*, UN Doc E/CN.4/AC.1/3/Add.1 (1947) at 78–94.

²⁹⁷ Oliver Diggelman & Maria Nicole Cleis, “How the Right to Privacy Became a Human Right” (2014) 14 Human Rights Law Review 441 at 442.

precedent in any national constitution.²⁹⁸ This development was not the result of a deliberate strategy, but rather an unintended consequence of the drafting process. They stressed that there “was no conscious decision to create an integral guarantee,”²⁹⁹ as “Umbrella terms were introduced, eliminated and replaced as if such decisions were mere editorial details.”³⁰⁰

Interestingly, the full potential of this newly created right was not immediately apparent. Diggelmann and Cleis point out that the potential of the right “was dramatically underestimated at the time of its creation.”³⁰¹ This underestimation, however, did not diminish its eventual impact. Despite its somewhat accidental inclusion in the UDHR, “The right to privacy has since become one of the most important human rights,”³⁰² with profound implications for individual freedoms and societal norms.

Privacy was first recognized as a right in international law in Article 12 of the UDHR,³⁰³ and it was later articulated in Article 17 of the Covenant on Civil and Political Rights (ICCPR),³⁰⁴ and other regional instruments such as Article 8 of the European Convention of Human Rights (ECHR).³⁰⁵ The contents and scope of this right have been developed through the case law from

²⁹⁸ See Diggelmann & Cleis, “How Privacy Became a Human Right”, *supra* note 297.

²⁹⁹ Diggelmann & Cleis, “How Privacy Became a Human Right”, *supra* note 297 at 457.

³⁰⁰ Diggelmann & Cleis, “How Privacy Became a Human Right”, *supra* note 297.

³⁰¹ Diggelmann & Cleis, “How Privacy Became a Human Right”, *supra* note 297 at 441.

³⁰² Beate Roessler, “X—Privacy as a Human Right” (2017) 117:2 Proceedings of the Aristotelian Society 187 at 193.

³⁰³ “No one shall be subjected to arbitrary interferences with his privacy, family, home or correspondence, not to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

³⁰⁴ “1. No one shall be subjected to arbitrary or unlawful interference with this privacy, family, home or correspondence, not to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.”

³⁰⁵ Additional regional instruments include *Pact of San Jose, Costa Rica*, *supra* note 196 at art 11; *Convention on the Rights of the Child*, 20 November 1989, 1577 UNTS 3 (entered into force: 2 September 1990) at art 16; *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, 2220 UNTS 3 (entered into force: 1 July 2003) at art 14; Organization of the Islamic Conference, *Cairo Declaration on Human Rights in Islam*, UN Doc [ST/GENEVA/JOIC/SEM/2002/2 (2002) at art 18; League

human rights tribunals,³⁰⁶ the General Comments by the Human Rights Committee (CCPR),³⁰⁷ the reports of the UN High Commissioner for Human Rights (OHCHR), and recommendation by special rapporteurs.

The right to privacy, recognized in the UDHR and ICCPR, has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others, free from states intervention and from excessive unsolicited intervention by other uninvited individuals.³⁰⁸ This definition is consistent with the interpretations of regional human rights courts.

The European Court of Human Rights (ECtHR) has explained that Article 8 of the ECHR is primarily intended to ensure the development, without outside interference, of the personality of each individual in their relations with others.³⁰⁹ Similarly, the Inter-American Court of Human Rights (IACtHR) has characterized the protection afforded by Article 11 of the Pact of San Jose as safeguarding individuals from abusive and arbitrary invasion or attack by third parties or the public authorities.³¹⁰

of Arab States, *Arab Charter on Human Rights*, OHCHR, UN Doc [ST/HR/]CHR/NONE/2004/40/Rev.1 (2004) at art 21(1); African Union, *African Charter on the Rights and Welfare of the Child*, July 1990 (entered into force on 29 November 1999) at art 10.

³⁰⁶ Such as the European Court of Human Rights (ECtHR), and the Inter-American Court of Human Rights (IACtHR).

³⁰⁷ One of the essential functions of the Human Rights Committee (created under article 28 of the ICCPR) is to issue General Comments which explain the meaning of ICCPR provisions. See UN, *Rules of Procedure of the Human Rights Committee*, CCPR, UN Doc CCPR/C/3/Rev.12 (2021) at rule 76. See also Sarah Joseph & Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, 3d ed (Oxford: Oxford University Press, 2013) at par 1.35; Helen Keller & Leena Grover, “General Comments of the Human Rights Committee and Their Legitimacy” in Helen Keller & Geir Ulfstein, eds, *UN Human Rights Treaty Bodies* (Cambridge, UK: Cambridge University Press, 2012) 116.

³⁰⁸ See OHCHR, *Right to Privacy* (2018), *supra* note 17 at par 5. See also UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14 at par 22.

³⁰⁹ See *Uzun v Germany*, No 35623/05, [2010] VI ECHR 1 at par 43 [*Uzun*]; *Van Hannover v Germany (no2)* [GC], No 40660/08 (7 February 2012) at par 95 [*Van Hannover*].

³¹⁰ See OAS, Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression, *Standards for a Free, Open, and Inclusive Internet*, by Lanza Edison, OEA/Ser.L/V/II CIDH/RELE/INF.17/17

Importantly, the scope of privacy has been interpreted broadly. It extends beyond the confines of the home, the content of communications, or private spaces. The expansive interpretation includes activities in public spaces³¹¹ and the metadata generated by digital interactions.³¹² Moreover, as an international human right, the right to privacy covers various aspects of an individual's self-development and personality, including a zone of interaction with others.³¹³

The value of privacy is multifaceted. It is recognized as an expression of human dignity,³¹⁴ and it is directly linked to the protection of human autonomy and personal identity.³¹⁵ In addition, privacy plays a critical role in enabling the enjoyment and exercise of other human rights online and offline, such as freedom of expression,³¹⁶ freedom of association and assembly,³¹⁷ and the prohibition of discrimination.³¹⁸

(2017) at par 187.

³¹¹ See e.g., *PG and JH v the United Kingdom*, No 44787/98, [2001] IX ECHR 195 at par 56-59 [*P.G.*].

³¹² See e.g., OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 6; *Escher*, *supra* note 199 at par 114.

³¹³ See e.g., *P.G.*, *supra* note 311 at par 56; *Peck v the United Kingdom*, No 44647/98, [2003] I ECHR 123 at par 57 [*Peck*].

See also Anja Seibert-Fohr, "Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy" in Joseph E David et al, eds, *Strengthening Human Rights Protections in Geneva, Israel, the West Bank and Beyond* (Cambridge, UK: Cambridge University Press, 2021) 40.

³¹⁴ Regarding the value of privacy, the literature can be broadly classified into scholars that argue that protecting privacy has a value only for the individual, and others who argue that it is valuable for the individual and for society. See e.g., Priscilla M Regan, "Privacy and the Common Good: Revisited" in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 50; Solove, *Understanding Privacy*, *supra* note 290 at 92–93; Julie E Cohen, "What Privacy is For" (2013) 126 *Harvard Law Review* 1904.

³¹⁵ See OHCHR, *The Right to Privacy in the Digital Age*, HRC, 48th Sess, UN Doc A/HRC/48/31 (2021) at par 7; UN, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment*, CRC, UN Doc CRC/C/GC/25 (2021) at par 67. See also Steeves, "Now You See Me", *supra* note 24 at 465.

³¹⁶ See e.g., *Big Brother [GC]*, *supra* note 220 at par 312; UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14; UN, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by David Kaye, HRC, 29th Sess, UN Doc A/HRC/29/32 (2015) at par 22.

³¹⁷ See e.g., OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 14.

³¹⁸ See e.g., OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 11.

Beyond its individual importance, privacy is recognized as vital for society beyond the individual or the group.³¹⁹ It fosters social relationships and is fundamental to the functioning of democracy. Recognizing this broader impact, privacy scholars have complemented the traditional focus on privacy as an individual right with an understanding of the value of privacy to society.³²⁰ They argue that privacy serves not only to protect the interest of the individual, but also to “enable social and professional relationships, democratic decision-making processes, and political participation.”³²¹

Extending this socializing role of privacy, scholars have emphasized its crucial role in enabling individuals to participate in different social roles (e.g., professional, religious, and intellectual) and relationships (e.g., friendship, intimacy, and among strangers).³²² This perspective recognizes that individuals do not live in isolation but engage in necessary daily interactions with many people.³²³ These interactions span a spectrum from the professional to the intimate,

³¹⁹ See Colin J Bennett & Charles D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, (Cambridge, MA: MIT Press, 2006) at 24.

See also Gavison, “Privacy and the Limits of Law”, *supra* note 291; Regan, “Privacy and the Common Good”, *supra* note 314; Beate Roessler & Dorota Mokrosinska, “Privacy and Social Interaction” (2013) 39:8 *Philosophy & Social Criticism* 771; Kirsty Hughes, “The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 225; Kirsty Hughes, “A Behavioural Understanding of Privacy and its Implications for Privacy Law” (2012) 75:5 *The Modern Law Review* 806; Dorota Mokrosinska & Beate Roessler, “Introduction” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 1.

³²⁰ This thesis follows Hughes preference on using the term “value of privacy to society” over “social value of privacy.” See Hughes, “Social Value of Privacy”, *supra* note 319 at 227–28.

³²¹ Mokrosinska & Roessler, “Introduction”, *supra* note 319 at 3–4. See also Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, (Chapel Hill: University of North Carolina Press, 1995); Regan, “Privacy and the Common Good”, *supra* note 314.

³²² For instance, Gavison argues that some privacy is necessary to contribute to a more pluralistic and tolerant society, where “individuals can grow, maintain their mental health and autonomy, create and maintain human relations, and lead meaningful lives.” Gavison, “Privacy and the Limits of Law”, *supra* note 291 at 455.

³²³ See Solove, *Understanding Privacy*, *supra* note 290 at 91.

See also Ferdinand David Schoeman, *Privacy and Social Freedom*, (Cambridge, UK: Cambridge University Press, 1992) at 8 (“[...]privacy is important largely because of how it facilitates association with people, not independence from people.”).

providing opportunities for diverse relationships but also potentially leading to situations of conflict and increased social control over individuals.³²⁴

Given these complex social dynamics, privacy plays a dual role. It allows individuals to engage in different types of interactions, while at the same time providing protection from excessive social control. This dual role of privacy, prevalent in certain sociological understandings,³²⁵ has led some authors to propose a dynamic conception of privacy.³²⁶ In this view, privacy is not a static state of seclusion, confidentiality, or restricted access, but rather a dynamic process that oscillates between interaction with others and time spent alone. This dynamic conception of privacy has been used to propose privacy regulation,³²⁷ and technical designs of current technologies,³²⁸ reflecting a more nuanced understanding of privacy in our interconnected world.

The international human rights system has also recognized the socializing role of privacy. For instance, the ECtHR has argued that respect for private life must include, to some extent, “the

³²⁴ See Solove, *Understanding Privacy*, *supra* note 290 at 94.

³²⁵ See e.g., Irwin Altman, “Privacy: A Conceptual Analysis” (1976) 8:1 *Environment and Behavior* 7; Irwin Altman, “Privacy Regulation: Culturally Universal or Culturally Specific?” (1977) 33:3 *Journal of Social Issues* 66.

³²⁶ See e.g., Valerie Steeves, “Reclaiming the Social Value of Privacy” in Ian Kerr, Valerie M Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford; New York: Oxford University Press, 2009) 191. See also Regan, “Privacy and the Common Good”, *supra* note 314.

³²⁷ See e.g., Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, (New Haven: Yale University Press, 2012); Mireille Hildebrandt, “Privacy and Identity” in Erik Claes, Antony Duff & Serge Gutwirth, eds, *Privacy and the Criminal Law* (Antwerp: Intersentia, 2006) 61.

³²⁸ See e.g., Jens Pedersen, “Privacy and Location Technologies” (Paper delivered at the Workshop on Location System Privacy and Control at Mobile HCI 2004, Glasgow, UK, September 2004) [unpublished] online: <<http://web.archive.org/web/20131227142149/http://itu.dk/people/jensp/locationprivacy.pdf>> ; Leysia Palen & Paul Dourish, “Unpacking ‘Privacy’ for a Networked World”(Paper delivered at the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, FL, April 5–10, 2003) in Gilbert Cockton & Panu Korhonen, eds, *CHI’ 03* (New York: ACM, 2003) 129, DOI:<10.1145/642611.642635>; Airi Lampinen, Fred Stutzman & Markus Bylund, “Privacy for a Networked World: Bridging Theory and Design”(Paper delivered at the CHI Conference on Human Factors in Computing, Vancouver, BC, May 7-12, 2011) in Desney Tan, Bo Begole & Wendy A. Kellogg, eds, *CHI EA’ 11* (New York: ACM, 2011) 2441, DOI:<10.1145/1979742.1979579>.

right to establish and develop relationships with other human beings,”³²⁹ thereby protecting “the possibility for the individual to develop his or her social identity.”³³⁰ Similarly, the IACtHR has held that respect for private life “encompasses aspects of physical and social identity,” including “the right to establish and develop relationships with other human beings and with the outside world.”³³¹

This broad concept of privacy underlines its value to both the individual and society. Some authors have emphasized the importance of privacy for liberal democracies and innovation,³³² arguing that it enables the development of autonomous and thoughtful individuals, supports their roles as citizens,³³³ and protects them from public scrutiny in certain areas of decision making.³³⁴ As a result, the protection of privacy is essential to sustain democracy and to foster a society that respects and protects values such as individual freedom.³³⁵

Recognizing the value of privacy in democracy, the UN Human Rights Council (HRC) has reaffirmed its importance in enabling individuals to participate in various aspects of life (i.e., political, economic, social, and cultural) and its role as the foundation of a democratic society.³³⁶

³²⁹ *Niemietz v Germany*, No 13710/88 (16 December 1992) at par 28 [*Niemietz*].

³³⁰ *Bărbulescu v Romania* [GC], No 61496/08 (5 September 2017) at par 70 [*Bărbulescu*].

³³¹ *Case of Artavia Murillo et al (“In Vitro Fertilization”) (Costa Rica)* (2012), Inter-Am Ct HR (Ser C) No 257 at par 143 [*Murillo*]. See also *Escher*, *supra* note 199 at par 114; Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression, *SP Freedom of Expression*, *supra* note 310 at par 187, 189.

³³² See e.g., Cohen, “What Privacy is For”, *supra* note 314 at 1927; Daniel J Solove, “The Meaning and Value of Privacy” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 71.

³³³ For instance, Westin describes privacy as a social good that requires continuous support from the enlightened public see Westin, “Social and Political Dimensions of Privacy”, *supra* note 293. See also Helen Nissenbaum, “Privacy as Contextual Integrity” (2004) 79:1 *Washington Law Review* 119.

³³⁴ See e.g., Nissenbaum, “Privacy as Contextual Integrity”, *supra* note 333 at 156–57 (She recognizes that privacy, besides protecting individual values such as autonomy, preservation of human relationship, and freedom, also protects democracy and other social values).

³³⁵ See Gavison, “Privacy and the Limits of Law”, *supra* note 291 at 455. See also Allen, “Coercing Privacy”, *supra* note 291 (For her privacy is a requirement for the individual’s well-being, for freedom, democracy, and autonomy).

³³⁶ See UN, *The Right to Privacy in the Digital Age*, HRC, 34th Sess, UN Doc A/HRC/RES/34/7 (2017) GA Res

Similarly, in the *Big Brother* case, the ECtHR judges in the concurring opinion recognized that privacy is a fundamental precondition for the existence of a democratic society.³³⁷ They further explained that the “encroachments on privacy do not merely diminish individual autonomy and mental and physical health, they also inhibit democratic self-governance.”³³⁸

Within the international human rights framework, courts have identified various instances where surveillance practices and systems interfere with the right to privacy. These intrusions generally occur when governments systematically collect and store data regardless of whether the data are generated from a private or public domain. For instance, in *Uzun v Germany*, the ECtHR held that the files collected by security services on a particular individual, even without the use of covert surveillance methods, constituted an interference with their private life.³³⁹

The ECtHR has also emphasized that the mere collection and retention of data constitute an interference with the right to privacy, regardless of whether government officials subsequently access or use the data.³⁴⁰ A similar conclusion has been reached by the OHCHR in relation to metadata.³⁴¹ The OHCHR argues that any collection of metadata is potentially an interference with privacy, and their collection and retention is an interference with privacy regardless of subsequent access or use.³⁴²

34/7.

³³⁷ See *Big Brother [GC]*, *supra* note 220 at paras 3, 6-8 Lemmens, Vehebović, and Bošnjak JJ, partly concurring.

³³⁸ *Big Brother [GC]*, *supra* note 220 at par 3 Lemmens, Vehebović, and Bošnjak JJ, partly concurring.

³³⁹ *Uzun*, *supra* note 309 at par 46. See also *P.G.*, *supra* note 311 at par 57.

³⁴⁰ In *S and Marper v. United Kingdom*, for instance, the Grand Chamber of the ECtHR held that “the mere storing of data relating to the private life of an individual’s amount to an interference within the meaning of Article 8.” ECtHR [GC], 2008, *S and Marper v The United Kingdom*, no 30562/04 and 30566/04 at par 67. See also ECtHR [GC], 2021, *Big Brother Watch and Others v the United Kingdom*, Application No. 58170/13, 62322/14, 24960/15 at par 330.

³⁴¹ For more details see Part III-B, *below*.

³⁴² See OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 26.

The evolution of privacy as a human right has been shaped not only by legal interpretations and philosophical debates, but also by technological advances. As digital technologies emerged and began to reshape societal and governmental functions, new dimensions of privacy came to the forefront—most notably the protection of personal information. As will be explained in the following paragraphs, this shift became particularly evident with the advent of large-scale data processing systems, which gave rise to the concept of information privacy and raised concerns about the implications of automated data collection and storage.

A. Privacy and Data Banks: Information Privacy

In the 1960s, when large computers became common and the use of information technology as tools for public administration emerged,³⁴³ the main privacy concern was the creation of a central national database.³⁴⁴ However, as David H. Flaherty explained, the avoidance of this scenario in the West resulted in a series of discrete databases that were not fully integrated by 1989.³⁴⁵ Since then, the landscape has changed significantly, with these discrete databases becoming increasingly interconnected, allowing data to flow almost seamlessly from one to another.

The evolution in data management coincided with growing concerns about the potential impact of automatic data processing on the right to privacy.³⁴⁶ In the late 1960s and the early 1970s, academics began to sound the alarm about the implications of centralized databases. They

³⁴³ See Simon G Davies, “Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity” in Philip Agre & Marc Rotenberg, eds, *Technology and Privacy: The New Landscape* (Cambridge, MA: MIT Press, 1997) 143 at 145.

³⁴⁴ See David H Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and United States*, (Chapel Hill: The University of North Carolina Press, 1989) at 3.

³⁴⁵ See Flaherty, *Protecting Privacy in Surveillance Societies*, *supra* note 344.

³⁴⁶ See James Michael, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*, (Paris: UNESCO, 1994) at 3.

argued that the ability to easily collect, store, and process information in these systems could lead to several problems: the retention of data beyond necessity or justification; the disclosure of information without the consent or knowledge of the individual;³⁴⁷ and the creation of detailed, accurate pictures of people's lives beyond what they or those close to them could provide.³⁴⁸

In response to these growing concerns, privacy became the subject of legislation in most developed countries.³⁴⁹ Inspired by Alan Westin's concept of privacy as control over personal information,³⁵⁰ from the 1970s onwards, lawmakers sought to establish a set of procedural safeguards to protect the rights of individuals to control the dissemination of information about themselves.

Building on this foundation, James Michael's 1994 study compared privacy and human rights in the light of the development of information technology. Michael identified "information privacy"—the notion that others should not obtain knowledge about others without their consent—as the aspect of privacy most affected and potentially threatened by recent technological advances.³⁵¹ This concept of information privacy continues to be central to international (and national) debates about the issues and risks posed by digital technologies and how they should be regulated.³⁵²

Westin's concept of information privacy has now been adopted by over 85 countries, and his set of data protection principles has become the cornerstone of global data protection

³⁴⁷ See Tom Gerety, "Redefining Privacy", *supra* note 295 at 287; Richard A Wasserstrom, "Privacy: Some Arguments and Assumptions" in Ferdinand D Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, UK: Cambridge University Press, 1984) 317 at 326.

³⁴⁸ See Wasserstrom, "Privacy", *supra* note 347 at 326.

³⁴⁹ See e.g., Michael, *Privacy and Human Rights*, *supra* note 346 at 53–118.

³⁵⁰ See Alan F Westin, *Privacy and Freedom*, (New York: Atheneum, 1967) at 7.

³⁵¹ See Michael, *Privacy and Human Rights*, *supra* note 346 at 3.

³⁵² See e.g., OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 5.

regulations.³⁵³ It is also present in two early frameworks drafted specifically to protect information privacy: the OECD’s *Guidelines on the Protection of Personal Privacy and Transborder Flow of Personal Data*,³⁵⁴ and the Council of Europe’s *Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data*.³⁵⁵

While the history of data protection frameworks and their role in regulating corporate surveillance practices is developed in detail in Chapter V,³⁵⁶ it is important to note that, in the context of digital technologies, human rights bodies have interpreted the right to privacy to include information privacy. In the UN system, for instance, information privacy has been defined as the right of individuals to know who holds information about them, and how that information is used.³⁵⁷ This definition covers information that exists or can be inferred about a person and her or his life, as well as decisions made on the basis of that information.³⁵⁸ Furthermore, the right to information privacy is not only impacted by the examination or use of information about a person by a human or an algorithm,³⁵⁹ but also by the mere generation and collection of data relating to a person’s identity, family or life, which, as the OHCHR has states, “Through those steps an individual loses some control over information that could put his or her privacy at risk.”³⁶⁰

As will be argued in the following chapters, this aspect of privacy—information privacy—has been the main focus of analysis in cases related to the use of digital technologies by

³⁵³ See e.g., Steeves, “Now You See Me”, *supra* note 24.

³⁵⁴ OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (Paris: OECD, 2001).

³⁵⁵ *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, 1496 UNTS 65 (entered into force: 1 October 1981).

³⁵⁶ See Chapter V-I, *below*.

³⁵⁷ See UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14 at 22.

³⁵⁸ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 5.

³⁵⁹ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 7.

³⁶⁰ OHCHR, *Right to Privacy (2018)*, *supra* note 17.

corporations. However, it is crucial to recognize that privacy as a human right encompasses more than just the flow and control of personal information.³⁶¹

III. International Human Rights Framework and Government-Led Surveillance

In the *General Comment No. 16*, the CCPR provides that “surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wiretapping and recording of conversations, should be prohibited.”³⁶² However, the right to privacy is not an absolute; it is a qualified right. This means that in certain cases, interference with this right may be justified.³⁶³ In some circumstances, the right to privacy can be restricted or limited. For instance, in *Klass v Germany*,³⁶⁴ the ECtHR accepted that in a democratic society, the existence of legislation granting powers of secret surveillance is necessary “under exceptional conditions,” in particular in the “interest of national security and/or for the prevention of disorder or crime.”³⁶⁵

When privacy is restricted, states are granted a degree of discretion, often referred to as a “margin of appreciation,” to determine the type of surveillance scheme that is necessary.³⁶⁶ This

³⁶¹ See Part II, *above*.

³⁶² OHCHR, *General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)*, CCPR, 32th Sess, UN Doc HRI/GEN/1/Rev.9 (Vol. I) (1988) at par 8.

³⁶³ See e.g., OHCHR, *General Comment No. 16*, *supra* note 362 at par 7.

³⁶⁴ This was an early case where the ECtHR had to consider whether the German system of intercepting telephone communications was an unjustifiable interference with privacy. *Klass and Others v Germany*, No 5029/71 (6 September 1978) [*Klass*].

³⁶⁵ *Klass*, *supra* note 364 at par 48.

³⁶⁶ The margin of appreciation doctrine “establishes a methodology for scrutiny by international courts of the decisions of national authorities – i.e., national governments, national courts and other national actors.” Yuval Shany, “Toward a General Margin of Appreciation Doctrine in International Law?” (2005) 16:5 *European Journal of International Law* 907–940, online: <<https://doi.org/10.1093/ejil/chi149>> at 909. See also Antoinette Scherz, “How

discretion extends to decisions such as whether to implement a mass surveillance regime to identify threats to national security or to protect essential national interests.³⁶⁷

Nevertheless, this discretion is not absolute. The surveillance regime chosen by the state must meet certain requirements and include certain safeguards. These measures are essential to ensure that any interference with the right to privacy is necessary in a democratic society.³⁶⁸ Consequently, surveillance laws or measures must comply with the principles of legality, necessity, proportionality, and adequate safeguards.³⁶⁹

The implementation of appropriate safeguards is essential to avoid arbitrary or unlawful interference with privacy, which could undermine accountability and facilitate abuse.³⁷⁰ A key distinction in this context is between targeted and mass surveillance systems. Targeted surveillance often requires prior authorization, either by the judiciary or the executive,³⁷¹ to review the necessity

Should Personal and Political Autonomy Feature in the ECtHR's Margin of Appreciation?" (2023) 5:2 *Jus Cogens* 149–170, online: <<https://doi.org/10.1007/s42439-023-00079-8>>.

³⁶⁷ See *Centrum För Rättvisa v Sweden* [GC], No 35252/08 (25 May 2021) at par 254 [*Centrum För Rättvisa* [GC]].

Governments around the world have invoked national security as a rationale for expanding their surveillance capabilities, exploiting the vagueness of its definition and the lack of concrete limits on the conditions for exceptional state surveillance. In this context, Lisa Austin explains that, from a rule of law perspective, these circumstances can be characterised as 'lawful illegality', where the legal exception goes beyond what is deemed necessary and proportionate to uphold the rule of law. See e.g., Lisa M Austin, "Surveillance and the Rule of Law" (2015) 13:2 *Surveillance & Society* 295; Lisa M Austin, "Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (University of Ottawa Press, 2015) 103.

³⁶⁸ See *Centrum För Rättvisa* [GC], *supra* note 367; *Big Brother* [GC], *supra* note 220.

³⁶⁹ See OHCHR, *General Comment No. 16*, *supra* note 362 at paras 7, 8; Huvig, *supra* note 285 at par 26; Escher, *supra* note 199 at paras 116, 129; UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14 at par 28.

See also Paul De Hert & Gianclaudio Malgieri, "One European Legal Framework for Surveillance: The ECtHR's Expanded Legality Testing Copied by the CJEU" in Valsamis Mitsilegas & Niovi Vavoula, eds, *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart Publishing, 2021) 255; Elspeth Guild, "Mapping Limitations on State Surveillance through the UN Human Rights Instruments" in Valsamis Mitsilegas & Niovi Vavoula, eds, *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart Publishing, 2021) 217.

³⁷⁰ See OHCHR, *Right to Privacy* (2014), *supra* note 251 at par 37; UN, *Report of Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, GA, 69th Sess, UN Doc A/69/397 (2014) at par 45.

³⁷¹ See e.g., UN, *SR Human Rights and Fundamental Freedoms while Countering Terrorism* (2014), *supra* note 370 at par 47; OHCHR, *Right to Privacy* (2018), *supra* note 17 at paras 38–40.

and proportionality of the measures before they are carried out. This review typically takes into account the specific circumstances of the case and the individual or organization that would be subject to surveillance.³⁷²

In contrast, mass surveillance systems present unique challenges due to their broad scope and lack of individualized suspicion.³⁷³ Unlike targeted surveillance, mass surveillance does not allow for case-by-case, prior review. Instead, the *ex-ante* review of mass surveillance is generally limited to authorizing the system as a whole, rather than its application to a specific individual.³⁷⁴ This fundamental difference in the review process has been identified as a key reason why mass surveillance systems are often found to be incompatible with international human rights law.³⁷⁵

The next sections examine how government-led surveillance is analyzed and addressed within the international human rights framework, focussing on its potential to intrude on privacy and the limitations imposed by human rights principles. Specifically, the next sections examine three types of surveillance practices: mass surveillance, mandatory data retention, and geolocation surveillance. What these practices have in common is that they rely on the collection and use of automated data generated by digital technologies.

A. Mass Interception Regimes

Since the use of the first form of remote communication, states have sought to intercept and monitor the private communication of individuals to serve law enforcement and national

³⁷² See e.g., UN, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, HRC, 41th Sess, UN Doc A/HRC/41/35 (2019) at paras 21-26.

³⁷³ See Part I-A, *above*.

³⁷⁴ See UN, *SR Human Rights and Fundamental Freedoms while Countering Terrorism* (2014), *supra* note 371 at par 47.

³⁷⁵ See Part III-A., *below*.

security interests.³⁷⁶ Today, however, governments not only intercept communications that take place on in private infrastructure, but they also rely on private companies to access various types of data that companies collect as part of their day-to-day operations.

Technological advances have enabled the simultaneous generation, collection, and processing of vast amounts of data on a large number of individuals. This has allowed the government to shift from the targeted surveillance based on reasonable suspicion of specific individuals to the indiscriminate mass collection and use of data on entire populations.³⁷⁷

The implications of this shift are significant. The UN and the ECtHR have argued that the mere existence of a mass surveillance program (or legislation authorizing the practice) constitutes an interference with privacy,³⁷⁸ with a potential chilling effect on rights such as freedom of expression and associations.³⁷⁹ In addition, mass surveillance not only limits individuals' capacity to freely and enthusiastically interact with others and participate in certain activities,³⁸⁰ but also imposes both internal and external pressures to conform, fostering submissiveness and deference.³⁸¹ There are also long-term risks associated with mass surveillance. The data generated and stored as a result of these programs could be misused, either by the government that mandated the surveillance or by future administrations and third parties.³⁸²

³⁷⁶ See UN, *SR Right to Freedom of Opinion and Expression*, *supra* note 14 at par 12.

³⁷⁷ See Part I-A., *above*, for more on this topic.

See also Marie-Helen Maras, "From Targeted to Mass Surveillance: Is The EU Data Retention Directive A Necessary Measure or An Unjustified Threat to Privacy?" in Benjamin J Goold & Daniel Neyland, eds, *New Directions in Surveillance and Privacy* (London: Willan Publishing, 2009) 74.

³⁷⁸ See e.g., OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 20; *Weber and Saravia v Germany*, No 54934/00, [2006] XI ECHR 309 at par 78 [*Weber*].

³⁷⁹ See e.g., OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 20; *Weber*, *supra* note 378 at par 78.

³⁸⁰ See e.g., *Big Brother [GC]*, *supra* note 220 at par 5 Lemmens, Vehebović, and Bošnjak JJ, partly concurring.

³⁸¹ See e.g., *Big Brother [GC]*, *supra* note 220 at par 6 Lemmens, Vehebović, and Bošnjak JJ, partly concurring.

³⁸² See e.g., UN, *Report of the Special Rapporteur on the Right to Privacy*, HRC, 34rd Sess, UN Doc A/HRC/34/60 (2017) at par 48.

In light of these concerns, international human rights bodies have taken a strong stance against mass surveillance. Within the UN human rights system, the HRC, the OHCHR, and various Special Rapporteurs have emphasized that mass surveillance is not acceptable under international human rights law because it precluded the possibility of conducting individualized necessity and proportionality analysis.³⁸³

On 18 December 2013, a few months after the Snowden revelations were made public, the UN General Assembly adopted Resolution 68/167 on the right to privacy in the digital age.³⁸⁴ This resolution expressed the international community's deep concern about the ability of governments to use new technologies for surveillance, interception, and data collection, potentially in violation of the ICCPR. Recognizing the need for further study, the resolution also requested the OHCHR to prepare a report on the protection of the right to privacy in both domestic and extraterritorial contexts, as well as in relation to the interception of digital communications and the collection of personal data.³⁸⁵

In response to this request, the OHCHR submitted the report *The Right to Privacy in the Digital Age*, which was adopted by the HRC on 30 June 2014.³⁸⁶ Building on the concerns raised in Resolution 68/167, the report delves deeper into the impact of technological advances on the right to privacy. The OHCHR acknowledged the positive impact of new technologies on daily life

³⁸³ See e.g., OHCHR, *Right to Privacy* (2018), *supra* note 17 at par 17; OHCHR, *Best Practices Protecting HHRR*, *supra* note 250 at par 58.

³⁸⁴ UN, *The Right to Privacy in the Digital Age*, GA, 68th Sess, UN Doc A/RES/68/167 (2013) GA Res 68/167. See also Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) 56:1 Harvard International Law Journal 81 (highlighting the relevance of the resolution in the international conversation on the application of human rights to mass surveillance).

³⁸⁵ See UN, *Right to Privacy* (GA, 2013), *supra* note 384 par 5.

³⁸⁶ OHCHR, *Right to Privacy* (2014), *supra* note 251.

For an analysis of the importance of this report see Guild, "Mapping Limitations on State Surveillance", *supra* note 369.

around the world, but also noted that these innovations have expanded the ability of states and others to conduct surveillance and data collection.³⁸⁷ This analysis highlighted a worrying trend: governments' interest in mass surveillance was becoming a dangerous habit rather than an exceptional measure.³⁸⁸

The report emphasized that the existence of a mass surveillance programs constitutes an interference with privacy, and therefore the onus is on the state to demonstrate that such interference is neither arbitrary nor unlawful.³⁸⁹ In order to justify surveillance practices, states must demonstrate compliance with the principles of legality, proportionality, and necessity.³⁹⁰ After analyzing these principles, the report concluded that mass or bulk surveillance programs, even when they are intended to serve a legitimate purpose and have been implemented within an accessible legal framework, can be considered arbitrary because they lack both necessity and proportionality.³⁹¹

Building on these findings, subsequent reports by the OHCHR and Special Rapporteurs have reinforced this perspective.³⁹² In the same year, for example, the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism argued that mass surveillance was inconsistent with the principle that states should adopt the least intrusive means available when interfering with protected human rights.³⁹³ Central to this

³⁸⁷ See OHCHR, *Right to Privacy (2014)*, *supra* note 251 at paras 1-2.

³⁸⁸ See OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 3.

³⁸⁹ See OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 20.

³⁹⁰ See OHCHR, *Right to Privacy (2014)*, *supra* note 251 at paras 22-25.

³⁹¹ See OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 25.

³⁹² See e.g., OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 17; OHCHR, *Best Practices Protecting HHRR*, *supra* note 250 at par 58.

³⁹³ See UN, *SR Human Rights and Fundamental Freedoms while Countering Terrorism (2014)*, *supra* note 370 at paras 51-52.

argument is the fundamental principle of the right to privacy in communication, which request that any interference must be rare and justified on an individual basis. Consequently, it is contrary to established notions of privacy for states to collect all communications or metadata indiscriminately and continuously. Such a practice would constitute a potentially excessive interference with this right, undermining the very essence of privacy protection in the digital age.³⁹⁴

For its part, the ECtHR has acknowledged that surveillance, including mass surveillance, falls within the “margin of appreciation” of states under certain conditions. To ensure that this discretion is not abused, the Court has developed a set of minimum safeguards that should be included in the law authorizing surveillance. These safeguards, known as the *Huvig/Weber* minimum safeguards, include a regulatory framework that has to clearly define: 1) the categories of persons whose communications may be intercepted; 2) the nature of the offences that may give rise to such an order; 3) the limit on the duration of interception; 4) the procedure to be followed for the examination, use, and storage of the data obtained; 5) the precautions to be taken when transmitting the data to other parties; and 6) the circumstance in which the intercepted data may or must be erased or destroyed.³⁹⁵

Originally developed in the context of an interception case, *Huvig v France*,³⁹⁶ these guidelines have subsequently been applied and developed by the ECtHR in cases of mass surveillance.³⁹⁷ In applying these guidelines, the Court has argued that there is no reason to apply different criteria for the foreseeability of rules governing the interception of individual

³⁹⁴ See UN, *SR Human Rights and Fundamental Freedoms while Countering Terrorism (2014)*, *supra* note 370.

³⁹⁵ See *Huvig*, *supra* note 285 at par 34; *Weber*, *supra* note 378 at par 95; *Roman Zakharov v Russia* [GC], No 47143/06, [2015] VIII ECHR 205 at par 231 [*Zakharov*].

³⁹⁶ *Huvig*, *supra* note 285.

³⁹⁷ See e.g., *Weber*, *supra* note 378; *Liberty and Others v the United Kingdom*, No 58243/00 (1 July 2008) at par 62 [*Liberty*].

communications and more general surveillance programs.³⁹⁸ Under this test, mass surveillance does not violate the ECHR, but the regulation must comply with all minimum safeguards.³⁹⁹

A turning point in the ECtHR's analysis of mass surveillance systems was marked by the cases of *Big Brother Watch and Others v. United Kingdom*⁴⁰⁰ and *Centrum för Rättvisa v. Sweden*.⁴⁰¹ In these cases, the ECtHR introduced a new approach by analyzing the bulk or mass surveillance regimes as a gradual process consisting of four stages, beginning with the interception and initial retention of data.⁴⁰²

Based on this framework, the Court found that individuals' rights to privacy were violated from the outset, with the degree of interference increasing as the process progressed.⁴⁰³ Despite this finding, the judgment of the Grand Chamber of the ECtHR reveals a nuanced perspective on mass surveillance. While the Court found violations of Article 8 of ECHR (right to private life), it also reaffirmed the importance of such surveillance methods.

In particular, the ECHR's decision emphasized not only that mass surveillance falls within the broad discretionary powers of states to protect national security, but also that it is of "vital

³⁹⁸ See *Liberty*, *supra* note 397 at par 63.

³⁹⁹ See De Hert & Malgieri, "One European Legal Framework", *supra* note 369 at 293; Lusine Vardanyan & Václav Stehlík, "Is the Case Law of ECtHR Ready to Prevent the Expansion of Mass Surveillance in the Post-Covid Europe?" (2020) 7 *European Studies* 253.

⁴⁰⁰ The applications on this case were presented as a result of Edward Snowden revelations about programs of surveillance and intelligence sharing between the USA and the United Kingdom. In addition to bulk interception, the case also dealt with the receipt of intercept material from foreign governments and intelligence agencies; and the obtaining of communications data from communication service providers. *Big Brother [GC]*, *supra* note 220.

⁴⁰¹ This case pertained to the Swedish bulk interception regime. The applicants argued that the foundation's communications had been or would be intercepted and examined by way of signals intelligence, as it communicated on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax, often on sensitive matters. *Centrum För Rättvisa [GC]*, *supra* note 367.

⁴⁰² The four stages were: (1) Interception and initial retention of communications and related metadata; (2) Application of specific selectors to the retained data; (3) Examination of selected data analysts; and (4) Subsequent retention of data and use of the 'final product,' which includes sharing of data with third parties. *Big Brother [GC]*, *supra* note 220 at par 325; *Centrum För Rättvisa [GC]*, *supra* note 367 at par 239.

⁴⁰³ See *Big Brother [GC]*, *supra* note 220 at par 325; *Centrum För Rättvisa [GC]*, *supra* note 367 at 239.

importance to Contracting States in identifying threats to their national security.” The Court went further, stating that “no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power.”⁴⁰⁴ This reasoning effectively rejected the arguments made by privacy activists and the OHCHR since the Snowden revelations, which claimed that such surveillance programs were inherently disproportionate.⁴⁰⁵ As a result, some scholars have argued that these rulings effectively normalize mass surveillance.⁴⁰⁶

However, in his partial dissent, Judge Pinto de Albuquerque contended that the majority overlooked the widespread agreement that mass surveillance should be prohibited. This is not only because it is disproportionate, but also because indiscriminate mass surveillance of communications has been demonstrated to be ineffective in preventing terrorism, and is therefore a threat to the protection of human rights and a waste of resources.⁴⁰⁷ He went on to criticize the majority judgment, arguing that the Court had surrendered to the *fait accompli* of mass surveillance

⁴⁰⁴ *Big Brother [GC]*, *supra* note 220 at par 424; *Centrum För Rättvisa [GC]*, *supra* note 367 at par 365.

⁴⁰⁵ For more on this reasoning by the OHCHR see the text accompanying note 393, *above*.

For more on this reasoning by privacy scholars see e.g., Alberto Cerda, “The Myth of Global Online Surveillance Exempted From Compliance with Human Rights” in *Global Information Society Watch 2014: Communications Surveillance in the Digital Age* (APC and Hivos, 2014) 25; Katitza Rodriguez, Cindy Cohn & Karen Gullo, “European Court on Human Rights Bought Spy Agencies’ Spin on Mass Surveillance” (26 May 2021) online: <eff.org> [<http://web.archive.org/web/20231221151759/https://www.eff.org/deeplinks/2021/05/european-court-human-rights-bought-spy-agencies-spin-mass-surveillance>]; Drew Mitnick, “UN Special Rapporteur Report on Mass Surveillance: Much to Like, Some to Debate” (17 October 2014) online (blog): <www.accessnow.org> [<http://web.archive.org/web/20230927124030/https://www.accessnow.org/un-special-rapporteur-report-on-mass-surveillance-much-to-like-some-to-deba/>].

⁴⁰⁶ See e.g., Monika Zalnieriute, “A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence” (4 June 2021) online (blog): <ejiltalk.org> [<http://web.archive.org/web/20231221143013/https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/>]; Marko Milanovic, “The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa” (26 May 2021) online (blog): <ejiltalk.org> [<http://web.archive.org/web/20230603080359/https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/>]. See also Vera Rusinova, “Privacy and the Legalisation of Mass Surveillance: In Search of A Second Wind for International Human Rights Law” (2022) 26:4 International Journal of Human Rights 740.

⁴⁰⁷ See *Big Brother [GC]*, *supra* note 220 at par 11 Pinto de Albuquerque J, partly dissenting.

by accepting that if it is useful, it should be allowed. But in a democratic society, utility is not synonymous with necessity or proportionality.⁴⁰⁸

In *Big Brother* and *Centrum för Rättvisa*, the majority of the ECtHR argued that the technological advances since cases such as *Weber* and *Liberty*, as well as key differences between targeted and mass surveillance, justified a departure from previous case law, including the minimum standards set out in *Hivig/Weber*.⁴⁰⁹ In place of these earlier standards, the Court proposed a new framework consisting of eight categories to be clearly defined in national legislation.⁴¹⁰

While these new requirements could be seen as a welcome development, they fall short of addressing the heightened risks posed by modern surveillance technologies. The Court has previously recognized the need to adapt safeguards in response to the growth of government surveillance powers, in particular, the automated and systematic collection of data that allows governments to amass vast amounts of data on individuals. For instance, in *Szabó and Vissy v. Hungary*,⁴¹¹ the ECtHR acknowledged that existing case law on interception needed to be strengthened to meet the challenges posed by technologically advance surveillance practices.⁴¹² However, in this case, the Court declined to fully address the issue on the grounds that Hungary's

⁴⁰⁸ See *Big Brother [GC]*, *supra* note 220 at par 58 Pinto de Albuquerque J, partly dissenting.

⁴⁰⁹ See e.g., *Centrum För Rättvisa [GC]*, *supra* note 368 at paras 255-60; *Big Brother [GC]*, *supra* note 217 at paras 341-46.

⁴¹⁰ See *Big Brother [GC]*, *supra* note 220 at par 361; *Centrum För Rättvisa [GC]*, *supra* note 367 at par 275.

⁴¹¹ This case concerned the Hungarian legislation on secret anti-terrorism surveillance enacted in 2011. The applicants complained about the potential for unjustified and excessively intrusive measures under the Hungarian legal framework for secret surveillance in the interest of national security. They claimed that this legal framework was susceptible to abuse due to a lack of judicial oversight. *Szabó and Vissy v Hungary*, No 37138/14 (12 January 2016) [*Szabó*].

⁴¹² See e.g., *Szabó*, *supra* note 411 at par 68.

system of safeguards was inadequate and did not even comply with the principles previously established in the case law.⁴¹³

Despite recognizing the need for stricter criteria to take account of the increasingly intrusive nature of current mass surveillance capabilities of governments,⁴¹⁴ the ECtHR's analysis in *Big Brother* and *Centrum för Rättvisa* has not strengthened safeguards. On the contrary, it has effectively weakened the safeguards.⁴¹⁵ As a result, the new framework allows mass surveillance practices that indiscriminately target every citizen to more easily comply with the ECHR.⁴¹⁶

Although *Big Brother Watch* and *Centrum för Rättvisa* represent a shift in the ECtHR's acceptance of mass surveillance, it is important to note that the Court still views surveillance practices as posing high risk to individuals and society. Therefore, domestic regulations must meet certain minimum requirements aimed at reducing these risks, including the abuse of power. Despite the greater acceptance shown by the majority of the ECtHR in these two cases, as the dissenting opinion suggests, this is hopefully a turning point that will be corrected in future cases.⁴¹⁷

In summary, the OHCHR and the ECtHR have taken different positions on mass surveillance. The OHCHR, along with other UN human rights bodies, has opposed mass surveillance, arguing that it is inconsistent with international human rights law. They maintain that

⁴¹³ See *Szabó*, *supra* note 411 at par 70.

⁴¹⁴ See e.g., *Centrum För Rättvisa [GC]*, *supra* note 367 at par 261; *Big Brother [GC]*, *supra* note 220 at par 347.

⁴¹⁵ See *Big Brother [GC]*, *supra* note 217 Lemmens, Vehebović, and Bošnjak JJ, partly concurring; *Big Brother [GC]*, *supra* note 217 Pinto de Albuquerque J, partly dissenting. See also Rodriguez, Cohn & Gullo, "ECtHR Bought Spy Agencies", *supra* note 406.

⁴¹⁶ See *Big Brother [GC]*, *supra* note 220 at par 59 Pinto de Albuquerque J, partly dissenting; De Hert & Malgieri, "One European Legal Framework", *supra* note 369 at 289–92.

⁴¹⁷ See *Big Brother [GC]*, *supra* note 220 at par 30 Lemmens, Vehebović, and Bošnjak JJ, partly concurring ("One may hope that in future cases raising questions of concrete interference with the rights of specific individuals, the Court will interpret and further develop the principles in a way which will properly uphold democratic society and the values it stands for").

such practices constitute an interference with privacy and cannot be justified because they lack necessity and proportionality. The OHCHR stresses that any surveillance should be rare, individually justified and subject to strict oversight. In contrast, the ECtHR has taken a more nuanced approach. While recognizing that mass surveillance interferes with the right to privacy, the Court has held that such practices may fall within the “margin of appreciation” of states, provided that certain safeguards are in place. The ECtHR has developed a set of minimum requirements for surveillance laws and has recognized the importance of mass surveillance for national security. This stance has been criticized by some as effectively normalizing mass surveillance.

Having examined the contrasting positions of the OHCHR and the ECtHR on mass surveillance, the following section examines the concept of metadata, its importance in surveillance programs, and the implementation of mandatory data retention regimes by governments.

B. Metadata and Mandatory Data Retention Regimes

As part of mass surveillance programs, governments also seek communications data (metadata).⁴¹⁸ As the ECtHR noted in *Szabó*, metadata can provide information about the context in which the primary data were acquired by the authorities, such as the time, location, and devices used to create computer files, digital images, electronic messages, and other comparable data.⁴¹⁹

⁴¹⁸ Bruce Schneier argued that “metadata equals surveillance.” See Bruce Schneier, “Metadata Equals Surveillance” (23 September 2013) online (blog): <schneier.com> [http://web.archive.org/web/20230925103941/https://www.schneier.com/blog/archives/2013/09/metadata_equals.html], quoted by Lyon, “Surveillance, Snowden, and Big Data”, *supra* note 224 at 3.

⁴¹⁹ See *Szabó*, *supra* note 411 at par 68.

Recognizing the value of this contextual information, many governments have introduced mandatory data retention regulations. These regulations require service providers to store metadata about their customers' communications and location for potential access by law enforcement and intelligence agencies.⁴²⁰ This practice has become a recurring feature of surveillance regimes in many states, highlighting the importance of metadata in various contexts, including criminal and national security investigations.

The ECtHR has consistently held that the acquisition of metadata constitutes an interference with the right to privacy. Initially, the Court considered the acquisition of metadata to be less intrusive than the acquisition of the content of the communication, as illustrated in *Malone v United Kingdom*.⁴²¹ In this case, the ECtHR ruled on the sharing of data obtained from metering.⁴²² The Court acknowledged that the metering records were less intrusive than the content of the intercepted communications. Nevertheless, the Court held that the disclosure of such data to the police “without the consent of the subscriber” still amounted to an interference with the right guaranteed by Article 8 of the ECHR. This decision was based on the recognition that metering records “contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone.”⁴²³

⁴²⁰ OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 26.

⁴²¹ See *Malone v the United Kingdom*, No 8691/79 (2 August 1984) at par 56 [*Malone*].

⁴²² This was process that involves the use of a device called a meter check printer which register the numbers dialled on a particular telephone and the time and duration of each call. This process was designed by the British Communication (previously Post Office) for its own purposes, which included: “ensuring that the subscriber is correctly charged, investigating complaints of poor-quality services and checking possible abuse of the telephone service. In making such record the British Communications, “makes use only of signals sent to itself.” *Malone*, *supra* note 421.

⁴²³ *Malone*, *supra* note 421 at par 84.

The rapid development of digital technologies and the increased generation of metadata, coupled with improved analytical capabilities,⁴²⁴ has blurred the distinction between metadata and communications content. This shift is due to the vast amount of metadata being created and the wealth of information that these can reveal.⁴²⁵ The ECtHR has emphasized that metadata can reveal significant personal information and that their mass collection could significantly increase interference with the right to privacy. This is because metadata can be analyzed to create an in-depth portrayal of individuals by tracking their social networks, location, Internet browsing, communication patterns, and associations.⁴²⁶

This view has also been supported by the OHCHR, which has stated that the aggregation of metadata “may give an insight into an individual’s behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.”⁴²⁷ Given the private and sensitive nature of metadata, the legitimacy of mandatory retention regulations has been challenged under international human rights law.

These regulations typically require companies to collect and store metadata about their users for long periods of time, primarily to ensure future accessibility.⁴²⁸ As a result, such

⁴²⁴ Part I-A, *above*, explains this in more detail.

⁴²⁵ See e.g., *Big Brother [GC]*, *supra* note 220 at par 363. The ECtHR was not persuaded that the mass interception of related communications data may not necessarily be less intrusive than the acquisition of content. Therefore, it regards the interception, retention, and searching of such data as subject to the same safeguards as those applicable to content.

⁴²⁶ See *Big Brother [GC]*, *supra* note 220 at par 342. See also *Szabó*, *supra* note 411 at par 70 (recognizing that these data could be useful for the Government to create a detailed profile of citizens’ most intimate aspects of life, which “may result in particularly invasive interferences with private life”).

⁴²⁷ OHCHR, *Right to Privacy (2014)*, *supra* note 251 at par 19. See also UN, *Right to Privacy (2017)*, *supra* note 336.

⁴²⁸ See Privacy International, *National Data Retention Laws since the CJEU’s Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe*, (London: Privacy International, 2017) online: <privacyinternational.org> [http://web.archive.org/web/20231219153941/https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf] at 6.

regulations have “inevitably resulted in the State having everyone’s digital footprint.”⁴²⁹ The OHCHR has criticized these practices, arguing that they appear to be “neither necessary nor proportionate.”⁴³⁰ Similarly, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has highlighted that broad mandatory data retention regulations undermine an individual’s ability to remain anonymous while significantly expanding the state’s capacity to conduct surveillance.⁴³¹

The criticism that mandatory data retention regulations fail to meet the standards of necessity and proportionality is particularly noteworthy because it contrasts sharply with the practices of many corporations, even in the absence of legal mandates. Today, corporations routinely collect and retain large amounts of metadata, including location data, as part of their business operations. These practices are not only permitted, but often incentivized by economic and commercial interests, raising privacy concerns beyond government-led surveillance.⁴³²

In the light of these concerns, two judgments of the Court of Justice of the European Union (CJEU) are particularly relevant: *Digital Rights Ireland*⁴³³ and *Tele2/Watson*.⁴³⁴ Although the CJEU is not a human rights court per se, these two judgments have become key references in the

⁴²⁹ UN, *SR Right to Freedom of Opinion and Expression (2015)*, *supra* note 316 at para 55.

⁴³⁰ OHCHR, *Right to Privacy (2014)*, *supra* note 251 at para 26.

⁴³¹ See UN, *SR Right to Freedom of Opinion and Expression (2015)*, *supra* note 316 at par 55.

⁴³² This point will be developed in more detail in Chapter IV-III, *below*.

⁴³³ *Digital Rights Ireland Ltd and Others* [GC], C-293/12, [2014] ECLI:EU:C:2014:238 [*Digital Rights Ireland*]. This case deals with mass metadata surveillance by police within the context of criminal law, and the legality of the Data Retention Directive (Directive 2006/24/EC), which provided that traffic and location data and subscriber data needed to be kept by the service providers on behalf of the law-enforcement authorities.

⁴³⁴ *Tele2 Sverige AB and Others* [GC], C-203/15, [2016] ECLI:EU:C:2016:970 [*Tele2/Watson*]. In this case the CJEU was asked by Swedish and British courts respectively to consider the scope and effect of its judgement in the *Digital Rights Ireland* case.

context of mandatory metadata retention regulations, making their discussion essential to this thesis.⁴³⁵

In these two judgments, the CJEU reaffirmed that states may enact data retention regimes, provided that they comply with the principles of legality, necessity, and proportionality. In *Digital Rights Ireland*, the Court found that the EU Data Retention Directive⁴³⁶ failed to meet human rights standards because it lacked proportionality and necessity. The scope of the Directive was found to be too broad, covering all individuals, communications, and data without distinction.⁴³⁷ It also lacked adequate safeguards, failing to impose sufficient limitations on access by national authorities and to tailor the duration of data retention to the nature or category of crime being investigated.⁴³⁸

Building on this precedent, the *Tele-2/Watson* judgment reinforced the principles established in *Digital Rights Ireland* and provided additional guidance on the minimum safeguards necessary for national data retention legislation to comply with the EU law.⁴³⁹ The Court clarified that while the EU Charter does not prohibit a Member State from enacting legislation allowing for the targeted retention of traffic and location data as a preventive measure against serious crime, such retention must be strictly necessary in terms of the categories of data retained, the means of communication affected, the individuals concerned, and the retention period.⁴⁴⁰

⁴³⁵ De Hert and Malgieri argued that in these cases, the court tacitly followed the ECtHR's jurisprudence, including the application of the *Huvig/Weber* minimal requirements see De Hert & Malgieri, "One European Legal Framework", *supra* note 369 at 285–88.

⁴³⁶ EU, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention Of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*, [2006] OJ, L105/54 [*Data Retention Directive*].

⁴³⁷ See CJEU, *Digital Rights Ireland*, *supra* note 433 at paras 57-59.

⁴³⁸ See CJEU, *Digital Rights Ireland*, *supra* note 433 at paras 60-64.

⁴³⁹ See CJEU, *Tele2/Watson*, *supra* note 434 at paras 108-111.

⁴⁴⁰ See CJEU, *Tele2/Watson*, *supra* note 434 at para 134.

This section has highlighted the evolving understanding of the importance of metadata. Once perceived as less intrusive than communications content, metadata is now recognized for its ability to reveal highly personal and sensitive information. It has also explored the challenges posed by mandatory data retention regulations, their critique under international human rights law, and the contrasting role of corporate practices in the collection and retention of metadata.

Building on this discussion of metadata collection and retention in the context of mass surveillance programs, the next section turns to the final surveillance practice under analysis: geolocation surveillance.

C. Geolocation Surveillance Practices

As noted above, among the various types of data generated, intercepted, and obtained by the security services, personal location data are one of the most highly sought-after.⁴⁴¹ Recognizing the sensitivity of location data, the OHCHR has highlighted the privacy risks posed by the inferences that can be drawn from them.⁴⁴² Building on this concern, reports have further highlighted the potential risks associated with location data. For instance, there have been documented cases of such data, collected as part of surveillance programs, being used to locate targets for lethal drone strikes.⁴⁴³

Geolocation surveillance practices generally fall into two categories. First, the government may use location technologies such as GPS to actively track an individual. For example, law enforcement can install a GPS device on a car to monitor its movements in real time. Second, the

⁴⁴¹ See Part I-B, *above*

⁴⁴² See e.g., UN, *Report of the Special Rapporteur on the Right to Privacy*, by Joseph A. Cannataci, GA, 76th Sess, UN Doc A/76/220 (2021) at para 53.

⁴⁴³ See e.g., OHCHR, *Right to Privacy (2014)*, *supra* note 251 at para 14.

government can use metadata collected by corporations, such as telecommunications providers, to track an individual's past movements. In this scenario, law enforcement requests access to data already stored by these corporations, either as part of their routine business operations or under legal data retention obligations. Given the relatively low cost and ease of use of modern software, governments are incentivized to rely on third-party metadata rather than direct GPS tracking, which is often more resource intensive.⁴⁴⁴

Despite the widespread use of geolocation surveillance, international and regional human rights courts have rarely addressed these practices. One significant case is *Uzun v Germany*, decided in 2010, in which German law enforcement authorities secretly installed a GPS receiver in the applicant's car.⁴⁴⁵ The receiver allowed the Federal Office for Criminal Investigation to determine the car's location and speed once a minute. However, the data were only retrieved every other day in order to avoid detection of the receiver.⁴⁴⁶ Over a period of three months, the authorities systematically collected and stored data on the whereabouts and movements of the applicant.⁴⁴⁷ The ECtHR acknowledged that GPS surveillance interfered with the right to privacy under Article 8 of the ECHR.⁴⁴⁸ However, it concluded that GPS tracking was less intrusive than visual or acoustic surveillance, which could reveal more about a person's behaviour, opinions, or feelings.⁴⁴⁹

⁴⁴⁴ See e.g., Banksto & Soltani, "Tiny Constables and the Cost of Surveillance", *supra* note 255. See also Lyon, "Surveillance, Snowden, and Big Data", *supra* note 224.

⁴⁴⁵ See *Uzun*, *supra* note 309.

⁴⁴⁶ See *Uzun*, *supra* note 309 at para 12.

⁴⁴⁷ See *Uzun*, *supra* note 309 at para 51.

⁴⁴⁸ See *Uzun*, *supra* note 309 at para 52.

⁴⁴⁹ See *Uzun*, *supra* note 309. See also *Ben Faiza c France*, No 31446/12 (8 February 2018) at para 53 [*Ben Faiza*].

Eight years later, the ECtHR revisited geolocation surveillance in *Ben Faiza c. France*.⁴⁵⁰ This case concerned the use of two types of geolocation practices by French agents during a criminal investigation: real-time GPS tracking,⁴⁵¹ and retrospective cell tower location data provided by a telecommunications provider. The Court found that both practices constituted an interference with the right to privacy.⁴⁵² However, it found that real-time GPS tracking was significantly more intrusive than *ex-post* analysis of cell tower data, and therefore required stricter safeguards.⁴⁵³

With regard to real-time GPS tracking, the Court ruled that it violated Article 8 of the ECHR because the French government lacked a clear and foreseeable legal basis for this method of surveillance, and therefore it failed the legality test, and did not provide sufficient safeguards against abuse.⁴⁵⁴ In contrast, the *ex-post* retrieval of cell site data involved accessing previously stored information, making it less intrusive.⁴⁵⁵ The Court distinguished between real-time tracking and retrospective geolocation practices, emphasizing the greater privacy implications of the former.⁴⁵⁶

⁴⁵⁰ *Ben Faiza*, *supra* note 449. See also Katrien Keyaerts, “Ben Faiza v. France: Use of Cell Site Location Information by Police is Acceptable Interference with Right to Privacy” (2019) 5:1 European Data Protection Law Review 120.

⁴⁵¹ The Court acknowledged that real-time geolocation tracking is a specialized investigative technique that enables the movement of a person or object to be monitored in real-time. This can be achieved through two methods: dynamic tracking of a telecommunications terminal using phone, tablet or GPS-equipped vehicle technology, or by installing a hardware device directly on a means of transport or other object, such as a beacon. See *Ben Faiza*, *supra* note 449 at para 53.

⁴⁵² See *Ben Faiza*, *supra* note 449 at paras 55-53, 67-68.

⁴⁵³ See *Ben Faiza*, *supra* note 449 at para 74.

⁴⁵⁴ See *Ben Faiza*, *supra* note 449 at paras 56-61.

⁴⁵⁵ See *Ben Faiza*, *supra* note 450 at para 67.

⁴⁵⁶ See *Ben Faiza*, *supra* note 449 at para 74.

Two key points emerge from these cases. First, *Ben Faiza* reinforced the conclusion in *Uzun* that GPS surveillance should be considered to be less intrusive than visual or acoustic methods because it reveals less information about a person's behaviour, opinions, or feelings. Second, *Ben Faiza* introduced a new dimension to the assessment: the timing of the surveillance. Real-time GPS tracking is significantly more intrusive than retrospective geolocation, such as the analysis of historical cell site data.⁴⁵⁷

This distinction is surprising. It overlooks the intrusive potential of historical location data, which can enable governments to draw detailed inferences about an individual's lifestyle, habits, and associations.⁴⁵⁸ Despite the Court's recognition in previous cases of the sensitive nature of location data,⁴⁵⁹ *Ben Faiza* did not fully address the privacy risks posed by the aggregation and analysis of historical data.

Finally, in *Ben Faiza*, the Court distinguished between two methods of generating geolocation data. The first involves real-time tracking through dynamic surveillance systems, such as GPS beacons or telephone line monitoring. The second involves access to previously stored data, such as cell site records held by corporations. While the Court recognized this distinction, it did not explore its wider implications.⁴⁶⁰ This omission is surprising, given the Court's previous

⁴⁵⁷ See also De Hert & Malgieri, "One European Legal Framework", *supra* note 369 at 273–275.

⁴⁵⁸ See Leszczynski, "Spatial Big Data", *supra* note 262.

See also Chapter IV-III.A, *below*, for a discussion of the different technological capabilities made possible by location technologies.

⁴⁵⁹ See e.g., Szabó, *supra* note 411 at para 49; FIDIS, "Mobility and Identity: Future of IDentity in the Information Society" (2006) online: <fidis.net> [<http://web.archive.org/web/20231221121811/http://www.fidis.net/resources/fidis-deliverables/mobility-and-identity/>]; "The Life of National Councillor Balthasar Glättli Under Surveillance: Interactive Visualisation of Data Retention in Switzerland" (26 April 2014) online (Digitale Gesellschaft): <<https://www.digitale-gesellschaft.ch/2014/04/27/the-life-of-national-councillor-balthasar-glaettli-under-surveillance-interactive-visualisation-of-data-retention-in-switzerland/>>.

⁴⁶⁰ See *Ben Faiza*, *supra* note 449 at para 74.

recognition of the potential privacy risks posed by the government's ability to access sensitive location data through interception or retention regimes.

This part has examined the international human rights framework's response to state surveillance practices, focussing on mass surveillance, mandatory data retention, and geolocation monitoring. The analysis underscores how technological advances have dramatically expanded state surveillance capabilities, heightening concerns about privacy and the balance between security and individual freedoms. International human rights bodies, particularly those within the UN system, have consistently argued that mass surveillance is incompatible with human rights law, emphasizing its failure to meet the standards of necessity and proportionality. In contrast, the ECtHR has taken a different approach, recognizing the security imperatives behind such practices while stressing the critical need for robust safeguards to prevent abuses.

Several key issues emerge from this review. The increasing reliance on metadata in surveillance has blurred the traditional distinction between content and contextual data, as both can now reveal highly sensitive personal information. Meanwhile, mandatory data retention regimes have been heavily criticized for their broad and indiscriminate scope, with courts calling for more tailored and proportionate solutions. In the context of geolocation surveillance, the ECtHR has drawn a distinction between real-time tracking, which is considered significantly more intrusive, and retrospective access to historical location data. Despite this distinction, concerns persist about the privacy risks associated with aggregated location data.

IV. Conclusion

The use of digital technologies by the government in the mass collection, retention, and tracking of data about individuals raise significant privacy concerns that require clear regulation and limitations, as evidenced by jurisprudence of regional human rights courts. While these

surveillance practices are considered necessary for the proper functioning of democracy, they interfere with privacy and other human rights, requiring the establishment of safeguards within the international human rights framework.

The surveillance capabilities that digital technologies provide to governments are also used by some corporations. The following chapters will argue that corporate surveillance also poses significant risks to privacy and society, and warrants a strong regulatory framework to limit it. They will highlight that despite their similarities, the international human rights framework has approached government and corporate practices differently.

As David Lyon points out, surveillance is always tied to specific purposes that would define the type of data that each organization seeks to collect and how it will use that data.⁴⁶¹ For instance, in the case of governments, location technologies are typically used to investigate crime or potential threats to national security. In the case of corporations, the underlying purpose is profit, which may include using customer insights to improve their own services or selling data to third parties.⁴⁶²

The following chapter will continue to map the current socio-technical landscape, focussing on corporations as key actors. It will show that corporations that rely on business models driven by extensive data collection, processing, and analysis exhibit psychopathic tendencies consistent with Bakan's framework. The chapter will also discuss corporate mass dataveillance systems as a manifestation of this psychopathic personality, examining the economic system in which these corporations operate, how this influences the design and marketing of technology, and the risks involved.

⁴⁶¹ See David Lyon, *Surveillance Studies: An Overview*, (Cambridge, UK: Polity, 2007) at 15.

⁴⁶² See Chapter IV, *below*.

Chapter IV. Corporate Mass Dataveillance

Digital technologies enable organizations to conduct data-based surveillance, monitoring people through the data trails that their behaviour leaves behind them—a phenomenon known as dataveillance.⁴⁶³ These dataveillance systems are implemented and maintained by different organizations for different purposes. While the previous chapter focussed on government-led systems for crime investigation and national security, this chapter examines mass dataveillance systems implemented by corporations for profit.

Dataveillance is not the exclusive domain of governments; certain corporations also engage in this pervasive practice. Like government, some corporations have the capacity to implement and manage extensive and intrusive location-based surveillance systems.⁴⁶⁴ These location dataveillance systems routinely generate and collect data on individuals' movements and locations, creating records that are then processed and analyzed using algorithmic techniques. This analysis sorts people into predetermined categories based on their perceived risk and economic value.⁴⁶⁵

Initially driven by the marketing industry,⁴⁶⁶ these digital technologies were primarily used to tailor marketing campaigns based on the highest probability of success. Today, a wide range of corporations are using these systems to provide individuals with an experience that appears to be

⁴⁶³ For an explanation and definition on dataveillance, see the text accompanying note 233, *above*.

⁴⁶⁴ See Michael & Clarke, "Location and Tracking of Mobile Devices", *supra* note 31 at 220.

⁴⁶⁵ See Chapter III-I.B.2, *above*.

See also Gandy, *Panoptic Sort*, *supra* note 9; Clarke, "Dataveillance", *supra* note 236 at 499; Lyon, "Introduction", *supra* note 242.

⁴⁶⁶ See e.g., Wolfie Christl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*, (Vienna: Cracked Labs, 2017) online: <crackedlabs.org> [http://web.archive.org/web/20231218113532/https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf].

more tailored to their needs and wants, not only in terms of advertising, but also in terms of services and information.⁴⁶⁷ However, this personalized experience is ultimately an illusion because it is not tailored to the individual, but to the presumed needs and wants of a manufactured statistical group into which the individual has been placed by corporate algorithms.⁴⁶⁸

Corporate dataveillance systems, like their government counterparts, are problematic because they create a context of constant data generation and collection data about individuals. This increases the amount and granularity of data available to corporations and third parties that can be used to make predictions and inferences about individuals. In addition, these data are often fed into government surveillance systems,⁴⁶⁹ further extending their reach.

The risks associated with corporate dataveillance systems are even more pronounced than those associated with government surveillance. Unlike government systems, corporations have direct access to individuals through the same devices used to generate and collect data. This direct access allows corporations, generally unconstrained by constitutional protections, to send inputs directly to individuals. As this chapter will explain, this direct access can have a significant impact on individual's behaviours and decision-making.

These mass dataveillance systems form the basis of an economic model centred on the increased generation, collection, use, and trade of data about individuals and their environment.

⁴⁶⁷ See e.g., Christl, *Corporate Surveillance in Everyday Life*, *supra* note 466.

⁴⁶⁸ This will be developed in detail in Part III-B, *below*.

⁴⁶⁹ See Chapter III-I, *above*.

This new logic of accumulation has motivated the expansion of dataveillance technologies in society,⁴⁷⁰ and influenced the design of many digital devices and services.⁴⁷¹

In this socio-economic ecosystem, corporations play a key role in designing marketing, maintaining, and profiting from these mass dataveillance systems. For this reason, it is highly relevant to understand and consider the personalities of these actors. To do this, this thesis draws on Bakan's conception of the corporation and its role in society. Bakan argued that "the corporation is a pathological institution, a dangerous possessor of the great power it wields over people and societies."⁴⁷² This thesis argues that the current practice of some corporations to generate, collect, and process as much data as possible about individuals and their environment is a facet of corporate pathology.

This chapter is divided in three parts. Part I introduces Bakan's theory of the corporation as a psychopathic institution and examines how corporations with data-driven business models—in particular those that profit from selling technologies, products, and services that rely on the collection and processing of data about individuals and their behaviours—fit this concept. Part II examines Uber Technologies Inc. (Uber Inc.) and Meta Platforms Inc. (Meta Inc.) as corporations that offer location-based services and have a business model that relies on the collection, processing, and analysis of data. This part demonstrates that these corporations exhibit psychopathic tendencies consistent with Bakan's theory. Finally, Part III discusses mass

⁴⁷⁰ A second motivator has been the government's interests on increase knowledge and control over the population for various motives (e.g., efficiency, security) see James B Rule, "Privacy: The Longue Durée" in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 11.

⁴⁷¹ See also Gary T Marx, *Windows into the Soul: Surveillance and Society in an Age of High Technology*, (Chicago: University of Chicago Press, 2016).

⁴⁷² Bakan, *The Corporation*, *supra* note 1 at 1–2.

Similarly, Glasbeek argued that the structure of the corporation for profit is one of anti-social and criminal behaviour see Harry Glasbeek, *Wealth By Stealth: Corporate Crime, Corporate Law, and the Perversion of Democracy*, (Toronto: Between The Lines, 2002).

dataveillance systems as a facet of the psychopathic personality, describing the economic model in which these corporations operate, and the risks posed by these systems.

I. Corporations as Psychopathic Institutions

There is an ongoing debate in academia about the nature of the corporation and the appropriate balance between public and private interests in its regulation.⁴⁷³ Bakan proposes a provocative conceptualization of the corporation, which distinguishes between the institution and the people who manage it. He characterizes the corporation as having a psychopathic personality, describing it as “*singularly* self-interested and unable to feel genuine concern for others in any context.”⁴⁷⁴

For Bakan, all publicly traded corporations, even the most respected and socially responsible, share the same flawed institutional character, characterized by traits such as “obsession with profit and share prices, greed, lack of concern for others, and a penchant for breaking legal rules.”⁴⁷⁵ Recognizing these psychopathic traits is important for understanding the role of the corporation in society and for designing regulatory frameworks to mitigate its harmful effects on individuals and society.

This view of the corporation is rooted in the shareholder theory,⁴⁷⁶ which holds that the primary purpose of a corporation is to maximize the wealth of its shareholders. According to this

⁴⁷³ See e.g., Robert Yalden et al, *Business Organizations: Principles, Policies and Practice*, (Toronto: Emond Montgomery, 2008).

⁴⁷⁴ Bakan, *The Corporation*, *supra* note 1 at 57.

⁴⁷⁵ Bakan, *The Corporation*, *supra* note 1 at 86.

⁴⁷⁶ This is one of the dominant theories of the legal mandate of the corporation, where the “best interests of the corporation” is interpreted to mean the “best interests of the shareholders.” Another view interprets this to include other stakeholders such as employees and consumers. See e.g., Yalden et al, *Business Organizations*, *supra* note 473 at 43.

See also Chapter VI, *below*.

theory, corporate managers act as the agents of the shareholders and are legally bound to prioritize the generation of profits.⁴⁷⁷ Bakan argues that this arrangement is problematic because it constrains the manager's decision making. Their choices are inherently restricted by the legal mandate to pursue the corporation's self-interest—namely, to generate profits for shareholders. Bakan argues that this singular focus on self-interest is a key element of the psychopathic personality of the corporation, as it leads corporations to care only for themselves.

The legal structure of the corporation allows it to pursue its goals with a high degree of impunity, even when its actions harm workers, consumers, communities, or the environment. Such harm is often dismissed as an unavoidable consequence of corporate activity—an externality.⁴⁷⁸ This tendency to externalize its costs, Bakan argues, is a major contributor to many global social and environmental problems, and “makes the corporation a profoundly dangerous institution.”⁴⁷⁹ For example, some corporations have increased their profits by exploiting natural resources for economic gain, ignoring environmental consequences, while others have violated human rights through extensive dataveillance systems.

Starting from the premise that a corporation is a legal person, Bakan sought to answer the question of what kind of person it is. Using case studies of corporate harm, he compared the actions of corporations with the World Health Organization's criteria for psychopathy, and concluded that the actions of corporations resemble those of human psychopaths.⁴⁸⁰

⁴⁷⁷ See e.g., Yalden et al, *Business Organizations*, *supra* note 473.

⁴⁷⁸ See Bakan, *The Corporation*, *supra* note 1 at 71.

⁴⁷⁹ Bakan, *The Corporation*, *supra* note 1 at 70–71.

⁴⁸⁰ Bakan explored the behavioural characteristics of the corporation using a personality diagnostic checklist based on the World Health Organization's ICD-10's Manual of Mental Disorders DSM-IV. The initial six criteria were: Callous unconcern for the feelings of others; Incapacity to maintain enduring relationships; Reckless disregard for the safety of others; Deceitfulness: repeated lying and conning others for profit; Incapacity to experience guilt; Failure to conform to social norms with respect to lawful behaviours. See Bakan, Achbar & Abbott, “Corporation Documentary”, *supra* note 166 at 41:09.

In 2020, Bakan described the rise of the “new” corporation movement, which claims to shift corporate priorities beyond shareholder value to a commitment to all stakeholders.⁴⁸¹ This shift was marked by the 2019 Statement on the Purpose of a Corporation, signed by the CEOs of major US corporations.⁴⁸² As part of this movement, corporations rebranded themselves to proclaim their commitment to embed social and environmental values deeply and across all of their operations.⁴⁸³

Bakan criticizes this movement as superficial because the legal structure that gave corporations their pathological personality remains unchanged. He argues that this rebranding is just part of a new narrative that aims to improve the public image of corporations without really changing their main priority of “making money for themselves and their shareholders.”⁴⁸⁴ Bakan warns that this rebranding makes corporations more charming, and they use this charm to convince

In 2011 the American Psychiatric Association added the seventh criteria: “Use of seduction, charm, glibness, or ingratiation to achieve one’s ends.” Bakan, *New Corporation*, *supra* note 5 at 57.

⁴⁸¹ See Bakan, *New Corporation*, *supra* note 5 at 4; Bakan & Abbott, “New Corporation Documentary”, *supra* note 166 at 6:00.

⁴⁸² Business Roundtable, “Business Roundtable Redefines the Purpose of a Corporation to Promote ‘An Economy That Serves All Americans’” (19 August 2019) online: <[businessroundtable.org](https://www.businessroundtable.org)> [<http://web.archive.org/web/20231220143611/https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans>].

See also Bakan & Abbott, “New Corporation Documentary”, *supra* note 166 at 6:13; Maggie Fitzgerald, “The CEOs of Nearly 200 Companies just Said Shareholder Value is No Longer Their Main Objective”, *CNBC* (19 August 2019), online: <[cnn.com](https://www.cnn.com)> [<http://web.archive.org/web/20240102162049/http://web.archive.org/screenshot/https://www.cnn.com/2019/08/19/the-ceos-of-nearly-two-hundred-companies-say-shareholder-value-is-no-longer-their-main-objective.html>].

⁴⁸³ See Bakan, *New Corporation*, *supra* note 5 at 17. Deva also pointed out that this commitment to shift the way corporation do business do “not use the term ‘rights’ or ‘human rights’ even once. Therefore, even if a shift were to take place in practice in future, it is unlikely to be rights-based.” Surya Deva, “From Business or Human Rights to Business and Human Rights: What Next?” in *Research Handbook on Human Rights and Business* (Cheltenham: Edward Elgar Publishing, 2020) 1 at 8.

⁴⁸⁴ Bakan, *New Corporation*, *supra* note 5 at 27.

the public that they are benevolent, and that regulators and society can let down their guard and let them take control.⁴⁸⁵

The concept of “doing well by doing good”⁴⁸⁶—this is, “making money through social and environmental values rather than in spite of them”⁴⁸⁷—illustrates this shift. Bakan points out that as part of this movement, corporations invest heavily in marketing campaigns that emphasize their benevolence and concern for certain values or rights.⁴⁸⁸ However, this image is often at odds with their actions. While claiming to care about society and the environment, corporations lobby governments for fewer regulations and legal constraints, “leaving citizens to suffer the consequences of their profit-driven irresponsibility.”⁴⁸⁹

This part is divided into two sections. The first section details the seven pathological traits that Bakan identified as characteristic of corporations as psychopathic institutions, and highlights how these traits manifest themselves in corporate behaviour and decision-making. These traits reveal the extent to which corporations prioritize profit over ethical considerations and societal well-being. Following this analysis, the second section examines how these pathological traits are specifically reflected in corporations with data-driven business models. This section focusses on the unique challenges posed by corporations and startups that profit from the selling of technologies, services, and products that rely on the collection and processing of data about individuals and their behaviours, this section examines how their business models and practices align with the psychopathic corporate personality described by Bakan.

⁴⁸⁵ See Bakan, *New Corporation*, *supra* note 5 at 4.

⁴⁸⁶ Bakan, *New Corporation*, *supra* note 5 at ch 3.

⁴⁸⁷ Bakan, *New Corporation*, *supra* note 5 at 29.

⁴⁸⁸ See Bakan, *New Corporation*, *supra* note 5.

⁴⁸⁹ Bakan, *New Corporation*, *supra* note 5 at 88.

A. Pathological Traits of Corporations

Bakan identifies seven pathological traits that define corporations as psychopathic institutions, revealing the extent to which they prioritize profit over ethical considerations or societal well-being.

The first personality trait analyzed by Bakan is that corporations have a reckless disregard for the safety of others, which is evident in their irresponsible behaviour that puts their goals ahead of public safety.⁴⁹⁰ For example, Bakan pointed out that some corporations knew about the risks and dangers of certain synthetic components to humans and the environment, but decided to continue marketing them and even downplayed these risks to the public.⁴⁹¹

Building on this disregard for safety, the second pathological trait is that corporations relate to others in a superficial way. They “present themselves to the public in a way that is appealing to the public [but] in fact may not be representative of what th[e] organization is really like.”⁴⁹² This behaviour mirrors that of individuals with psychopathic tendencies, who charm people to conceal their dangerously self-centred personalities. Similarly, corporations may rely on corporate social responsibility programs to project an image of compassion and care, despite their inherent inability to empathize with anyone or anything beyond their own profit-driven interests.⁴⁹³

The third pathological trait is closely related to the first two: corporations often refuse to take responsibility for their actions and are incapable of feeling remorse. When they are caught

⁴⁹⁰ See Bakan, *The Corporation*, *supra* note 1 at 57.

⁴⁹¹ See Bakan, Achbar & Abbott, “Corporation Documentary”, *supra* note 166 at 28:00.

⁴⁹² Bakan, *New Corporation*, *supra* note 5 at 57.

⁴⁹³ See Bakan, *New Corporation*, *supra* note 5.

breaking the law, they simply pay fines and continue their previous behaviour.⁴⁹⁴ Bakan cites examples of corporations settling in court and paying damages, but never admitting guilt.⁴⁹⁵

The lack of accountability is reinforced by the fourth trait: a lack of empathy. Corporate behaviour shows a disregard for the people affected by their actions.⁴⁹⁶ For example, clothing manufacturers in poor countries hire people, often underage children, and pay them outrageously low wages to produce goods that are then sold at much higher prices.⁴⁹⁷

Closely related to this lack of empathy is the fifth trait: failure to conform to the social norms of lawful behaviour or asocial tendencies. Bakan illustrates this with examples of numerous fines paid by corporations for violating various laws and regulations, including antitrust, environmental violations, financial fraud, and illegal exports.⁴⁹⁸

The sixth personality trait focusses on manipulation. In their pursuit of profit, corporations try to manipulate, “everything, including public opinion.”⁴⁹⁹ Bakan illustrates this with Monsanto’s promotion of an artificial hormone for cows, which was marketed as a solution to a non-existent problem, while knowing that it posed risks to the cows and milk consumers.⁵⁰⁰

Finally, the seventh trait, particularly relevant to the new corporation movement, is the creation of a “good neighbour” image.⁵⁰¹ Corporations present themselves not as institutions, but as friends, neighbours, or even saviours, doing good for individuals and society.⁵⁰² This image

⁴⁹⁴ See Bakan, *New Corporation*, *supra* note 5.

⁴⁹⁵ See Bakan, Achbar & Abbott, “Corporation Documentary”, *supra* note 166 at 33:00.

⁴⁹⁶ See Bakan, *The Corporation*, *supra* note 1 at 57.

⁴⁹⁷ See Bakan, Achbar & Abbott, “Corporation Documentary”, *supra* note 166 at 23:00.

⁴⁹⁸ See Bakan, Achbar & Abbott, “Corporation Documentary”, *supra* note 166 at 37:00.

⁴⁹⁹ Bakan, *The Corporation*, *supra* note 1 at 57.

⁵⁰⁰ See Bakan, Achbar & Abbott, “Corporation Documentary”, *supra* note 166 at 31:00.

⁵⁰¹ See Bakan, *New Corporation*, *supra* note 5 at 57.

⁵⁰² See e.g., Bakan, *New Corporation*, *supra* note 5 at 14, 23.

serves to hide or divert attention from the negative impacts of their activities. Bakan cites the example of big oil corporations' public campaigns about their transition to green energy technologies, while at the same time continuing, or even intensifying, their extractive operations.⁵⁰³

Taken together, these seven traits paint a picture of a pathological organization, driven by its primary goal of generating profit for shareholders, that often behaves in ways that are detrimental to society and the environment. This psychopathic behaviour, Bakan argues, raises serious questions about the role and regulation of corporations in modern society. The following section examines how these pathological traits are reflected in corporations with data-driven business models.

B. The Psychopathic Personality of Corporations with Data-Driven Business Models

This thesis focusses primarily on corporations with data-driven business models, particularly those that profit from selling technologies, products, and services that rely on the collection and processing of data about individuals and their behaviours. Bakan argues that these corporations share the same economic logic as twentieth-century industrial corporations, using new technologies to centralize power, eliminate competitors, and take advantage of workers and customers. Their actions harm individuals and the environment, and they use their excessive power to lobby for self-serving laws and regulations.⁵⁰⁴

However, corporations with data-driven business models differ from their industrial predecessors in two key ways: their power and sphere of influence over people and regulators, and

⁵⁰³ See Bakan & Abbott, "New Corporation Documentary", *supra* note 166 at 1:07:00-1:08:40.

⁵⁰⁴ See Bakan, *New Corporation*, *supra* note 5 at 106.

their relatively low cost of capital.⁵⁰⁵ Initially represented mainly by Silicon Valley companies,⁵⁰⁶ these corporations have gained significant influence in various areas of society, including politics, individual lives, the media and the dissemination of information in a democracy, and have proposed solutions to many of today's social problems.⁵⁰⁷

For Bakan, one of the most pressing concerns is the potential for these corporations to exploit the growing and universal belief that technology holds the key to solving humanity's challenges, all in the pursuit of financial gain.⁵⁰⁸ In cases where corporations offer a technology as a solution, it is not just the technology itself that is valuable to them; the data that they can collect and process with the technology are a significant source of revenue for them. This data-driven approach has become central to their business models and continues to shape their strategies for expansion and influence.

While Bakan's theory focusses primarily on publicly traded corporations, similar personality traits can be observed in tech startups. A startup has been defined as "an organization formed to search for a repeatable and scalable business model."⁵⁰⁹ Backed by venture capital and other forms of investment, tech startups develop technologies or service with the aim of scaling up quickly. It can be argued that they are almost forced to develop a psychopathic personality from

⁵⁰⁵ See Bakan, *New Corporation*, *supra* note 5 at 93. See also Tufekci, "As the Pirates Become CEOs", *supra* note 19 at 65–78; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170.

⁵⁰⁶ Given the profitability of data, a number of corporations that initially did not rely on this type of business model are now shifting at least part of their profit sources to data about individuals and their behaviour. See Part III and Chapter VI, *below*.

⁵⁰⁷ See Bakan & Abbott, "New Corporation Documentary", *supra* note 166 at 38:00. See also Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 672.

⁵⁰⁸ See Bakan, *New Corporation*, *supra* note 5 at 104.

⁵⁰⁹ Blank, Steve, "What's A Startup? First Principles" (25 January 2010) online (blog): <steveblank.com> [<http://web.archive.org/web/20231221115305/https://steveblank.com/2010/01/25/whats-a-startup-first-principles/>] referenced by Rowan Wilken, *Cultural Economies of Locative Media*, (New York: Oxford University Press, 2019) at 66.

their early stages, even before (and regardless of whether) they become publicly traded corporations.⁵¹⁰ This is because their growth and survival depend largely on private investment from venture capitalists, larger corporations, or individual investors, each of whom expects a return on their investment. This funding system parallels the legal obligation of public corporations to make a profit for their shareholders, potentially fostering similar pathological traits. Uber is a good example of this phenomenon. As the next part of this chapter will explore, its psychopathic traits were evident even before it became a publicly traded corporation.

Furthermore, it could be argued that is precisely these pathological traits in early corporations with data-driven business models, coupled with the startups financing system, that facilitated what Zuboff describes as “surveillance capitalism”—a new form of market with a “unique logic of accumulation in which surveillance is a foundational mechanism in the transformation of investment into profit.”⁵¹¹ Zuboff argues that this market form was pioneered by Google and later adopted by Facebook, even before they became a publicly traded corporation, as they needed to adapt their business models and philosophies to rapidly transform “investment into revenue and capital.”⁵¹²

⁵¹⁰ A good number of startups fail, and other are acquired by big tech-companies either as a way of stop competition, or to expand their data collection practices to other contexts. See Gené Teare, “What Are The Odds Of Success For A US Seed Funded Startup?” (1 December 2021) online: <news.crunchbase.com> [<http://web.archive.org/web/20231221115535/https://news.crunchbase.com/liquidity/seed-funding-series-a-success/>].

⁵¹¹ Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 99. See also Maša Galič, Tjerk Timan & Bert-Jaap Koops, “Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation” (2017) 30 *Philosophy & Technology* 9 at 22 (the chief idea of this system is that “from all the data that people generate in daily behaviour [. . .], profit should be made”).

⁵¹² Shoshana Zuboff, ““We Make Them Dance”: Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights” in Rikke Frank Jørgensen, ed, *Human Rights in the Age of Platforms* (Cambridge, MA: The MIT Press, 2019) 3 at 9.

While Zuboff sees surveillance capitalism as an evolutionary turn of traditional capitalism,⁵¹³ resulting from the combination of the data-generating and data-processing capabilities of digital technologies and the corporate obsession with profit,⁵¹⁴ Bakan's theory suggests a more systemic problem. The pathological personality of corporations, including their disregard for others in the pursuit of profit, combined with unchecked power, has enabled them to commodify the behaviour and environment of individuals. Thus, what Zuboff refers to as the dispossession and modification of human behaviour can be seen as concrete examples of the pathological behaviour of the corporation driven to maximize profit.

Ari Waldman's research complements Bakan's theory by providing concrete examples of psychopathic corporate behaviour in undermining privacy. Waldman's research suggests that corporations with data-driven business models have deliberately designed a system to undermine privacy by "inculcate[ing] anti privacy norms, undermin[ing] privacy laws, and marginaliz[ing] privacy in design,"⁵¹⁵ in order to profit from data about individuals and their environments.⁵¹⁶ These findings demonstrate how these corporations actively contribute to the implementation and maintenance of mass dataveillance systems for their own profit, and further support that these systems are manifestations of the pathological personality of corporations described by Bakan.

Waldman argues that the current dataveillance landscape is the product of "organizational structures where antiprivacy work is habituated and normalized by ongoing performance."⁵¹⁷ He identifies three types of privacy performance used by corporations with data-driven business

⁵¹³ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 29.

⁵¹⁴ This will be further developed in Part III-B., *below*.

⁵¹⁵ Waldman, *Industry Unbound*, *supra* note 15 at 232.

⁵¹⁶ See Waldman, *Industry Unbound*, *supra* note 15 at 224.

⁵¹⁷ Waldman, *Industry Unbound*, *supra* note 15 at 10.

models: discourse, compliance, and design. These performances exemplify the psychopathic personality of these corporations, particularly their manipulative and “good neighbour” traits.

First, these corporations manipulate privacy discourse to normalize a corporate-friendly understanding of privacy, weakening the ground on which individuals think, debate, and write about privacy.⁵¹⁸ This manipulation has helped these corporations to maintain their dataveillance systems, even as the number of privacy professionals grows, and data protection regulations are enacted around the world. Second, with this weakened ground, corporations employ bureaucracies that constrain privacy offices, leading to symbolic compliance practices that prioritized appearance over substance.⁵¹⁹ Finally, using weak privacy discourses and symbolic compliance, these corporations ensure that their technologies are designed to perpetuate their data-extracting practices.⁵²⁰ The result, Waldman argues, is a system in which privacy advocates and privacy professionals are modelled to serve the data-extractive interests of these corporations, and the meaning of privacy is subtly transformed.⁵²¹

The following subsections examine these stages of privacy performance in detail. The first subsection examines the manipulation of privacy discourse, which clearly demonstrates the manipulative personality traits of these corporations. The second subsection examines symbolic compliance and technology design, which can be seen as an example of corporate manipulation directed at its own employees rather than at the public or regulators—internal manipulation.

⁵¹⁸ See Waldman, *Industry Unbound*, *supra* note 15 at ch 2.

⁵¹⁹ See Waldman, *Industry Unbound*, *supra* note 15 at ch 3.

⁵²⁰ See Waldman, *Industry Unbound*, *supra* note 15 at ch 4.

⁵²¹ See Waldman, *Industry Unbound*, *supra* note 15 at ch 5.

1) Manipulation of the Privacy Discourse

In academia, privacy has been conceptualized in different ways, as discussed in Chapter II. However, when it comes to corporate data processing, regulatory and policy discourses have defined privacy primarily in terms of choice and control. Waldman argues that this dominant conception privacy is not accidental, but rather the result of a multifaceted approach implemented by certain corporations to promote a privacy discourse that benefits their data-based business models.⁵²²

This approach has involved several strategies. First, corporations have engaged in lobbying campaigns to weaken privacy laws.⁵²³ Second, they have reinforced a narrow conception of privacy, defined as choice and control, by relying on “seemingly independent academic research.”⁵²⁴ Waldman claims that “it is one of the singular triumphs” of these corporations “that policy makers and regulators talk about privacy using discourses of control, consent, transparency, and choice.”⁵²⁵ Consequently, by manipulating the privacy discourse, these corporations have also influenced the content of the regulations to ensure the expansion of their dataveillance systems.⁵²⁶

This strategy is in line with Bakan’s theory, which suggests that as part of their image as good neighbours, corporations tend to narrow the definition and of the values they wish to promote.

⁵²² See Waldman, *Industry Unbound*, *supra* note 15 at 74–75.

⁵²³ See e.g., Carole Cadwalladr & Duncan Campbell, “Revealed: Facebook’s Global Lobbying Against Data Privacy Laws”, *The Observer* (2 March 2019), online: <theguardian.com> [<http://web.archive.org/web/20240102154749/http://web.archive.org/screenshot/https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment>]; Natasha Lomas, “Report Reveals how Big Tech Lobbied to Weaken EU Rules”, *TechCrunch* (22 April 2022), online: <techcrunch.com> [<http://web.archive.org/web/20240102151532/http://web.archive.org/screenshot/https://techcrunch.com/2022/04/22/google-facebook-apple-eu-lobbying-report/>].

⁵²⁴ Waldman, *Industry Unbound*, *supra* note 15 at 90.

⁵²⁵ Waldman, *Industry Unbound*, *supra* note 15 at 66.

⁵²⁶ See Waldman, *Industry Unbound*, *supra* note 15 at ch 4; Steeves, “Now You See Me”, *supra* note 24.

They then institutionalize their own definition in public opinion and government through lobbying, marketing, and public relations.⁵²⁷

In addition to defining privacy as a matter of choice, control, and consent, Waldman argues that corporations also tend to mix privacy protection with security improvements.⁵²⁸ This mixing serves two purposes: it helps corporations define privacy narrowly and, most importantly, it allows them to argue that they are actively working to improve the privacy of their services and devices. However, security is fundamentally about “preventing, assessing, and addressing unauthorized access to systems and attacks on data safety and integrity.”⁵²⁹ By using privacy to discuss the implementation and improvement of security measures, such as end-to-end encryption and two-factor identification, corporations can claim to care about privacy and to be taking proactive steps to protect it without making any substantive changes to their dataveillance-based business model.⁵³⁰

Moreover, this narrow definition of privacy contributes to the construction of a good neighbour image. It allows corporations to make public commitments to privacy and reassure their users of its prioritization without significantly changing their profitable data processing practices. This practice is known as “privacy-washing.”⁵³¹

⁵²⁷ See Bakan, *New Corporation*, *supra* note 5 at 57–58.

⁵²⁸ See Waldman, *Industry Unbound*, *supra* note 15 at 85.

⁵²⁹ Waldman, *Industry Unbound*, *supra* note 15.

⁵³⁰ See Waldman, *Industry Unbound*, *supra* note 15.

⁵³¹ See e.g., Geoffrey A Fowler, “At CES, Apple, Facebook and Amazon are Preaching Privacy. Don’t Believe the Hype”, (8 January 2020), online: <[washingtonpost.com](http://web.archive.org/web/20230608081904/https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/)> [<http://web.archive.org/web/20230608081904/https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/>]; Ben Wolford, “Privacy Washing: Google’s Attempts to Redefine What Privacy Means” (7 August 2023) online (blog): <proton.me/blog>.

The term privacy-washing has also been used in technology literature to describe situations where a technology or technique is marketed as protecting privacy, but it does not actually do so, or where the technology does not mitigate the harm. See e.g., *Response to the RFI on Advancing Privacy-Enhancing Technologies*, by Ran Canetti et al, Request for Information (RFI), Federal Register Notice 87 FR 35250 (2022) at 4; Office of the Privacy Commissioner of Canada, *Privacy and AI Ethics: Understanding The Convergences and Tensions for the*

To illustrate this point, consider Meta Inc. (formerly Facebook Inc.), which generates more than 95% of its revenue from advertising.⁵³² This revenue is generated by displaying advertising products on Facebook, Instagram, Messenger, and third-party mobile applications. Marketers pay for advertising products “based on the number of impressions delivered or the number of actions, such as clicks, taken by users.”⁵³³ Similarly, Uber Inc. is also investing more in its advertising arm, stating in its annual report it is using its data and scale “to offer marketplace-centric advertising to connect merchants and brands with our platform network and unlocking cross-platform advertising formats.”⁵³⁴ As a result, both corporations rely heavily on collecting and processing data about individuals and their behaviours, giving them little incentive to reduce their data-processing operations. Nevertheless, both have made clear and consistent commitments to privacy.

Meta Inc., has repeatedly emphasized its commitment to privacy, framing it in terms of control and transparency. This commitment has evolved from a “clear and formal long-term commitment” in 2011 to provide users “tools to control” who can see their information⁵³⁵ to a 2023 reaffirmation of its commitment to user privacy by “continually investing in new technology and processes to allow our community to manage their advertising and privacy preferences.”⁵³⁶ These

Responsible Development of Machine Learning, by Sébastien Gambs, Contributions Program 2020-2021 (Ottawa: OPC, 2021) online: <priv.gc.ca> [https://web.archive.org/web/20231218154442/https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2020-2021/p_2020-21_09/] at 40.

⁵³² See Meta Platforms Inc, *Annual Report 2021 (Form 10-K)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2022) at 65; Meta Platforms Inc, *Annual Report 2022 (Form 10-K)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2023) at 70.

⁵³³ Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 68.

⁵³⁴ Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 5.

⁵³⁵ Mark Zuckerberg, “Our Commitment to the Facebook Community” (29 November 2011) online: <blog.facebook.com> [https://web.archive.org/web/20111130104852/http://blog.facebook.com/blog.php?post=10150378701937131].

⁵³⁶ Meta, “How Meta Uses Legal Bases for Processing Ads in the EU” (4 January 2023) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221153329/https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/].

efforts include providing its users with more detailed information about data use and sharing, as well as offering tools for greater control over the information they share.⁵³⁷

Similarly, Uber Inc. has emphasized its commitment to privacy through its privacy principles, which also frame privacy in terms of choice and control. For instance, they state: “We give users clear choices about their privacy and controls that are easy to use so that they can manage their data.”⁵³⁸ Uber Inc. has also highlighted its commitment to privacy and privacy leadership, claiming to go beyond legal requirements by “working with the privacy engineering and product teams on new features that make Uber’s offerings more transparent or beneficial for users.”⁵³⁹ However, these “innovations” are largely limited to helping “users understand and control how [Uber inc.] use[s] their data.”⁵⁴⁰

2) *Internal Manipulative Behaviours*

Bakan’s framework focussed primarily on the behaviour of corporations towards the public or regulators. Waldman’s research showed that corporations whose business model is based on data have also developed internal strategies, or misdirection as he calls them, to manipulate their employees’ perceptions of privacy and align them with the corporation’s profit-driven services.

Waldman’s research found that the majority of privacy professionals he interviewed—those who design the technologies or are responsible for the corporation’s privacy compliance—

⁵³⁷ See Meta, *supra* note 536.

⁵³⁸ Uber, “Privacy Overview” (last visited 20 December 2023) online: <<https://www.uber.com/global/en/privacy/overview/>>.

⁵³⁹ Jennifer Bryant, “Uber’s CPO on Embracing the Challenge of Privacy” (19 October 2020) online (blog): <iapp.org> [<http://web.archive.org/web/20230325204334/https://iapp.org/news/a/uber-cpo-the-turn-around-queen-embraces-the-challenge-of-privacy/>].

⁵⁴⁰ See e.g., Uber Inc, “ESG Report 2022” (last visited 28 April 2023) online (PDF): <<https://uber.app.box.com/s/7otjao7978mio4x59kqovh47dopp4w>> at 71; Ruby Zefo, “Living Up to Our Privacy Principles: Introducing Uber’s Privacy Center” (18 January 2022) online (Newsroom): <uber.com/newsroom> [<http://web.archive.org/web/20230306225003/https://www.uber.com/newsroom/privacycenter/>].

discussed privacy primarily in terms of encryption, security, choice and control, and transparency.⁵⁴¹ He also examined internal documents that emphasized the benefits of privacy notices and choice and control, which drew heavily on research by Facebook Fellows, Google-funded projects, and Microsoft Research work on encryption.⁵⁴²

Waldman argues that corporations use subtle and sometimes imperceptible tactics to stifle privacy advocates and manipulate the work of their employees to further their own agendas.⁵⁴³ He identifies three types of anti-privacy practices that have become commonplace among employees responsible for privacy in corporations:

1. Equating compliance with the law with bureaucratic requirements. This practice leads privacy professionals to confuse mere symbols of compliance, such as paper audits, checkboxes, and pre-filled reports from outsourced corporations, with actual compliance with data protection laws. By reducing the law to these superficial measures, these corporations can escape accountability.⁵⁴⁴
2. Limiting privacy to notice or security. This approach narrows employees' view of privacy to focus only on features that provide users with notice of data processing and improve the security of systems and databases. This limited view prevents employees from thinking about privacy in a broader way.
3. Assigning narrow technical problems to small teams. This practice keeps engineers focussed on a particular problem and isolates them from the rest of the design problems. As a result, engineers become accustomed to not dealing with privacy issues directly, assuming that they are the responsibility of another team.⁵⁴⁵

These practices are problematic because they shape employees' understanding of what privacy laws are, making it difficult for them to see alternative approaches.⁵⁴⁶ As a result, corporate

⁵⁴¹ See Waldman, *Industry Unbound*, *supra* note 15 at 45–46.

⁵⁴² See Waldman, *Industry Unbound*, *supra* note 15 at 93.

⁵⁴³ See Waldman, *Industry Unbound*, *supra* note 15 at 6.

⁵⁴⁴ See Waldman, *Industry Unbound*, *supra* note 15 at 9.

⁵⁴⁵ See Waldman, *Industry Unbound*, *supra* note 15.

⁵⁴⁶ See Waldman, *Industry Unbound*, *supra* note 15.

data extraction and the technologies that enable it are normalized by employees as ordinary and routine.

The cumulative effect of these anti-privacy practices is the silencing of pro-privacy voices, and the normalization of work that serves corporate data extraction.⁵⁴⁷ As these practices become habitual, they reinforce a corporate culture that prioritizes data collection over privacy concerns, compromising users' privacy in the long run.

This corporate culture has a direct impact on the design of technologies. Given the purpose and the pathological nature of corporations, it is evident that corporations engaged in data collection and processing will prioritize designs that facilitate the generation and collection of large amounts of data at all costs.⁵⁴⁸ For instance, most location technologies are designed to ensure that the benefits they provide to users are tied together to the ability of the corporations to access individual's location data.⁵⁴⁹ As Pedrechi et al. explain, the trace of mobility that individuals leave behind "are an artefact of the design of services such that their collection and storage are difficult to avoid."⁵⁵⁰

In addition, corporations design and market devices and services to seduce individuals to use them by highlighting some of their (potential) benefits, ranging from peace of mind and security to increased savings and convenience.⁵⁵¹ Mark Monmonier, for example, noted that

⁵⁴⁷ See Waldman, *Industry Unbound*, *supra* note 15 at 211.

⁵⁴⁸ See Bakan, *New Corporation*, *supra* note 5 at 97.

⁵⁴⁹ See e.g., Pentland, "Society's Nervous System", *supra* note 10 at 37; Carlos Barreneche & Rowan Wilken, "Platform Specificity and the Politics of Location Data Extraction" (2015) 18:4–5 *European Journal of Cultural Studies* 497 at 508; Rule, "Privacy", *supra* note 470 at 14.

⁵⁵⁰ Pedreschi et al, "Privacy Protection", *supra* note 31 at 101.

⁵⁵¹ See e.g., Julie E Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 75 *The University of Chicago Law Review* 181 at 186–87; Julie E Cohen, "The Surveillance–Innovation Complex: The Irony of the Participatory Turn" in Darin Barney et al, eds, *The Participatory Condition in the Digital Age* (Minneapolis: University of Minnesota Press, 2016) 207 at 208; Kevin D Haggerty & Richard V Ericson, "The Surveillant Assemblage" (2000) 51:4 *British Journal of Sociology* 605 at 615.

satellite positioning has turned location into a commodity that the location-based services (LBS) industry sells to those interested in people's whereabouts. Because LBS can be convenient when individuals need to find something, people become "both a part of the product and a potential consumer[s]." ⁵⁵²

The influence of corporations on the design of digital technologies is also evident in how location data are generated, collected, stored, and shared. Some corporations choose to collect and store location data in combination with other data points, potentially allowing the re-identification or linking of data to a specific user, even without explicit individual identification.

A notable example of this occurred in 2021, when the *New York Times* received a dataset containing the precise locations of anonymous smartphones belonging to thousands of Trump's supporters, rioters, and passersby in Washington, D.C., on January 6 of 2021. ⁵⁵³ The *New York Times* team successfully de-anonymized some individuals by matching the same "mobile Ad ID" across marketing and app databases. This process created a new database containing the first and last names, home addresses, phone numbers, email addresses, app names, exact locations, dates,

⁵⁵² Monmonier, *Spying with Maps*, *supra* note 9 at 175.

See also Bennett & Crowe, *Surveillance of Mobility*, *supra* note 39 at 33 (arguing that surveillance processes [mediated by technologies] both empower and constrain).

⁵⁵³ See Charlie Warzel & Stuart A Thompson, "They Stormed the Capitol. Their Apps Tracked Them.", *The New York Times* (5 February 2021), online: <nytimes.com> [<http://web.archive.org/web/20240102150552/https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html>]. See also Stuart A Thompson & Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy", *The New York Times* (19 December 2019), online: <nytimes.com> [<http://web.archive.org/web/20240102151033/https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>].

and times.⁵⁵⁴ This case not only highlights the extent and specificity of location data held by corporations, but also shows that the storage format of these data is not truly anonymous.⁵⁵⁵

The following section provides an overview of Uber Inc. and Meta Inc. and analyzes both using Bakan's pathological personality framework. This analysis will further illustrate how corporate practices and priorities shape technology design and data handling, often at the expense of user rights and society.

II. Case Examples: Uber Technologies Inc. and Meta Platforms Inc.

This part examines Uber Inc. and Meta Inc. as LBS corporations whose business model depends on the collection, processing, and analysis of large amounts of data. Both corporations operate mass dataveillance systems to collect and process these data for various revenue purposes. This part will draw on recent events, their public communications on privacy, and their annual reports to demonstrate that their behaviour is consistent with the psychopathic traits defined by Bakan.

Rowan Wilken categorizes the services provided by Meta Inc. and Uber Inc. as third-generation LBS, involving ubiquitous geospatial data collection. This means that location data are at the heart of these services, integrated into both the customer-facing interfaces and back-end processes such as algorithmic processing, database building, and monetization strategies.⁵⁵⁶ These

⁵⁵⁴ See Warzel & Thompson, "They Stormed the Capitol", *supra* note 553. See also Thompson & Warzel, "Twelve Million Phones", *supra* note 553.

⁵⁵⁵ See also Dan Calacci et al, "The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good" (2019) arXiv, DOI: <10.48550/arXiv.1905.09350> at 1.

⁵⁵⁶ See Rowan Wilken, "The Necessity of Geomedia: Understanding the Significance of Location-Based Services and Data-Driven Platforms" in Karin Fast et al, eds, *Geomedia Studies: Spaces and Mobilities in Mediatized Worlds* (New York: Routledge, 2017) 21 at 26.

services capture and disseminate geospatial data “at a scale, speed and level of complexity that is markedly different from earlier incarnations of similar services.”⁵⁵⁷

For Wilken, the Uber platform serves as an example of a “native” third-generation service because the geolocation and geocoded data are seamlessly integrated into the operation of the service at all levels and are critical to its operation.⁵⁵⁸ For example, location data are essential for matching riders and drivers, and allowing users to book rides and track approaching cars on a map.⁵⁵⁹ Uber Inc. also uses the location data generated and collected by its various services for research, development, and marketing purposes.⁵⁶⁰ In addition, location data plays an important role in enabling some of Uber’s controversial practices, such as Greyball, a software used to present a “ghost” version of the Uber app to selected individuals in order to evade law enforcement in unauthorized areas of operation.⁵⁶¹ This tool was made possible in large part by the location capabilities of the platform, including geofencing and targeting people in specific locations.⁵⁶²

The Facebook platform became a third-generation service by redesigning its operations to integrate ubiquitous geospatial data collection at various scales.⁵⁶³ Wilken argues that geospatial

⁵⁵⁷ Wilken, “The Necessity of Geomedia”, *supra* note 556 at 29.

⁵⁵⁸ See Wilken, “The Necessity of Geomedia”, *supra* note 556 at 26.

⁵⁵⁹ See Wilken, “The Necessity of Geomedia”, *supra* note 556.

⁵⁶⁰ See Uber, “Uber Privacy Notice (6/13/2022)” (13 June 2022) online: <<https://www.uber.com/legal/en/document/>>; Uber, “Uber Privacy Notice (12/1/2023)” (12 January 2023) online: <<https://www.uber.com/legal/en/document/>>; Uber Inc, “Advertising on Uber: Rides, Eats, and In App Ads” (last visited 27 December 2022) online (Uber): <<https://www.uber.com/hu/en/advertising/>>.

⁵⁶¹ This tool, and how it exemplifies Uber’s pathological personality, is analyzed in more detail in Section C-5, *below*.

⁵⁶² See Rob Davies & Johana Bhuiyan, “Uber Used Greyball Fake App To Evade Police Across Europe, Leak Reveals”, *The Guardian* (12 July 2022), online: <[theguardian.com](https://www.theguardian.com)> [<http://web.archive.org/web/20240102172652/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/12/uber-used-greyball-fake-app-to-evade-police-across-europe-leak-reveals>]; Julia Carrie Wong, “Greyball: How Uber Used Secret Software to Dodge the Law”, *The Guardian* (4 March 2017), online: <[theguardian.com](https://www.theguardian.com)> [<http://web.archive.org/web/20170313181501/https://www.theguardian.com/technology/2017/mar/03/uber-secret-program-greyball-resignation-ed-baker>].

⁵⁶³ See Wilken, “The Necessity of Geomedia”, *supra* note 556 at 26.

data should be seen as a “fourth pillar” that connects to and informs the other three pillars of the platform: newsfeed, timeline, and graph search.⁵⁶⁴ Meta Inc. uses location-based information to deliver, personalize, and improve all of its products,⁵⁶⁵ “including ads, for [the main user] and others.”⁵⁶⁶

This part is divided into three sections. The first two sections present the history of Uber Inc. and Meta Inc. as corporations. The third section, and the main one of this part, examines the actions of these two corporations against the psychopathic traits identified by Bakan to demonstrate that these corporations exhibit psychopathic tendencies consistent with his theory.

A. Uber Technologies Inc. (Uber Inc.)

Founded in 2010, Uber Inc. became a publicly traded corporation nine years later, in 2019.⁵⁶⁷ Its product portfolio includes Uber Ride, Uber Eats, Uber Transit, Uber Health, Uber Freight, and Uber for Business.⁵⁶⁸ According to its annual reports, Uber Inc. generates revenue

⁵⁶⁴ See Wilken, *Cultural Economies*, *supra* note 509 at 86.

⁵⁶⁵ Meta products include: Facebook, Messenger, Instagram (including apps like Boomerang), Facebook Portal products, Meta Platforms Technologies Products (e.g., Meta Horizon Worlds or Meta Quest [when using a Facebook or Meta account]), Shops, Marketplace, Spark AR, Meta Business Tools, Meta Audience Network, NPE Team apps, Facebook View. See Meta, “Privacy Policy: What Products Does This Policy Cover?” (last visited 5 January 2023) online (Privacy Center): <[https://www.facebook.com/privacy/policy/?annotations\[0\]=0.ex.0-WhatProductsDoesThis](https://www.facebook.com/privacy/policy/?annotations[0]=0.ex.0-WhatProductsDoesThis)>; Facebook, “What are the Meta Products?” (last visited 20 September 2023) online (Help Center): <<https://www.facebook.com/help/1561485474074139>>.

⁵⁶⁶ Meta, “Privacy Policy: How We Use Location-Related Information” (last visited 12 January 2024) online (Privacy Center): <<https://www.facebook.com/privacy/policy/?subpage=2.subpage.6-HowWeUseLocation>>. See also Meta, “Privacy Policy: Personalizing Ads for You and Others” (last visited 12 January 2024) online (Privacy Center): <[https://www.facebook.com/privacy/policy/?annotations\[0\]=2.story.3-PersonalizingAdsForYou&subpage=2.subpage.6-HowWeUseLocation](https://www.facebook.com/privacy/policy/?annotations[0]=2.story.3-PersonalizingAdsForYou&subpage=2.subpage.6-HowWeUseLocation)>.

⁵⁶⁷ See Uber Technologies Inc, *Registration Statement (Form S-1)*, Registration No. 333-230812 (United States Securities and Exchange Commission, 2019).

⁵⁶⁸ See Uber, “Uber Apps, Products, and Offerings” (last visited 20 September 2023) online: <<https://www.uber.com/us/en/about/uber-offerings/>>.

primarily from drivers and merchants using its Uber Ride and Uber Eats platforms. In certain markets, it also charges end-users a fee for delivery services through Uber Eats.⁵⁶⁹

In 2022, Uber Inc. formally launched its advertising division, leveraging its data and scale to offer marketplace-centric advertising. This new venture aims to connect merchants and brands with its platform network through cross-platform advertising formats.⁵⁷⁰ In addition, Uber Inc. will provide comprehensive reporting and analytics to help brands refine their “understanding of consumers and create more impactful campaigns as they connect with consumers at relevant points throughout their journeys and transactions.”⁵⁷¹ This increased investment in targeted advertising aligns parts of its business model closely with Meta Inc., a model based on the ability to deliver the most relevant ads to each user.

Uber Inc. has a history of controversial practices that suggest its psychopathic behaviour. These include using data collected on the platform for experiments,⁵⁷² engaging in tax evasion schemes,⁵⁷³ and aggressively lobbying and implementing strategies to enter markets despite violating local laws and regulations.⁵⁷⁴

⁵⁶⁹ See Uber Technologies Inc, *Annual Report 2021 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2022) at 87.

⁵⁷⁰ See Uber Technologies Inc, *Annual Report 2022 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2023) at 5.

⁵⁷¹ Uber Technologies Inc, *Uber 10-K 2022*, *supra* note 570.

⁵⁷² See e.g., Voytek, “Rides of Glory” (26 March 2012) online (blog): <blog.uber.com> [https://web.archive.org/web/20141118192805/https://blog.uber.com/ridesofglory].

⁵⁷³ See e.g., Sydney P Freedberg et al, “How Uber Won Access to World Leaders, Deceived Investigators and Exploited Violence Against Its Drivers in Battle for Global Dominance”, *International Consortium of Investigative Journalists* (10 July 2022), online: <icij.org> [http://web.archive.org/web/20240102143849/https://www.icij.org/investigations/uber-files/uber-global-rise-lobbying-violence-technology/]; Scilla Alecci, “Uber Shifted Scrutiny to Drivers as it Dodged Tens of Millions in Taxes”, *International Consortium of Investigative Journalists* (11 July 2022), online: <icij.org> [http://web.archive.org/web/20240102172331/http://web.archive.org/screenshot/https://www.icij.org/investigations/uber-files/uber-tax-havens-dodge-drivers/].

⁵⁷⁴ See Section C-5, *below*.

In 2022, whistleblower Marc MacGann leaked documents to *The Guardian* revealing Uber Inc.'s questionable practices between 2014 and 2016.⁵⁷⁵ The leaked information, known as the “Uber Files,” revealed how the corporation launched operations in European markets in violation of local regulations, lobbied global politicians, used technology to obstruct legal investigations, and struck deals with currently sanctioned Russian tycoons. *The Guardian* worked with the *International Consortium of Investigative Journalists* (ICIJ) to publish these findings.⁵⁷⁶ Each of these findings provides evidence of the pathological personality of Uber Inc.

The Uber Files revealed a sophisticated strategy employed by Uber Inc. that included a wide range of tactics, such as the use of technology to circumvent regulatory bodies and extensive lobbying to influence politicians, the media, and the general public. This strategy facilitated Uber Inc.'s rapid expansion into different markets and countries. The main objective of this rapid expansion was to speed up the process of platform intermediation, even if it meant sacrificing quarterly profits, which is considered the ultimate goal of key investors.⁵⁷⁷ The strategy also aimed to preserve the corporation's gig economy business model, which relies on a large pool of independent contractors (or freelancers) to generate profit while avoiding the costs associated with

⁵⁷⁵ *The Guardian* led a major global investigation into the leaked Uber documents, distributing the information to media organisations around the world through the *International Consortium of Investigative Journalists* (ICIJ). See Harry Davies et al, “Uber Broke Laws, Duped Police and Secretly Lobbied Governments, Leak Reveals”, *The Guardian* (11 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102170300/https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign].

⁵⁷⁶ See “The Uber files”, *The Guardian* (last visited 2 January 2024), online: <theguardian.com> [https://web.archive.org/web/20240102163254/http://web.archive.org/screenshot/https://www.theguardian.com/news/series/uber-files]; “Uber Files Archives”, *International Consortium of Investigative Journalists* (last visited 2 January 2024), online: <icij.org> [http://web.archive.org/screenshot/https://www.icij.org/tags/uber-files/].

⁵⁷⁷ See Sarah Barns, “Joining the Dots: Platform Intermediation and the Recombinatory Governance of Uber's Ecosystem” in Mike Hodson et al, eds, *Urban Platforms and the Future City: Transformations in Infrastructure, Governance, Knowledge and Everyday Life* (London: Routledge, 2020) 87 at 92.

traditional employment, such as vacation compensation and pensions.⁵⁷⁸ Various elements of this strategy are good examples of its manipulative and asocial personality traits.

In 2017, Uber Inc. replaced its CEO, and, as stated in several public statements by the corporation, this change led to the modification or cessation of numerous behaviours that were exposed in the Uber Files.⁵⁷⁹ While these changes can be attributed to the new leadership and management adjustments, it is important to note that these changes became feasible as Uber Inc established itself in various markets, reducing the need for an aggressive or guerrilla strategy. As the corporation stated in 2022, “Uber is now one of the largest platforms for work in the world and an integral part of everyday life for over 100 million people. We’ve moved from an era of confrontation to one of collaboration.”⁵⁸⁰

Despite these changes, Uber Inc.’s psychopathic personality persists, particularly in its relationship with drivers and delivery workers. As developed below, Uber Inc. continues to demonstrate a lack of empathy and a refusal to acknowledge its responsibility to these individuals, challenging their rights and denying what should be considered fair treatment and compensation.⁵⁸¹

⁵⁷⁸ See Johana Bhuiyan & Dan Milmo, “‘Embrace The Chaos’: A History Of Uber’s Rapid Expansion And Fall From Favour”, (15 July 2022), online: <theguardian.com> [http://web.archive.org/web/20230730100557/https://www.theguardian.com/news/2022/jul/15/embrace-the-chaos-a-history-of-ubers-rapid-expansion-and-fall-from-favour].

⁵⁷⁹ See e.g., Davies et al, “Uber Broke Laws”, *supra* note 575; “‘We Will Not Make Excuses’: Uber Responds To Uber Files Leak”, *The Guardian* (10 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102173940/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/10/uber-response-uber-files-leak].

⁵⁸⁰ Jill Hazelbaker, “Statement on the ICIJ Investigation” (10 July 2022) online (Newsroom): <uber.com> [http://web.archive.org/web/20231221121214/https://www.uber.com/newsroom/icij-statement/].

⁵⁸¹ See Section C-4, *below*.

B. Meta Platforms Inc. (Meta Inc)

Meta Inc., formerly Facebook Inc., was founded in 2004 and became a publicly traded corporation eight years later, in 2012.⁵⁸² Its product portfolio includes the popular platforms Facebook, Messenger, Instagram (with apps such as Threads and Boomerang),⁵⁸³ and WhatsApp,⁵⁸⁴ as well as hardware offerings such as VR glasses (Meta Quest, formerly Oculus),⁵⁸⁵ and AR glasses in partnership with Ray-Ban.⁵⁸⁶

As mentioned above, Meta Inc.'s annual reports show that over 95% of its revenue comes from advertising.⁵⁸⁷ This revenue stream is primarily derived from the display of advertising products across its platforms, including Facebook, Instagram, Messenger, and third party mobile applications.⁵⁸⁸ In order to maximize user engagement with ads, Meta Inc. promises its clients to target ads to the appropriate user segments, which requires the generation, collection, and processing of vast amounts of user data.

Throughout its history, Meta Inc., has exhibited traits consistent with a psychopathic personality, as evidenced by several well-documented incidents. For instance, the Facebook user

⁵⁸² See Facebook Inc, *Registration Statement (Form S-1)*, Registration No.333-179287 (United States Securities and Exchange Commission, 2012).

⁵⁸³ See Facebook, "What are the Meta Products?", *supra* note 565.

⁵⁸⁴ See Meta, "WhatsApp" (last visited 20 September 2023) online: <<https://about.meta.com/uk/technologies/whatsapp/>>.

⁵⁸⁵ See Meta, "Meta Platforms Technologies Products Definition" (last visited 20 September 2023) online: <https://www.meta.com/gb/legal/meta-platforms-technologies-products/?utm_source=www.facebook.com&utm_medium=dollyredirect>.

⁵⁸⁶ Meta, "Ray-Ban Meta Smart Glasses" (last visited 20 December 2023) online: <<https://www.meta.com/gb/smart-glasses/>>.

⁵⁸⁷ See Part I-B.1, *above*.

See Meta Platforms Inc, *Meta 10-K 2021*, *supra* note 532 at 65; Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 70.

⁵⁸⁸ Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 68.

contagion experiment illustrates the corporation's asocial and superficial traits.⁵⁸⁹ Similarly, the Cambridge Analytica scandal highlighted the irresponsible, asocial, and manipulative traits of Meta Inc.⁵⁹⁰ Despite being aware of the data breach, the corporation delayed taking action and informing the public. Internal documents revealed that the corporation had discovered the massive harvesting of Facebook user data in late 2015, but chose not to alert users or investors.⁵⁹¹ Instead, it took limited steps to recover and secure private data, simply asking the researcher and Cambridge Analytica to delete the data.⁵⁹² It was not until 2018 that the corporation finally suspended Cambridge Analytica from Facebook.⁵⁹³

⁵⁸⁹ See Adam D I Kramer, Jamie E Guillory & Jeffrey T Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks" (2014) 111:24 PNAS 8788; Daniel J Solove, "Facebook's Psych Experiment: Consent, Privacy, And Manipulation", *The Huffington Post* (30 June 2014), online: <huffingtonpost.com> [http://web.archive.org/web/20240102125002/http://web.archive.org/screenshot/http://www.huffingtonpost.com/daniel-j-solove/facebook-psych-experiment_b_5545372.html].

⁵⁹⁰ In June 2014, an academic researcher, Aleksandr Kogan, and Cambridge Analytica (a data analytics firm) contracted, whereby Cambridge Analytica would pay for the researcher to collect data on Facebook users. To collect his data, Kogan's team developed a personality survey that obtained data from approximately 50 million Facebook users.

See Carole Cadwalladr & Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach", *The Guardian* (17 March 2018), online: <theguardian.com> [http://web.archive.org/web/20240102151856/http://web.archive.org/screenshot/https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election]; Carole Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower", *The Guardian* (18 March 2018), online: <theguardian.com> [http://web.archive.org/web/20240102144227/https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump].

⁵⁹¹ See US Securities and Exchange Commission, "SEC v Facebook, Inc Case No 3:19-cv-04241-JD (ND Cal)" (last visited 28 April 2023) online: <sec.gov> [https://web.archive.org/web/20231218145706/https://www.sec.gov/enforcement/information-for-harmed-investors/facebook].

⁵⁹² See e.g., Natasha Lomas, "Facebook Ignored Staff Warnings about 'Sketchy' Cambridge Analytica in September 2015", *TechCrunch* (25 July 2019), online: <techcrunch.com> [http://web.archive.org/web/20190823164659/https://techcrunch.com/2019/07/25/facebook-ignored-staff-warnings-about-sketchy-cambridge-analytica-in-september-2015/]; Cadwalladr & Graham-Harrison, "Revealed", *supra* note 590.

⁵⁹³ See Meta, "Suspending Cambridge Analytica and SCL Group From Facebook" (17 March 2018) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20230427101118/https://about.fb.com/news/2018/03/suspending-cambridge-analytica/]; Jonathan Shieber, "Facebook Suspends Cambridge Analytica, the Data Analysis Firm that Worked on the Trump Campaign", *TechCrunch* (17 March 2018), online: <techcrunch.com>

In 2021, whistleblower Frances Haugen’s leak of internal documents led to the publication of “The Facebook Files” by the *Wall Street Journal* and *The Guardian*.⁵⁹⁴ These files shed light on the corporation’s handling of misinformation and harmful content on Facebook and Instagram between 2018 and 2020. The documents further corroborated the corporation’s psychopathic behavioural traits, including irresponsibility, manipulability, lack of empathy, inability to take responsibility, and a relentless effort to maintain a “good neighbour” image.

The leaked documents revealed that Meta Inc. researchers repeatedly recognized the harmful effects of the platforms. Despite congressional hearings, public commitments, and extensive media coverage, Meta Inc. has failed to effectively address these issues. These internal documents provide the most comprehensive insight yet into the extent to which Meta Inc. recognizes the problems plaguing Facebook and Instagram, yet struggles to implement a meaningful solution.⁵⁹⁵

C. The Psychopathic Personality of Uber Inc and Meta Inc

This section examines the behaviour of Uber Inc. and Meta Inc. through the lens of the psychopathic traits identified by Bakan. The analysis includes their privacy-related actions as well as their broader operations, with the aim of demonstrating how these two corporations, as representatives of corporations with data-driven business models, exhibit most, if not all, of the pathological characteristics of psychopathic corporations. These traits include irresponsibility,

[<https://web.archive.org/web/20240102123256/http://web.archive.org/screenshot/https://techcrunch.com/2018/03/16/facebook-suspends-cambridge-analytica-the-data-analysis-firm-that-worked-for-the-trump-campaign/>].

⁵⁹⁴ See Wall Street Journal, “The Facebook Files”, *Wall Street Journal* (last visited 2 January 2024), online: <[wsj.com](https://www.wsj.com)>

[<http://web.archive.org/web/20240102164327/http://web.archive.org/screenshot/https://www.wsj.com/articles/the-facebook-files-11631713039>].

⁵⁹⁵ See Wall Street Journal, *supra* note 594.

superficial relationships with others, refusal to take responsibility, lack of empathy, asocial tendencies, and building and maintaining a deceptive “good neighbour” image.⁵⁹⁶

1) Irresponsibility

Meta Inc.’s handling of changes to the Facebook platform’s algorithm is an example of its irresponsible behaviour. Despite being aware of the risks and potential harms enabled by its platforms, and how the changes it made to its algorithm were being used to cause harm in certain countries, Meta Inc. often chose to delay or avoid implementing changes. When confronted with these risks, the corporation typically downplayed their significance to the public and regulators.

In 2018, Meta Inc. (then Facebook Inc.) changed the primary goal of Facebook’s algorithms: instead of focussing on helping users find relevant content, the new goal was to improve interactions between friends and family. This shift was apparently prompted by research suggesting that passive media consumption, particularly video, which had grown significantly on the platform, was less beneficial to users’ well-being than social interactions.⁵⁹⁷

However, leaked documents reported by the *Wall Street Journal* revealed that this algorithmic change had a dual purpose. While publicly presented as a means to “strengthen connections between users and improve their well-being,”⁵⁹⁸ the internal motivations were less

⁵⁹⁶ For an explanation of each of these traits see Part I-A, *above*.

The seventh trait identified by Bakan is manipulative behaviour. Part I-B.1, *above*, provided concrete examples of this behaviour exhibited by Uber Inc. and Meta Inc., particularly with regard to their manipulation of the privacy discourse.

⁵⁹⁷ See Keach Hagey & Jeff Horwitz, “Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead”, *Wall Street Journal* (15 September 2021), online: <wsj.com> [<https://web.archive.org/web/20240102124309/http://web.archive.org/screenshot/https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215>].

⁵⁹⁸ Hagey & Horwitz, *supra* note 597.

altruistic. The corporation was concerned about declining user engagement,⁵⁹⁹ a trend that threatened its revenue model, which relies heavily on the amount of time users spend on Facebook and Instagram platforms, as this determines the amount of user data it can generate and collect, and the attention it can sell to advertisers.

Internal reports warned that this change was actually having unintended consequences. Facebook was becoming a more hostile environment as publishers and political parties adjusted their content to favour outrage and sensationalism, which generated more comments and reactions—the metrics of success under the new algorithm. The internal reports found that this approach was having a detrimental effect on important public content such as politics and news. The new algorithm’s emphasis on re-shared material in the News Feed amplified angry voices, with misinformation, toxicity, and violent content disproportionately represented among re-shares.⁶⁰⁰

Despite these troubling findings, Meta Inc. chose to largely ignore these reports. When changes were made, they were often small and implemented slowly, prioritizing testing for potential impacts on user engagement over addressing the problems identified. This response shows a pattern of irresponsible behaviour, as the corporation knowingly allowed the platform to become “angrier,” contributing to increased polarization and the spread of misinformation, all in the service of maintaining high levels of user engagement, and protecting its business model.

⁵⁹⁹ See Hagey & Horwitz, *supra* note 597.

⁶⁰⁰ See Hagey & Horwitz, *supra* note 597.

2) Superficial Relationships

The leaked files reveal Uber Inc.'s superficial relationship with its drivers and illustrate its broader approach to stakeholder interactions. When entering a market, Uber Inc. would use investor funds to attract drivers with attractive hourly rates and incentives such as bonuses and car leases, portraying the Uber platform as lucrative. However, once the corporation had secured a significant market share and a sufficient driver base, it would reduce the incentives and increase its commission, dramatically affecting drivers' monthly income.⁶⁰¹ MacGann described this tactic as "bait-and-switch."⁶⁰²

When drivers resisted these changes, Uber Inc. manipulated the platform's algorithms to resolve the situation. For instance, in October 2014, following price cuts and payment reductions to drivers in Italy, a manager reported a potential strike that would result in only a small number of drivers being available. The corporation responded with "exceptionally high incentives," which prevented the strike and increased the number of hours drivers worked. This incident illustrates a key aspect of Uber Inc.'s business model: the use of dynamic pricing to influence workers' decisions about when and where to work.⁶⁰³ Such algorithmic manipulation allows the corporation to control driver behaviour without direct management.

⁶⁰¹ See Brenda Medina, "As Uber Expanded Globally, Many Drivers Felt Left Behind", (19 July 2022), online: <icij.org> [<http://web.archive.org/web/20230531005548/https://www.icij.org/investigations/uber-files/as-uber-expanded-globally-many-drivers-felt-left-behind/>]. See also Felicity Lawrence, "'They Were Taking Us for a Ride': How Uber Used Investor Cash to Seduce Drivers", *The Guardian* (12 July 2022), online: <theguardian.com> [<http://web.archive.org/web/20240102165430/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/12/they-were-taking-us-for-a-ride-how-uber-used-investor-cash-to-seduce-drivers>].

⁶⁰² Brenda Medina & Nicole Sadek, "'We Co-Opted Democracy,' Uber Files Whistleblower Tells European Parliament", *International Consortium of Investigative Journalists* (25 October 2022), online: <icij.org> [<http://web.archive.org/web/20240102173748/http://web.archive.org/screenshot/https://www.icij.org/investigations/uber-files/we-co-opted-democracy-uber-files-whistleblower-tells-european-parliament/>].

⁶⁰³ See Lawrence, "'They Were Taking Us for a Ride'", *supra* note 601.

Similarly, Meta Inc.'s leaked documents reveal a superficial relationship and lack of empathy, with its users, as the way it responds to known harms and risks varies from country to country, particularly whether the user is in the US or not. According to Boland, who oversaw partnerships with ISPs in Africa and Asia before stepping down, the corporation sees harms in developing countries as a routine cost of doing business. Meta Inc. has focussed its safety initiatives on wealthier markets with strong government and media institutions, while targeting poorer countries to expand its user base.⁶⁰⁴

This approach is particularly worrying given that more than 90% of Meta Inc.'s monthly users live outside the US and Canada, with the Global South accounting for a significant proportion of its user base. While growth has stalled in Europe and North America, Facebook continues to attract new users from the Global South, where it serves as a primary online communication channel and news source.⁶⁰⁵ Despite this, Meta Inc. has devoted fewer resources to preventing harm overseas than in the US. In 2020, only 13% of the more than 3.2 million hours spent identifying and categorizing false or misleading information was dedicated to content from outside the US. Conversely, the corporation spent almost three times as many hours on “brand safety”—protecting advertisers from having their ads appear alongside inappropriate content—outside the US,⁶⁰⁶ prioritizing the protection of its direct source of revenue.

Meta Inc.'s superficial relationship and lack of empathy towards its users in the Global South is further illustrated by its inaction in Myanmar, despite explicit warnings about the risks of

⁶⁰⁴ See Justin Scheck, Newley Purnell & Jeff Horwitz, “Facebook Employees Flag Drug Cartels and Human Traffickers. The Company’s Response Is Weak, Documents Show”, *Wall Street Journal* (16 September 2021), online: <wsj.com> [<http://web.archive.org/web/20240102120837/https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953>].

⁶⁰⁵ See Scheck, Purnell & Horwitz, *supra* note 604.

⁶⁰⁶ See Scheck, Purnell & Horwitz, *supra* note 604.

its platform contributing to genocide or other forms of mass violence against the Rohingya. Despite receiving multiple communications from experts and civil society activists in the five years leading up to the Rohingya genocide in 2017, Meta Inc. failed to take the necessary steps to change its algorithms to address the issues raised in these communications and mitigate the risks highlighted.⁶⁰⁷

This pattern of awareness without action was not limited to Myanmar.⁶⁰⁸ The leaked documents show that Meta Inc. consistently entered new countries “Without fully understanding its potential impact on local culture and politics, and [failed] to deploy the resources to act on issues once they occur.”⁶⁰⁹ This approach underlines the corporation’s superficial relationship with users in the Global South and its prioritization of growth over user safety and social impact.

⁶⁰⁷ See Amnesty International, *Myanmar: The Social Atrocity: Meta and the Right to Remedy for the Rohingya*, (London: Amnesty International, 2022) online: <amnesty.org> [<http://web.archive.org/web/20240403045056/https://www.amnesty.org/en/documents/asa16/5933/2022/en/>] at ch 7; “Rohingya Crisis” (last visited 10 April 2024) online (Myanmar Internet Project): <myanmarinternet.info> [<http://web.archive.org/web/20240404235924/https://www.myanmarinternet.info/rohingya-crisis/>].

⁶⁰⁸ See e.g., Julia Carrie Wong, “How Facebook Let Fake Engagement Distort Global Politics: A Whistleblower’s Account”, *The Guardian* (12 April 2021), online: <theguardian.com> [<http://web.archive.org/web/20240412081030/https://www.theguardian.com/technology/2021/apr/12/facebook-fake-engagement-whistleblower-sophie-zhang>].

⁶⁰⁹ Sheera Frenkel & Davey Alba, “In India, Facebook Grapples With an Amplified Version of Its Problems”, *The New York Times* (23 October 2021), online: <nytimes.com> [<http://web.archive.org/web/20240404035812/https://www.nytimes.com/2021/10/23/technology/facebook-india-misinformation.html>].

3) Refusal to Take Responsibility

Uber Inc. has a long list of settled lawsuits in various countries⁶¹⁰ over issues such as data privacy and security,⁶¹¹ employee classification, and the language used to describe its services.⁶¹² Most of these settlements were reached under the leadership of the previous CEO. Notably, following the release of the Uber Files, the corporation issued a press statement acknowledging past misconduct: “We have not and will not make excuses for past behaviour that is clearly not in line with our present values.”⁶¹³ This response potentially demonstrates Uber Inc.’s willingness to admit fault, although it could be argued that the corporation’s restructuring at the executive and management levels made this admission an easy response—a kind of “that was the old us, not the new us.”

Under the new CEO, Uber Inc. has continued to settle cases, particularly involving employee-related issues. However, the corporation has consistently denied any wrongdoing in these cases.⁶¹⁴ Displaying the psychopathic trait of refusing to take responsibility.

⁶¹⁰ For a summary of cases from 2009-2016 see Sam Levin, “Uber Lawsuits Timeline: Company Ordered to Pay Out \$161.9m since 2009”, *The Guardian* (13 April 2016), online: <theguardian.com> [http://web.archive.org/web/20240102171330/https://www.theguardian.com/technology/2016/apr/13/uber-lawsuits-619-million-ride-hailing-app].

⁶¹¹ See e.g., Office of the New York State Attorney General, “AG Schneiderman Announces Settlement with Uber to Enhance Rider Privacy” (6 January 2016) online (News release): <ag.ny.gov> [http://web.archive.org/web/20231221150249/https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy].

⁶¹² See e.g., Molly Spaeth, “Class Action Settlement” (11 February 2016) online (Newsroom): <uber.com> [http://web.archive.org/web/20231221151337/https://www.uber.com/newsroom/class-action-settlement/].

⁶¹³ Hazelbaker, “Statement on the ICIJ Investigation”, *supra* note 580.

See also Théo Bourgery-Gonse, “Uber is Not What it Used to Be, CEO Tells French MPs”, *Euractiv* (26 May 2023), online: <euractiv.com> [http://web.archive.org/web/20240102171148/http://web.archive.org/screenshot/https://www.euractiv.com/section/ig-economy/news/uber-is-not-what-it-used-to-be-ceo-tells-french-mps/].

⁶¹⁴ See e.g., *Colopy v Uber Techs Inc*, 2019 WL 6841218, (ND Cal 2019) [*Colopy*]; Settlement Administrator, “James et al v Uber Technologies Inc” (last visited 10 October 2023) online: <jamesvuber.com> [http://web.archive.org/web/20231220141023/https://www.jamesvuber.com/].

In contrast, Meta Inc.’s response to the Facebook Files illustrates a different approach, and it is a good example of this pathological trait. As reported by the *Wall Street Journal* and *Politico*, a Meta Inc spokesman said: “When our work is being mischaracterized, we’re not going to apologize. . . . We’re going to defend our record.”⁶¹⁵ Instead of accepting at least a small measure of responsibility for its actions revealed by the documents, or asking for forgiveness, Meta Inc. chose to attack the credibility of the whistleblower and emphasize the billions of dollars it had invested in online safety and partnerships with external institutions and experts.⁶¹⁶

Another example of this trait is that Meta Inc. has settled a number of privacy-related complaints by agreeing to pay for damages without admitting wrongdoing. For instance, the corporation settled a class action lawsuit in 2020 for \$650 million,⁶¹⁷ followed by another in 2023 for \$725 million.⁶¹⁸ In both cases, Meta Inc. agreed to make product changes but denied breaking the law. A spokesperson for Meta Inc, as reported by *Reuters*, stated that the 2023 settlement was

⁶¹⁵ Emily Birnbaum, “Facebook Looking for Its Voice at a ‘Watershed Moment’”, *Politico* (25 October 2021), online: <politico.com> [http://web.archive.org/web/20211026071733/https://www.politico.com/news/2021/10/25/facebook-pr-war-517128]; Keach Hagey et al, “Facebook’s Pushback: Stem the Leaks, Spin the Politics, Don’t Say Sorry”, *Wall Street Journal* (29 December 2021), online: <wsj.com> [http://web.archive.org/web/20240102130635/http://web.archive.org/screenshot/https://www.wsj.com/articles/facebook-whistleblower-pushback-political-spin-zuckerberg-11640786831].

⁶¹⁶ See Hagey et al, “Facebook’s Pushback”, *supra* note 615 (For instance, the article reported that in a hearing, Meta’s global head of safety “pointed to the company’s work with its safety advisory board, created more than a decade ago, which includes internet-safety experts from around the world”); Birnbaum, “Facebook Looking for Its Voice”, *supra* note 615 (Politico reported that in a call with investors CEO Mark Zuckerberg said that “what we are seeing is a coordinated effort to selectively use leaked documents to paint a false picture of our company”).

⁶¹⁷ See *In re: Facebook Biometric Information Privacy Litigation*, 522 F. Supp. 3d 617, (ND Cal 2021) [*In re: Facebook Biometric*]; Associated Press, “Judge Approves \$650m Settlement of Privacy Lawsuit Against Facebook”, *The Guardian* (27 February 2021), online: <theguardian.com> [http://web.archive.org/web/20240324122846/https://www.theguardian.com/technology/2021/feb/27/facebook-illinois-privacy-lawsuit-settlement]; “Facebook Biometric Information Privacy Litigation” (last visited 19 September 2023) online: <https://www.facebookbipaclaimaction.com/>.

⁶¹⁸ See *In re: Facebook, Inc Consumer Privacy User Profile Litigation, Settlement Agreement*, 2023 U.S. Dist. LEXIS 182191, (ND Cal 2023) at para 9 [*In re: Facebook, Inc. Consumer Privacy*]; Alex Hern, “Facebook Owner To Settle Class-Action Suit Over Cambridge Analytica Scandal”, *The Guardian* (23 December 2022), online: <theguardian.com> [https://web.archive.org/web/20240102122349/https://www.theguardian.com/business/2022/dec/23/facebook-owner-to-settle-class-action-suit-over-cambridge-analytica-scandal].

pursued in the best interests of its community and shareholders. The statement also emphasized the corporation's efforts to improve its approach to privacy and implement a comprehensive privacy program.⁶¹⁹

4) Lack of Empathy

According to the Uber Files, Uber Inc.'s relationship with its drivers reveals a lack of empathy. *The Guardian* reported that the drivers were frequently mentioned in the corporation leaked documents, but mostly as “supply” or “liquidity”—commodities to be controlled algorithmically.⁶²⁰ While Uber claimed to be transforming the workforce in each market, which was an essential element of the corporation's strategy, some drivers claimed that they were deceived. They claimed that Uber Inc. lured them onto its platform with financial incentives that were not honoured, while significantly increasing its share of each trip that forced them to work longer hours to maintain their income.⁶²¹

This lack of empathy is further demonstrated by Uber Inc.'s response to violence against its drivers, and its handling of issues of sexual violence. MacGann's statement to the European Parliament that “the corporation ‘played with people's lives’ by trivializing violence against its drivers from rival taxi groups”⁶²² highlights the corporation's disregard for driver safety. He added:

⁶¹⁹ See Nate Raymond, “Facebook Parent Meta to Settle Cambridge Analytica Scandal Case for \$725 Million”, *Reuters* (23 December 2022), online: <reuters.com> [http://web.archive.org/web/20231016162427/https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/].

⁶²⁰ See Lawrence, “‘They Were Taking Us for a Ride’”, *supra* note 601.

⁶²¹ See Freedberg et al, “How Uber Won Access to World Leaders”, *supra* note 573.

⁶²² Medina & Sadek, “We Co-Opted Democracy”, *supra* note 602.

“We weaponized our drivers and we weaponized our customers. They were ours to use in the service of the mission.”⁶²³

Uber Inc.’s strategy of entering markets without government approval directly affected its drivers, making them the target of traditional taxi drivers who felt their business threatened by competitors who did not have to play by the same rules. In Europe, Asia, and South America, taxi drivers “staged protests, harassed Uber customers, beat Uber drivers and set fire to their cars.”⁶²⁴ While these attacks posed a clear challenge to Uber Inc., by potentially discourage drivers from using its platform, the corporation actually benefited from the violence.

The Guardian reported that Uber Inc. had a calculated strategy that it used in various countries: when an Uber driver was subjected to violence, such as being beaten, stabbed, or attacked by other taxi drivers, executives at Uber Inc.’s country office would notify the national media to get free publicity and support against taxis.⁶²⁵ Subsequently, the corporation’s lobbyists would use the incident to arrange meetings with government officials and ministers to push for favourable legislation. This approach was evident during the 2016 taxis protest in France, where leaked documents revealed that “Uber moved swiftly to leverage the violence in a campaign to pressure governments to rewrite laws that stymied Uber’s chances of expansion.”⁶²⁶

⁶²³ Medina & Sadek, *supra* note 602.

⁶²⁴ Freedberg et al, “How Uber Won Access to World Leaders”, *supra* note 573. See also Angelique Chrisafis, “France Hit by Day of Protest as Security Forces Fire Teargas at Taxi Strike”, *The Guardian* (26 January 2016), online: <theguardian.com> [http://web.archive.org/web/20240102132224/http://web.archive.org/screenshot/https://www.theguardian.com/world/2016/jan/26/french-taxi-drivers-block-paris-roads-in-uber-protest].

⁶²⁵ See Freedberg et al, “How Uber Won Access to World Leaders”, *supra* note 573.

⁶²⁶ Felicity Lawrence & Jon Henley, “‘Violence Guarantees Success’: How Uber Exploited Taxi Protests”, *The Guardian* (10 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102173558/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/10/violence-guarantees-success-how-uber-exploited-taxi-protests].

Uber Inc's response to allegations of sexual violence involving both drivers and passengers, with victims and perpetrators on both sides, has been equally inadequate. Victims have reported being ignored or dismissed, and the corporation's efforts to address the problem have been insufficient. One particular concern is Uber Inc.'s failure to thoroughly investigate or modify the design of its platform to prevent such incidents of violence.⁶²⁷

While Uber Inc. claims to be working with organizations around the world to tackle gender-based violence,⁶²⁸ its transparency is limited. The two safety and security reports published by the corporation only included figures and policies for its US market, raising questions about its commitment to safety in other regions. Uber Inc. has used these reports to differentiate itself from other corporations, emphasizing that, unlike corporations that avoid discussing "these hard issues," it believes that keeping this information secret does not make anyone safer.⁶²⁹

These reports have also helped Uber Inc. build an image of caring about its drivers and users. The corporation claims that by sharing hard data about serious safety issues, such as sexual violence, it can hold itself responsible and share best practices with other corporations for the benefit of all.⁶³⁰ However, the lack of transparency about data and policies for markets outside the US undermines the claim and suggests a lack of empathy and genuine commitment to safety outside of the US. To demonstrate a sincere commitment to safety for all, Uber Inc. should provide

⁶²⁷ See Amanda Turnbull, "Onlife Harms: Uber and Sexual Violence" (2022) 19:2 Canadian Journal of Law and Technology 277.

⁶²⁸ See Elise Maiolino, "Driving Change: Partnering to End Gender-Based Violence" (15 December 2022) online (Uber Newsroom): <uber.com> [<http://web.archive.org/web/20230120035101/https://www.uber.com/newsroom/driving-change-to-end-gender-based-violence/>].

⁶²⁹ See Uber, "Uber's US Safety Reports: Part of our Commitment to Making Uber a Safe Platform for Everyone" (last visited 21 May 2024) online (Uber): <uber.com> [<https://web.archive.org/web/20240427151017/https://www.uber.com/us/en/about/reports/us-safety-report/>] at Frequently asked questions.

⁶³⁰ See Uber, *supra* note 629.

clear data, policies, and explanations of how it is working to reduce risk for victims, regardless of their location.

Uber Inc.'s lack of empathy for its drivers is evident not only in its “weaponization” of drivers, but also in its treatment of drivers as independent contractors and the corporation’s responsibility towards them. Bakan argued that Uber Inc.’s platform and consistent effort to circumvent regulations have “transform a job protected by regulations and employment law—professional driving—into one that is precarious and unprotected.”⁶³¹ He went on to stress that with “Uber heavily subsidized by investors who are now demanding profitability, the corporation will likely resist wage increases even more vociferously than it has—or swap them for rate hikes that diminish service for poorer customers and in poorer districts.”⁶³²

This issue has attracted global attention, with Uber drivers in various countries taking legal action to be recognized as employees and to secure minimum working conditions, such as minimum wage and holiday leave. Regulators worldwide are also engaged in this debate. However, Uber Inc. has consistently resisted such effort.⁶³³

A good example of Uber Inc.’s resistance is its response to California’s 2019 labour law, AB5, which would require the corporation to classify drivers as employees—a significant change to its business model. When a court ordered Uber Inc to comply with the law’s requirements, the corporation’s response was twofold: in August 2020, it threatened to cease operations in California,⁶³⁴ while simultaneously launching a lobbying campaign to overturn the law through a

⁶³¹ Bakan, *New Corporation*, *supra* note 5 at 102.

⁶³² Bakan, *New Corporation*, *supra* note 5.

⁶³³ See e.g., Lawrence, “‘They Were Taking Us for a Ride’”, *supra* note 601.

⁶³⁴ See Ha Mansukhani, “Rideshare in California is at Risk” (18 August 2020) online (blog): <uber.com/blog> [http://web.archive.org/web/20231005010747/https://www.uber.com/blog/rideshare-in-california-is-at-risk/].

referendum known as Proposition 22. Uber was part of a coalition of gig economy corporations that invested \$220 million in this campaign,⁶³⁵ which was ultimately approved by 59% of voters.⁶³⁶

The events described in the previous paragraphs illustrate Uber Inc.’s determination to maintain its current business model, even in the face of legal challenges, and potential improvements to driver welfare, and concerns for the safety of drivers and passengers—including its troubling record on sexual violence. The corporation’s actions demonstrate a prioritization of profitability over the well-being of its workforce and users, and further underline its lack of empathy in its relationship with drivers and customers.

Turning to Meta Inc., similar issues of lack of empathy are evident, particularly in the corporation’s treatment of content moderators, particularly those outside the US. A *Times* investigation found out that the workers in one of Meta Inc’s content moderation offices in Nairobi “[were] among the lowest-paid workers for the platform anywhere in the world, with some of them

⁶³⁵ See Kari Paul & Julia Carrie Wong, “California Passes Prop 22 in a Major Victory for Uber and Lyft”, (4 November 2020), online: <theguardian.com> [http://web.archive.org/web/20230714162120/https://www.theguardian.com/us-news/2020/nov/04/california-election-voters-prop-22-uber-lyft].

See also Lawrence, “‘They Were Taking Us for a Ride’”, *supra* note 601.

⁶³⁶ In June 30 of 2023, the California Supreme Court granted the petition for review the Court of Appeal judgement to Proposition 22 and determine its constitutionality. Supreme Court of California, “Summary of Cases Accepted and Related Actions During Week of June 20, 2022” (30 June 2023) online (News Release): <supreme.courts.ca.gov> [http://web.archive.org/web/20231221120848/https://supreme.courts.ca.gov/sites/default/files/supremecourt/default/documents/ws062623.pdf].

See also Kellen Browning, “California Court Mostly Upholds Prop. 22 in Win for Uber and Other Gig Companies”, (13 March 2023), online: <nytimes.com> [http://web.archive.org/web/20230314040043/https://www.nytimes.com/2023/03/13/business/prop-22-upheld-california.html].

taking home as little as \$1.50 per hour.”⁶³⁷ The corporation also fails to provide psychological support for these workers, despite the negative impact their work has on their mental health.⁶³⁸

The Facebook Files also revealed that Meta Inc. was aware that its platforms Facebook and Instagram were being used for harmful activities. This included human trafficking, incitement to violence, and government crackdown on political dissent. Although the corporation removed some offensive content, it failed to address the underlying issues, instead prioritizing maintaining its user base, supporting business partners, and the appeasing authoritarian governments.

Specifically, the documents revealed that traffickers in the Middle East were using Facebook to lure women into exploitative labour situations where they were subjected to slavery or forced into sex work, armed groups in Ethiopia were inciting violence against ethnic minorities, and the platform was used to sell organs and pornography. Despite the removal of some pages, the documents showed that many active pages remained on Facebook.⁶³⁹

The Facebook Files additionally provided evidence that Meta Inc.’s actions are motivated by economic pressure rather than empathy or concern for its users. For example, it only took decisive action against human trafficking on its platforms after Apple Inc. warned that it would remove Meta Inc.’s products from its App Store. This ultimatum came in response to a BBC report on the sales of domestic workers. An internal summary of the episode revealed that Meta Inc. knew

⁶³⁷ Billy Perrigo, “Inside Facebook’s African Sweatshop”, *Time* (14 February 2022), online: <time.com> [http://web.archive.org/web/20230802045128/https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/].

See also Vittoria Elliott, “Meta Lurches Toward Another Moderation Crisis”, *Wired* (23 January 2023), online: <wired.com> [http://web.archive.org/web/20230821104014/https://www.wired.com/story/metanew-moderation-contractor-may-be-worse-than-its-last-one/].

⁶³⁸ See e.g., Casey Newton, “The Trauma Floor: The Secret Lives of Facebook Moderators in America”, *The Verge* (25 February 2019), online: <theverge.com> [http://web.archive.org/web/20240102162750/https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona].

⁶³⁹ See Scheck, Purnell & Horwitz, “Facebook Employees Flag Drug Cartels and Human Traffickers”, *supra* note 604.

about these issues before the BBC investigation and Apple Inc.'s ultimatum, but only began to act more quickly after the ultimatum, because the removal of its products from the App Store would negatively impact the corporation's revenue.⁶⁴⁰

In these cases, the pathological trait of lack of empathy can be complemented to the corporation's relationship with society, which Zuboff characterized as "radical indifference." She argues that from the perspective of surveillance capitalist corporations, the only thing that matters is the accumulation of data; they do not care about the actions and behaviours of individuals as they use their services or platforms. Individuals are free to engage in any activity they wish, as long as the corporations are able to generate, collect, and analyze data on those activities.⁶⁴¹

The pattern of superficial action without addressing root causes extends to Meta Inc.'s approach to various problems. When problems were discovered, the corporation claimed it had taken action by removing the offending content. However, it would not implement permanent solutions to prevent the recurrence of the inappropriate behaviour. Instead, Meta Inc. focussed on maintaining its user base, supporting business partners, and appeasing authoritarian governments to ensure continued operations within their borders.⁶⁴²

An example of this approach is Meta Inc's 2020 agreement with the Vietnamese government. The corporation agreed to restrict access to political content deemed illegal by the government in exchange for the government not slowing down Meta Inc.'s local servers.⁶⁴³ A former Facebook employee who worked in Asia revealed that the corporation was aware that the

⁶⁴⁰ See Scheck, Purnell & Horwitz, *supra* note 604.

⁶⁴¹ See Shoshana Zuboff et al, "Surveillance Capitalism: An Interview with Shoshana Zuboff" (2019) 17:1/2 *Surveillance & Society* 257 at 262; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 671–82.

⁶⁴² See Scheck, Purnell & Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers", *supra* note 604.

⁶⁴³ See Scheck, Purnell & Horwitz, *supra* note 604.

Vietnamese government was using the platform to stifle dissent, but tolerated this behaviour because Vietnam is a fast-growing advertising market.⁶⁴⁴

In conclusion, both Uber Inc. and Meta Inc. demonstrate a worrying lack of empathy in their relationships with workers, users, and society at large. Their actions often prioritize profit and growth over the well-being and safety of individuals.

5) Asocial Behaviour

Uber Inc.'s global expansion was largely driven by one personality trait: asocial behaviour. Uber Inc. aggressively expanded its business model worldwide, despite knowing that it was illegal in the majority of the cities in which it chose to operate. The leaked documents show that Uber Inc.'s expansion strategy consistently created regulatory crises in each new market.⁶⁴⁵

Rather than following standard licensing procedures or attempting to change existing local laws and regulations, Uber Inc. took a multifaceted approach. This strategy included attracting drivers with lucrative incentives, undercutting its competitors by offering rides at deeply discounted prices, and employing various strategies to deal with legal and regulatory challenges.⁶⁴⁶

In Europe, for instance, Uber Inc. executives categorized legal challenges into what they called a “pyramid of shit,” which included driver lawsuits, regulatory investigations, administrative proceeding, and direct litigation.⁶⁴⁷ When accused of violating regulations, the corporation would mobilize customers as grassroots lobbyists, encouraging them to sign petitions

⁶⁴⁴ See Scheck, Purnell & Horwitz, *supra* note 604.

⁶⁴⁵ See e.g., Medina & Sadek, “We Co-Opted Democracy”, *supra* note 602.

⁶⁴⁶ See Freedberg et al, “How Uber Won Access to World Leaders”, *supra* note 573.

⁶⁴⁷ See Freedberg et al, *supra* note 573.

to “save Uber.”⁶⁴⁸ And, when Uber Inc.’s agenda required academic support, it would pay friendly academics to produce research favourable to its business model.⁶⁴⁹

As MacGann told the European Parliament: “When politicians tried to stop us or slow us down, we co-opted democracy itself by leveraging consumers’ political power, putting very public pressure on elected officials to back off, drowning them in millions of driver petitions.”⁶⁵⁰ After putting pressure on the elected officials, Uber Inc. negotiated with them to secure legal reforms that would directly benefit the corporation.⁶⁵¹

The leaked documents revealed that Uber Inc. was not only aware of the illegality of its business model,⁶⁵² but also saw this unlicensed operation as critical to its financial success.⁶⁵³ For instance, in emails and text messages reviewed by *The Guardian*, executives acknowledged that fighting enforcement was necessary and “extremely strategic” to the corporation’s ability to scale its business in Europe.⁶⁵⁴

Uber Inc.’s asocial behaviour extended to its use of a technological tool designed to evade law enforcement. One of such tools, Greyball, was designed to deceive law enforcement officers and regulators by providing a fake view of the app to help its unlicensed drivers avoid detection.⁶⁵⁵

⁶⁴⁸ Freedberg et al, *supra* note 573.

⁶⁴⁹ See Freedberg et al, *supra* note 573; Davies et al, “Uber Broke Laws”, *supra* note 575.

⁶⁵⁰ Medina & Sadek, “We Co-Opted Democracy”, *supra* note 602.

⁶⁵¹ See Medina & Sadek, *supra* note 602.

⁶⁵² According to *The Guardian* article, in a 2014 email the then head of global communications said “sometimes we have problems because, well, we’re just fucking illegal.” Bhuiyan & Milmo, “Embrace the Chaos”, *supra* note 578.

⁶⁵³ See Bhuiyan & Milmo, *supra* note 578.

⁶⁵⁴ See Bhuiyan & Milmo, *supra* note 578.

⁶⁵⁵ In 2014, Gore-Coty, then Uber Inc.’s head of Western Europe, wrote an email to colleagues discussing the benefits of Greyball. In the email, he included a section titled ‘Fighting Enforcement’, highlighting its importance to Uber Inc.’s ability to grow its business. See Davies & Bhuiyan, “Uber Used Greyball Fake App To Evade Police”, *supra* note 562.

The tool targeted specific individuals suspected of being associated with law enforcement or regulatory agencies, using various data points (such as geolocation data, credit card details, and social media accounts) to identify them. These individuals would see a lack of cars in the area, or display phantom cars not associated with any real drivers.⁶⁵⁶

Another controversial tool, God View, allowed Uber Inc. to monitor the real-time movements of its customers. This was used to thwart sting operations in Brussels, where Uber Inc. staff actively monitored God View and if a potentially “risky” customer booked a ride, staff would instruct the driver to take a detour and then inform the customer through the app that they were stuck in traffic and could not pick them up, rather than immediately cancelling the ride.⁶⁵⁷

Uber Inc. also developed a “kill switch” system to prevent law enforcement from accessing certain data during raids on its offices.⁶⁵⁸ This system was implemented in response to a series of police raids and regulatory investigations to protect Uber Inc.’s unlicensed taxi service from being shut down, and to prevent the collection of incriminating evidence.⁶⁵⁹

⁶⁵⁶ See Davies & Bhuiyan, *supra* note 562.

See also Mike Isaac, “How Uber Deceives the Authorities Worldwide”, *The New York Times* (3 March 2017), online: <nytimes.com> [http://web.archive.org/web/20200210205756/https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html?searchResultPosition=1].

⁶⁵⁷ See Davies & Bhuiyan, “Uber Used Greyball Fake App To Evade Police”, *supra* note 562.

See also Isaac, “Uber Deceives the Authorities Worldwide”, *supra* note 656.

⁶⁵⁸ See Rob Davies & Simon Goodley, “Uber Bosses Told Staff to Use ‘Kill Switch’ During Raids to Stop Police Seeing Data”, *The Guardian* (10 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102170046/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/10/uber-bosses-told-staff-use-kill-switch-raids-stop-police-seeing-data].

⁶⁵⁹ For example, the leaked documents revealed that several weeks before a raid in Amsterdam, Uber Inc had taken precautions by renting an off-site storage facility, moving all necessary documents there, and compiling a list of all employees to ensure that a kill switch would be effective on the computers of everyone in the office. See Davies & Goodley, *supra* note 658.

Taken together, these tactics demonstrate Uber Inc.’s systematic approach to evading regulation and resisting enforcement efforts, and highlight the corporation’s asocial behaviour in its pursuit of rapid global expansion.

6) *Building and Maintaining a Deceptive “good neighbour” Image*

An example of Meta Inc. trait of building and maintain a deceptive “good neighbour” image was its rebranding from Facebook Inc. to Meta Inc. Conveniently, this rebranding was announced during the “Facebook Connect 2021” event in October, just one month after the Facebook Files were published. During this event and in the subsequent “Founder Letter,” the CEO of Meta Inc., Mark Zuckerberg, notably avoided addressing any of the allegations made in leaked documents. Instead, he focussed on the change of name and the corporation’s future plans around the metaverse, emphasizing that the corporation’s mission to “design technology around people” remained unchanged.⁶⁶⁰ This strategic shift effectively redirected public attention from the Facebook Files to the potential benefits of the metaverse and Meta Inc.’s role in making it a reality.

Meta Inc.’s’ response to online news legislation in Canada and Australia further illustrates the corporation’s “good neighbour” image, coupled with its refusal to take responsibility and tendency towards manipulative behaviour. In 2019, Meta Inc. introduced “Facebook News,” arguing that “journalism plays a critical role in our democracy. When news is deeply-reported and well-sourced it gives people information they can rely on. When it’s not, we lose an essential tool for making good decisions.”⁶⁶¹ However, in 2020, when Australia enacted legislating requiring

⁶⁶⁰ See Mark Zuckerberg, “Founder’s Letter, 2021” (28 October 2021) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221152944/https://about.fb.com/news/2021/10/founders-letter/].

⁶⁶¹ Campbell Brown, “Introducing Facebook News” (25 October 2019) online (Newsroom): <about.fb.com> [http://web.archive.org/web/20240526020429/https://about.fb.com/news/2019/10/introducing-facebook-news/].

digital platforms to pay publishers for news content, Meta Inc.'s' initial reaction was threatening to remove news from its platform altogether.⁶⁶² This stance, which leverages the corporation's influence over public access to information, was eventually softened when Meta Inc. reached an agreement with Australian publishers.

A similar scenario unfolded in Canada in 2023, when the government introduced a bill to require payments to publishers for news content.⁶⁶³ Meta Inc. lobbied against the bill, warning that it would restrict the access to all news content in the country if passed. The corporation downplayed the importance of news, claiming that only 3% of its global users consumed news on Facebook. This claim contradicted a survey showing that 24% of Canadians use Facebook for news, highlighting the platform's' significant role in the dissemination of information in Canada.⁶⁶⁴ After the bill was approved, Meta Inc. made good of its threat and banned all news content, a move that was criticized for affecting people's ability to stay informed during severe wildfires in the north of Canada.⁶⁶⁵

⁶⁶² See e.g., Will Easton, "An Update About Changes to Facebook's Services in Australia" (31 August 2020) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20240429055730/https://about.fb.com/news/2020/08/changes-to-facebooks-services-in-australia/].

⁶⁶³ This bill was different from the Australian counterpart, as Geist argued, the governments could have enacted a regulation with a more limited scope. See Michael Geist, "Why Is Meta Blocking All News Links? Because Bill C-18 Covers All News Outlets - Michael Geist" (11 August 2023) online (blog): <michaelgeist.ca> [http://web.archive.org/web/20240120074255/https://www.michaelgeist.ca/2023/08/why-is-meta-blocking-all-news-links-because-bill-c-18-covers-all-news-outlets/].

⁶⁶⁴ See e.g., Ashley Belanger, "Meta Won't Negotiate with Publishers, Will End Facebook News in Canada", *Ars Technica* (23 June 2023), online: <arstechnica.com> [http://web.archive.org/web/20240227094559/https://arstechnica.com/tech-policy/2023/06/facebook-cutting-off-news-in-canada-to-avoid-paying-publishers-for-content/]; "Canada Social Media Sites Used for News 2023" (last visited 24 May 2024) online (Statista): <statista.com> [http://web.archive.org/web/20231004200730/https://www.statista.com/statistics/563514/social-networks-used-for-news-canada/].

⁶⁶⁵ See e.g., Tracey Lindeman, "'Disaster': Warning for Democracy As experts Condemn Meta over Canada news ban", *The Guardian* (4 August 2023), online: <theguardian.com> [http://web.archive.org/web/20240404081941/https://www.theguardian.com/world/2023/aug/04/canada-meta-news-ban-facebook-fake]; Hibaq Farah, "How is Meta's News Ban Affecting Communications Amid Canada Wildfires?", *The Guardian* (18 August 2023), online: <theguardian.com>

In March 2024, Meta Inc. announced that it would remove its News tab globally and stop paying publishers, prioritizing profitability over its stated goal of keeping users informed.⁶⁶⁶ These actions suggest that Meta Inc.’s initial commitment to news was more about user engagement than supporting journalism. When regulations threatened its revenue model, Meta Inc. chose to withdraw from news distribution rather than negotiate sustainable solutions, reflecting a broader trend of the corporation prioritizing profits over social responsibility in its influential role in public discourse.

For corporations with data-driven business models, maintaining an image of caring about privacy is crucial. Waldman points out that these corporations rely on the corporate rhetoric of “we care about your privacy,” constantly reassure people that they can be trusted with their data. However, he argues that corporations are aware of the public distrust,⁶⁶⁷ and therefore corporations use the privacy discourse as a marketing tool, rather than a genuine commitment.⁶⁶⁸ These declarations about the importance of privacy, trust, loyalty, and care serve to conceal the reality of their data policies, which involve the extensive collection, processing, and commercialization of individuals’ data for financial gain.⁶⁶⁹

[<http://web.archive.org/web/20240516005031/https://www.theguardian.com/world/2023/aug/18/how-is-meta-news-ban-affecting-communications-amid-canada-wildfires-facebook>].

⁶⁶⁶ See e.g., Richard Lawler, “Facebook Will Remove its News Tab and Stop Paying Publishers for News”, *The Verge* (1 March 2024), online: <[theverge.com](https://www.theverge.com)> [<https://www.theverge.com/2024/2/29/24087220/facebook-news-tab-united-states-australia>]; Meta, “An Update on Facebook News” (1 March 2024) online (Newsroom): <about.fb.com> [<http://web.archive.org/web/20240523143912/https://about.fb.com/news/2024/02/update-on-facebook-news-us-australia/>].

⁶⁶⁷ See Waldman, *Industry Unbound*, *supra* note 15 at 75.

⁶⁶⁸ See Joseph Turow et al, “The Federal Trade Commission and Consumer Privacy in the Coming Decade” (2007) 3:3 I/S: A Journal of Law and Policy for the Information Society 723 at 747 referenced by Waldman, *Industry Unbound*, *supra* note 15.

⁶⁶⁹ See Waldman, *Industry Unbound*, *supra* note 15.

Waldman’s research found that these corporations also construct this privacy-friendly image through a variety of means: advertising campaigns that promote privacy-friendly product design,⁶⁷⁰ public communications that reassure users about privacy,⁶⁷¹ sponsorship of events dedicated to data protection, privacy, and human rights in the digital age,⁶⁷² and membership in pro-privacy associations.⁶⁷³ This benevolent “good neighbour” image extends beyond individual users to influence regulators, leading to rules that require these corporations to act as protectors of

⁶⁷⁰ See e.g., Google, “Google Privacy & Security” (last visited 1 August 2023) online (video): <youtube.com> [http://web.archive.org/web/20231221124225/https://www.youtube.com/playlist?list=PL590L5WQmH8cDdey4_8Fy9qJnkHWFxcDg]; Meta, “Facebook Here Together (UK)” (25 April 2018) online (video): <youtube.com> [http://web.archive.org/web/20231220131821/https://www.youtube.com/watch?v=Q4zd7X98eOs]; Apple, “Privacy on iPhone: The Waiting Room” (24 May 2023) online (video): <youtube.com> [http://web.archive.org/web/20231221121550/https://www.youtube.com/watch?v=4-7jSoINyq4].

⁶⁷¹ See e.g., Tim Cook, “You Deserve Privacy Online. Here’s How You Could Actually Get It”, *Time* (2019), online: <time.com> [http://web.archive.org/web/20220618030148/https://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/]; Sundar Pichai, “Google’s Sundar Pichai: Privacy Should Not Be a Luxury Good”, *The New York Times* (8 May 2019), online: <nytimes.com> [http://web.archive.org/web/20190701181756/https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html]; Charlotte Jee, “Google Has Promised to Make it Easier to Protect your Privacy”, *MIT Technology Review* (8 May 2019), online: <technologyreview.com> [http://web.archive.org/web/20240102133757/https://www.technologyreview.com/2019/05/08/135461/google-has-promised-to-make-it-easier-to-protect-your-privacy/]; Mark Zuckerberg, “A Privacy-Focused Vision for Social Networking” (26 September 2018) online: <facebook.com/notes/mark-zuckerberg> [https://webcache.googleusercontent.com/search?q=cache:Ts_epQrWoysJ:https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/&cd=1&hl=en&ct=clnk&gl=ch]; Karissa Bell, “Mark Zuckerberg Promises to Rebuild Facebook as ‘Privacy-Focused’ Social Network”, *Mashable* (6 March 2019), online: <mashable.com> [http://web.archive.org/web/20240102145430/http://web.archive.org/screenshot/https://mashable.com/article/mark-zuckerberg-privacy-focused-social-network].

⁶⁷² Such as RightsCon featuring companies such as Google, Microsoft, Amazon, Meta, and Apple, and consultation events organized by Human Rights Council. See e.g., RightsCon, “Welcome to all RightsCon Sponsors” (last visited 2 August 2023) online: <rightscon.org> [http://web.archive.org/web/20231220142454/https://www.rightscon.org/sponsors/]; UN, *Report of the Special Rapporteur on the Right to Privacy*, HRC, 43th Sess, UN Doc A/HRC/43/52 (2020) at 2.

Also IAPP conferences featuring companies such as Meta and Google, and CPDP featuring companies like Apple, Meta, Google, Microsoft, and Uber. See e.g., IAPP, “IAPP Europe Data Protection Congress 2023” (last visited 2 August 2023) online: <iapp.org> [http://web.archive.org/web/20230810214727/https://iapp.org/conference/iapp-europe-data-protection-congress/]; CPDP Conferences, “CPDP 2023 Sponsors” (last visited 2 August 2023) online: <cpdpconferences.org> [http://web.archive.org/web/20231221114859/https://www.cdpconferences.org/sponsors-and-partners/platinum-sponsors].

⁶⁷³ For instance, the Global Network Initiative is an alliance of various stakeholders including technology corporations (such as Meta, Google, and Microsoft), which mission is “to protect and advance freedom of expression and privacy in the ICT industry globally.” See Global Network Initiative, “The GNI Principles” (last visited 2 December 2022) online: <globalnetworkinitiative.org> [http://web.archive.org/web/20231220132905/https://globalnetworkinitiative.org/gni-principles/] at preamble.

their users. For example, recent regulatory proposals require corporations that provide online services accessible to children to protect them from harmful content and practices on their platforms.⁶⁷⁴ By complying with such regulation, these corporations can reinforce their benevolent image by implementing measures such as enhanced parental controls and age-appropriate design,⁶⁷⁵ without fundamentally changing their business model or addressing underlying issues such as addiction.⁶⁷⁶

Waldman noted that corporations also remind individuals of their commitment to privacy through tools such as privacy policies and direct communications. For example, when the GDPR came into force, corporations sent emails to their users informing them of changes to their privacy policies, framing mandatory legal compliance as a proactive measure.⁶⁷⁷ Similarly, both Uber Inc. and Meta Inc. have celebrated “Data Privacy Day”⁶⁷⁸ annually for at least the past three years,

⁶⁷⁴ See e.g., Bill C-63, Online Harms Act, 1st reading, *House of Commons*, 44-1, (26 February 2024) online: <parl.ca> [http://web.archive.org/web/20240421093611/https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading] arts 64–66.

See also Lorna Woods & Will Perrin, “Obliging Platforms to Accept a Duty of Care” in Martin Moore & Damian Tambini, eds, *Regulating Big Tech: Policy Responses to Digital Dominance* (New York: Oxford University Press, 2021) 93; EU, *Regulation of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC*, [2022] OJ, L 277/ 1 [*Digital Services Act*] art 28.

⁶⁷⁵ See e.g., Meta, “New Protections to Give Teens More Age-Appropriate Experiences on Our Apps” (9 January 2024) online (Newsroom): <about.fb.com> [http://web.archive.org/web/20240421205258/https://about.fb.com/news/2024/01/teen-protections-age-appropriate-experiences-on-our-apps/]; Meta, “Continuing to Create Age-Appropriate Ad Experiences for Teens” (10 January 2023) online (Newsroom): <about.fb.com/> [http://web.archive.org/web/20240406183038/https://about.fb.com/news/2023/01/age-appropriate-ads-for-teens/].

⁶⁷⁶ See e.g., Kari Paul, “Meta Sued by 33 States over Claims Youth Mental Health Endangered by Instagram”, *The Guardian* (24 October 2023), online: <theguardian.com> [http://web.archive.org/web/20240202090915/https://www.theguardian.com/technology/2023/oct/24/instagram-lawsuit-meta-sued-teen-mental-health-us]; Cecilia Kang & Mike Isaac, “State Attorneys General Open an Inquiry into Instagram’s Impact on Teens.”, *The New York Times* (18 November 2021), online: <nytimes.com> [http://web.archive.org/web/20240224093949/https://www.nytimes.com/2021/11/18/technology/meta-instagram-investigation-teens.html].

⁶⁷⁷ See Waldman, *Industry Unbound*, *supra* note 15 at 75.

⁶⁷⁸ This is a date set by the Council of Europe in 2006 to “raise awareness about the rights to personal data protection and privacy.” Council of Europe, “28 January: Data Protection day” (last visited 12 October 2023) online: <coe.int> [http://web.archive.org/web/20231219170934/https://www.coe.int/en/web/portal/28-january-data-protection-day].

using this internationally recognized date to reaffirm their privacy commitment through in-app messages to users,⁶⁷⁹ and blog posts outlining advances in privacy features of their products.

For example, in 2023, Uber launched a new privacy product in the US and Canada,⁶⁸⁰ while in 2022, it introduced its “Privacy Center,” and in 2021,⁶⁸¹ it published its “Privacy Principles.”⁶⁸² Similarly, in 2023, Meta published the third iteration of its “Privacy Progress Update,” and summarized all the work it has done to advance privacy in its products.⁶⁸³ In 2022, it rolled out encryption updates on Messenger, and announced new investments in privacy research,⁶⁸⁴ while in 2021, it revisited some of its recent privacy product updates.⁶⁸⁵

An important aspect of this discourse is that while these corporations constantly emphasize the importance of privacy, they rarely define what privacy means to them.⁶⁸⁶ This ambiguity, also part of their manipulative trait, allows them to shape the concept of privacy in a way that suits their interests.⁶⁸⁷ Waldman observed that these corporations often present themselves as remorseful and

⁶⁷⁹ See e.g., Zefo, “Introducing Uber’s Privacy Center”, *supra* note 542; Erin Egan, “Marking Data Privacy Day 2019” (28 January 2019) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20230923021031/https://about.fb.com/news/2019/01/data-privacy-day/].

⁶⁸⁰ See Jessie Yang, “5 Tips to Protect Your Data Privacy with Uber” (26 January 2023) online (blog): <medium.com/uber-security-privacy/> [http://web.archive.org/web/20231221142446/https://medium.com/uber-security-privacy/5-tips-to-protect-your-data-privacy-with-uber-d6e2edf792f9].

⁶⁸¹ See Zefo, “Introducing Uber’s Privacy Center”, *supra* note 540.

⁶⁸² See Ruby Zefo, “Celebrating Data Privacy Day” (26 January 2019) online (Uber Newsroom): <https://www.uber.com/newsroom/celebrating-data-privacy-day/>.

⁶⁸³ See Michel Protti, “Building and Innovating With Privacy in Mind” (23 January 2023) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221150511/https://about.fb.com/news/2023/01/building-and-innovating-with-privacy-in-mind/].

⁶⁸⁴ See Meta, “Recapping Our Privacy Efforts on Data Privacy Day” (28 January 2022) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20230913013408/https://about.fb.com/news/2022/01/recapping-our-privacy-efforts-on-data-privacy-day/].

⁶⁸⁵ See Meta, “Recapping Our Privacy Controls on Data Privacy Day” (28 January 2021) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20230520175443/https://about.fb.com/news/2021/01/recapping-our-privacy-controls-on-data-privacy-day/].

⁶⁸⁶ See Waldman, *Industry Unbound*, *supra* note 15 at 76.

⁶⁸⁷ The manipulative trait of corporations was developed in detail in Part I-B.1, *above*.

committed to improving their privacy obligations,⁶⁸⁸ as long as privacy is consistent with their interpretation.⁶⁸⁹

In conclusion, the constant reiteration of the importance of privacy in corporate communications and product releases serves to reinforce the “good neighbour” image. Corporations reaffirm their commitment to privacy and outline the steps they have taken to protect it in their products and services, without providing concrete explanations of what these actions entail. For instance, Meta Inc.’s launch of Generative AI in 2023 was accompanied by a blog post entitled “Privacy Matters: Meta’s Generative AI Features,”⁶⁹⁰ which began by asserting that, as with other Meta Inc. products, the corporation has taken steps to protect individuals’ privacy and “offer greater transparency,” in developing, “these exciting new features.” Aside from stating that the corporation had “developed privacy mitigations through [their] privacy review process and external engagements,”⁶⁹¹ the blog post provided few details about the actual policies implemented or what it meant by privacy.

This part analyzed Uber Inc. and Meta Inc. as two examples of corporations that provide LBS and have data-driven business models. By examining recent events, their communications with users, and their annual reports, it was shown that these corporations exhibit psychopathic tendencies, consistent with Bakan’s theory.

The following part focusses on mass dataveillance systems as one facet of this psychopathic personality. Using location dataveillance as an example, this part first examines the

⁶⁸⁸ See Waldman, *Industry Unbound*, *supra* note 15 at 4.

⁶⁸⁹ See Waldman, *Industry Unbound*, *supra* note 15 at 47.

⁶⁹⁰ Mike Clark, “Privacy Matters: Meta’s Generative AI Features” (27 September 2023) online (Newsroom): <about.fb.com/news> [<http://web.archive.org/web/20231010061401/https://about.fb.com/news/2023/09/privacy-matters-metas-generative-ai-features/>].

⁶⁹¹ Clark, *supra* note 690.

technological capabilities that enable corporations to implement data-driven business models. It then moves on to explain the economic model in which corporations with data-driven business models operate, and will highlight the risks and harms created by these systems.

III. Mass Dataveillance Systems as a Facet of Corporate Pathology: The Example of Location Dataveillance

The current technological context is characterized by devices equipped with various sensors that collect data about the environment and the behaviours of individuals.⁶⁹² These interconnected sensors form a wireless network⁶⁹³ that enables corporations to use machine learning to understand people's behaviour, both as individuals and socially, effectively bridging the gap between the virtual and physical worlds.⁶⁹⁴ Central to this bridge is location data, which provide critical information about the geographic location of people and objects at specific times and dates.⁶⁹⁵

Location data have become increasingly valuable to corporations, with one marketer describing it to the *New York Times* as the “the Holy Grail of advertising” because of their ability

⁶⁹² See e.g., Friedemann Mattern & Christian Floerkemeier, “From the Internet of Computers to the Internet of Things” in Kai Sachs, Ilia Petrov & Pablo Guerrero, eds, *From Active Data Management to Event-Based Systems and More* (Berlin: Springer, 2010) 242.

⁶⁹³ See Pentland, “Society's Nervous System”, *supra* note 10 at 32; Fosca Giannotti & Dino Pedreschi, “Mobility, Data Mining and Privacy: A Vision of Convergence” in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 1 at 2.

⁶⁹⁴ See e.g., Friedemann Mattern & Christian Floerkemeier, “From the Internet of Computers to the Internet of Things” in Kai Sachs, Ilia Petrov & Pablo Guerrero, eds, *From Active Data Management to Event-Based Systems and More* (Berlin: Springer, 2010) 242 at 244.

⁶⁹⁵ See e.g., Ehsan Ahvar et al, “On Analyzing User Location Discovery Methods in Smart Homes: A Taxonomy and Survey” (2016) 76 *Journal of Network and Computer Applications* 75 at 76; Aztiria Asier, Juan Carlos Augusto & Izaguirre Alberto, “Spatial and Temporal Aspects for Pattern Representation and Discovery in Intelligent Environments” (Paper delivered at the Workshop on Spatial and Temporal Reasoning at 18th European Conference on Artificial Intelligence, Patras, Greece, July 2008) [unpublished] online: <<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7f0ed8fabe7cc6f7dd684e15568fcb773cc6f3ae>> at 1; Liang Chen et al, “Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey” (2017) 5 *IEEE Access* 8956.

to provide a “complete picture that connects all our interests and online activity with our real-world actions.”⁶⁹⁶ The shift to smart mobile devices, wearable computing, and the Internet of Things (IoT) has greatly expanded the availability of location data, making commercial data collection an almost continuous process.⁶⁹⁷

This market shift goes hand in hand with the architecture of the physical world being embedded or augmented by the increasing presence of network infrastructure, such as Wi-Fi access points, cell towers, and Bluetooth beacons around the globe.⁶⁹⁸ This infrastructure is critical for mobile devices to determine their location as they move. The ubiquity of these networks means that, as people move around, the mobile devices that they carry with them are “communicating” with them more frequently.

Using artificial intelligence techniques, corporations can map these networks, aggregating and analyzing data from multiple sensors to create a more accurate picture of people’s movement patterns.⁶⁹⁹ As technologies with location capabilities become more integrated into indoor and outdoor architecture, they are reshaping the physical spaces in which people live and interact.⁷⁰⁰

⁶⁹⁶ Thompson & Warzel, “Twelve Million Phones”, *supra* note 553.

⁶⁹⁷ See Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, (New York: Oxford University Press, 2019) at 57.

⁶⁹⁸ See Mozilla Location Service, “Statistics” (last visited 21 October 2020) online: <location.services.mozilla> [http://web.archive.org/web/20231221121039/https://location.services.mozilla.com/stats].

See also Quoc Duy Vo & Pradipta De, “A Survey of Fingerprint-Based Outdoor Localization” (2016) 18:1 IEEE Communications Surveys Tutorials 491; Anthony LaMarca & Eyal de Lara, *Location Systems: An Introduction to the Technology Behind Location Awareness*, (Morgan & Claypool, 2008) at 34–39; Ramon F Brena et al, “Evolution of Indoor Positioning Technologies: A Survey” (2017) Journal of Sensors 1 at 5; *Location Sensing Techniques*, by Jeffrey Hightower & Gaetano Borriello, UW CSE 01-07-01 (University of Washington, Department of Computer Science and Engineering, 2001); Apple, “iBeacon” (last visited 21 October 2019) online: <developer.apple.com> [http://web.archive.org/web/20231221122652/https://developer.apple.com/ibeacon/].

⁶⁹⁹ For instance, Skyhook, a data analytics company, allows companies to locate, “devices using Wi-Fi, GNSS and Cell signals, ensuring that all devices can be located in all environments.” Skyhook Wireless Inc, “Locate and Position Devices Worldwide” (last visited 23 October 2020) online: <skyhook.com> [http://web.archive.org/web/20210612141916/https://www.skyhook.com/precision-location].

⁷⁰⁰ See Cresswell, *Place*, *supra* note 268 at 147.

This restructuring is significant because people do not go about their daily activities in a vacuum, but they live and behave in material places where the concrete structure and properties of these physical spaces constrain their actions.⁷⁰¹ This increasing ubiquity of digital technologies in everyday life makes it increasingly difficult for individuals to avoid being monitored and enables certain corporations to constantly monitor the movements of individuals.

Technological advances that allow corporations to generate revenue from the collection and processing of data about individuals and their behaviour, combined with a pathological personality that prioritizes profit above all else, have led to the implementation and maintenance of extensive corporate mass dataveillance systems. These systems are characterized by the routine collection and storage of data about individuals and their behaviour, and the organization of the data to support decision-making about those individuals.⁷⁰²

This section is divided into three parts. First, it examines the technological capabilities that enable corporations to implement data-driven business models, using location dataveillance as an example. It explains how digital technologies generate and collect location data, which are essential to the functioning of mass dataveillance systems, and how these serve as valuable business assets for many corporations. The second section uses Zuboff's theory of surveillance capitalism as a framework to analyze the economic model in which corporate mass dataveillance systems are implemented and maintained. Finally, the third section examines the potential risks these systems pose to individuals and society, which help to highlight the need for effective regulation of these systems.

⁷⁰¹ See Cresswell, *Place*, *supra* note 268 at 70; N Andrienko et al, "Basic Concepts of Movement Data" in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 15 at 20–22.

⁷⁰² This is in line with the definition provided by Rule about the systems of mass surveillance. See Rule, *Privacy in Peril*, *supra* note 8 at 14.

A. From Human Mobility to Digital Movement Records

Individuals move; they move to go to work, to eat, to exercise, and to interact with people. They move to survive, to be part of society. In this sense, mobility “is a fact of life. To be human, indeed, to be an animal, is to have some kind of capacity for mobility. We experience the world as we move through it.”⁷⁰³ Digital technologies with location capabilities generate and collect data about this way of experiencing.

Movement was observed long before the development of location technologies.⁷⁰⁴ However, digital technologies have changed the way individuals perceive and process location information, making it possible to “store and analyze location not as a place per se, but as data.”⁷⁰⁵ This has created the possibility “of pursuing the *archaeology of the present*: discovering, in real time, precise representations of what we do, how and where we do it through the digital traces of our mobility activity.”⁷⁰⁶

This section is divided into three subsections. First it examines the different localization techniques used by digital technologies, followed by the identification methods used to link these data to a specific entity (individuals or devices). Building on this, the third subsection examines how corporations can use location data to create movement records for specific entities and how they use these records.

⁷⁰³ Tim Cresswell, *On the Move: Mobility in the Modern Western World*, (New York: Routledge, 2006) at 22.

⁷⁰⁴ See Andrienko et al, “Basic Concepts of Movement Data”, *supra* note 701.

⁷⁰⁵ Kenneth Cukier & Viktor Mayer-Schönberger, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, (Boston: Houghton Mifflin Harcourt, 2013) at 87.

⁷⁰⁶ Pedreschi et al, “Privacy Protection”, *supra* note 31 at 102.

1) Localization Techniques

Location is an integral part of many devices that people use every day for navigation, home security, fitness tracking, and communication. These devices create a digital record that can pinpoint the location of an entity, whether a person or a device, at any given time. There are three main techniques for automatically determining this location: triangulation, scene analysis, and proximity sensing.⁷⁰⁷ The choice of technique depends on a number of factors, including whether the locations need to be determined outdoors or indoors, the geographical and physical configuration of the terrain, the desired granularity according to the purpose of the data, and the available infrastructure.

Triangulation techniques use multiple sensors to determine the location of an entity.⁷⁰⁸ The position is calculated by measuring the distance (trilateration) or angles (triangulation) created by the entity and the reference sensors.⁷⁰⁹ For instance, in the case of Global Navigation Satellite Systems (GNSS),⁷¹⁰ a device such as a GPS navigator sends and receives a signal from a number

⁷⁰⁷ See Robert Minch, “Issues in the Development of Location Privacy Theory”(Paper delivered at the 44th Hawaii International Conference on System Sciences, Kauai, HI, January 4-7, 2011) in Ralph H. Sprague, ed, *Proceedings HICSS 2011* (California: IEEE, 2011), DOI:<10.1109/HICSS.2011.262> at 5; Eddie C L Chan & George Baciú, *Introduction to Wireless Localization*, (Singapore: John Wiley & Sons, 2012) at 35; Hightower & Borriello, *Location Sensing Techniques*, *supra* note 698.

For other classification of these techniques see Brena et al, “Evolution of Indoor Positioning Technologies”, *supra* note 698.

⁷⁰⁸ See Hightower & Borriello, *Location Sensing Techniques*, *supra* note 698; Laoudias et al, “Survey of Enabling Technologies”, *supra* note 257; Brena et al, “Evolution of Indoor Positioning Technologies”, *supra* note 698 at 3–4.

⁷⁰⁹ The location can be estimated using different measurements such as signal strengths (RSS), time of arrival (ToA), and time difference of arrival (TDoA). For a detail explanation of each of these measurement techniques see Seyed A Reza Zekavat, Stuti Kansal & Allen H Levesque, “Wireless Positioning Systems: Operation, Application, and Comparison” in Seyed A Reza Zekavat & R Michael Buehrer, eds, *Handbook of Position Location* (Hoboken, NJ, USA: John Wiley & Sons, 2011) 3 at 5–8; Chan & Baciú, *Introduction to Wireless Localization*, *supra* note 707 at 37–46; Ali Yassin et al, “Recent Advances in Indoor Localization: A Survey on Theoretical Approaches and Applications” (2017) 19:2 IEEE Communications Surveys Tutorials 1327 at 1329–1330; Laoudias et al, “Survey of Enabling Technologies”, *supra* note 257 at 3609–3611.

⁷¹⁰ There are in place different GNSS systems: the US GPS system, such as the EU Galileo system, the Russian GLONASS system, the Chinese BeiDou.

of satellites, which provides a set of coordinates (latitude, longitude, and altitude) representing the geographical position at that moment, and throughout the journey.⁷¹¹

Scene analysis, or fingerprint-based localization, determines the location of a device by collecting environmental features and matching them against a pre-existing database.⁷¹² This technique differs from the other two in that it always requires an *a priori* step to build the geotagging database that will be used to match the observed features. This technique includes signal, motion, and visual fingerprinting.⁷¹³

Signal fingerprinting determines a device's location by comparing signals received from different Wi-Fi access points or cell towers to a database,⁷¹⁴ while motion fingerprinting uses data from motion sensors such as an accelerometer and gyroscope to estimate distance and direction of travel.⁷¹⁵ Visual fingerprinting compares images taken by a device, such as the architecture or geography of a location, to a database of geotagged images.⁷¹⁶

Proximity techniques locate objects or people when they approach or come into contact with a sensor at a known location.⁷¹⁷ These techniques use a variety of sensors, from Bluetooth beacons and Wi-Fi access points,⁷¹⁸ to video or audio-enabled sensors.⁷¹⁹ Unlike the previous two

⁷¹¹ For a technical explanation of how GPS work, see Zekavat, Kansal & Levesque, “Wireless Positioning Systems”, *supra* note 709 at 9–12; LaMarca & de Lara, *Location Systems*, *supra* note 698 at 7–16.

⁷¹² For an explanation of the different stages of the fingerprint-based localization techniques, see Vo & De, “Survey of Fingerprint-Based Outdoor Localization”, *supra* note 698..

⁷¹³ See Vo & De, “Survey of Fingerprint-Based Outdoor Localization”, *supra* note 698.

⁷¹⁴ See Vo & De, “Survey of Fingerprint-Based Outdoor Localization”, *supra* note 698; LaMarca & de Lara, *Location Systems*, *supra* note 698 at 34–39.

⁷¹⁵ See Vo & De, “Survey of Fingerprint-Based Outdoor Localization”, *supra* note 698 at 495–96.

⁷¹⁶ See Vo & De, “Survey of Fingerprint-Based Outdoor Localization”, *supra* note 698 at 492.

⁷¹⁷ See Brena et al, “Evolution of Indoor Positioning Technologies”, *supra* note 698 at 5.

⁷¹⁸ See Brena et al, “Evolution of Indoor Positioning Technologies”, *supra* note 698; Hightower & Borriello, *Location Sensing Techniques*, *supra* note 698.

⁷¹⁹ For instance, video cameras, and in-car positioning systems and home assistants who use voice profiles to recognize (and position) an individual.

techniques, this technique can be used to locate not only entities that are carrying a tag or sensor (e.g., Bluetooth-enabled tag⁷²⁰), but also entities that do not carry a sensor (e.g., an individual captured by a video camera).⁷²¹

2) Identification Methods

Location data collected using any of the location techniques described above can be associated with a specific entity in three scenarios: device-based identification, biometric identification, and movement pattern identification.

In the first scenario, data are collected and stored with a unique device identifier. For instance, when a device's location is determined by using the existing Wi-Fi infrastructure, the base station collects the device's MAC addresses and SSID to identify each device.⁷²² In the second scenario, in combination with a biometric system,⁷²³ the location data are collected and stored with a biometric identifier, which can be almost any human physiological or behavioural

See e.g., Jorge Torres-Solis, Tiago H Falk & Tom Chau, "A Review of Indoor Localization Technologies: towards Navigational Assistance for Topographical Disorientation" in Felix Jesus Villanueva Molina, ed, *Ambient Intelligence* (InTech, 2010) at 62–68; Michael Feld, Tim Schwartz & Christian Müller, "This Is Me: Using Ambient Voice Patterns for In-Car Positioning" (Paper delivered at the First International Joint Conference Aml, Málaga, Spain, November 10-12, 2010) in Boris Ruyter et al, eds, *Ambient Intelligence* (Berlin: Springer, 2010) 290, DOI:<10.1007/978-3-642-16917-5_33>; Google, "Voice Match and Media on Google Nest and Google Home speakers and displays" (last visited 31 August 2020) online (Help Center): <support.google.com> [http://web.archive.org/web/20231221115839/https://support.google.com/googlenest/answer/7342711].

⁷²⁰ See e.g., Apple, "iBeacon", *supra* note 698.

⁷²¹ See LaMarca & de Lara, *Location Systems*, *supra* note 698 at 59.

This technique is also used in some cases for machine-to-machine communication. See e.g., Mattern & Floerkemeier, "From the Internet of Computers to the Internet of Things", *supra* note 694.

⁷²² See LaMarca & de Lara, *Location Systems*, *supra* note 698 at 33.

⁷²³ See Anil K Jain & Arun Ross, "Introduction to Biometrics" in Anil K Jain, Patrick Flynn & Arun A Ross, eds, *Handbook of Biometrics* (Boston, MA: Springer US, 2008) 1.

See also Jessica Gabel Cino, "Facial Recognition is Increasingly Common, but How Does It Work?" (4 April 2017) online (blog): <theconversation.com> [http://web.archive.org/web/20231221152836/https://theconversation.com/facial-recognition-is-increasingly-common-but-how-does-it-work-61354].

characteristic,⁷²⁴ such as facial images,⁷²⁵ gait,⁷²⁶ voice,⁷²⁷ or infrared images.⁷²⁸ In the last scenario, data collected and stored without an identifier can be associated with an entity based on their movement patterns.⁷²⁹ For instance, one study found that it was possible to identify 95% of individuals from anonymized mobile phone records using three spatiotemporal points,⁷³⁰ concluding that due to the uniqueness of human mobility data, “Little outside information is

⁷²⁴ See AK Jain, A Ross & S Prabhakar, “An Introduction to Biometric Recognition” (2004) 14:1 IEEE Transactions on Circuits and Systems for Video Technology 4; WP29, *Working Document on Biometrics*, 12168/02/EN WP 80 (2003); Information and Privacy Commissioner Ontario, *Privacy and Biometrics*, by Ann Cavoukian, (Toronto: IPC-ON, 1999) at 9–10.

⁷²⁵ See e.g., Kate Conger, Richard Fausset & Serge F Kovaleski, “San Francisco Bans Facial Recognition Technology”, *The New York Times* (14 May 2019), online: <nytimes.com> [http://web.archive.org/web/20220709132351/https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html]; Spencer Soper, “Amazon Pitches Facial Recognition to Monitor Immigrants”, (23 October 2018), online: <bloomberg.com> [http://web.archive.org/web/20181106103109/https://www.bloomberg.com/news/articles/2018-10-23/amazon-pitches-facial-recognition-tools-to-monitor-immigrants].

⁷²⁶ See e.g., Yasushi Makihara, Mark S Nixon & Yasushi Yagi, “Gait Recognition: Databases, Representations, and Applications” in Katsushi Ikeuchi, ed, *Computer Vision: A Reference Guide* (Cham: Springer, 2020) 1; Mohammad Omar Derawi et al, “Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition”(Paper delivered at the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany, 15-17 October 2010) in Isao Echizen et al, eds, *Proceedings IIHMSP 2010* (California: IEEE, 2010) 306, DOI:<10.1109/IIHMSP.2010.83>; Ryan O’Hare, “Software Analyses Your Unique Gait from CCTV Footage”, *Daily Mail* (15 February 2016), online: <dailymail.co.uk> [http://web.archive.org/web/20240102160415/http://web.archive.org/screenshot/https://www.dailymail.co.uk/science/article-3447957/Nowhere-run-Software-identify-way-WALK-using-grainy-CCTV-footage.html].

⁷²⁷ See e.g., Chris Welch, “Amazon’s Alexa Can Now Recognize Different Voices and Give Personalized Responses”, (11 October 2017), online: <theverge.com> [http://web.archive.org/web/20181023112538/https://www.theverge.com/circuitbreaker/2017/10/11/16460120/amazon-echo-multi-user-voice-new-feature]; Lisa Eadicicco, “Amazon Developing Advanced Voice-Recognition for Alexa”, *Time* (27 February 2017), online: <time.com> [http://web.archive.org/web/20180308102426/https://time.com/4683981/amazon-echo-voice-id-feature-2017/]; Hayley Tsukayama, “Why It Matters that Google Home Can Now Identify You by Voice”, *The Washington Post* (20 April 2017), online: <washingtonpost.com> [http://web.archive.org/web/20170421012451/https://www.washingtonpost.com/web/20170421012451/https://www.washingtonpost.com/news/the-switch/wp/2017/04/20/why-it-matters-that-google-home-can-now-identify-you-by-voice/?utm_term=.8e5e3b86e2aa].

⁷²⁸ See e.g., Reza Shoja Ghiass et al, “Infrared Face Recognition: A Comprehensive Review of Methodologies and Databases” (2014) 47 Pattern Recognition 2807.

⁷²⁹ See e.g., Rossi, Walker & Musolesi, “User Identification by GPS Mobility Data”, *supra* note 75. See also Chapter II-A.2.b, *above*.

⁷³⁰ See de Montjoye et al, “Unique in the Crowd”, *supra* note 26. See also Song, Dahlmeier & Bressan, “Not so Unique in the Crowd”, *supra* note 80.

needed to re-identify the trace of a targeted individual even in a sparse, large scale, and coarse mobility dataset.”⁷³¹

3) Movement Records

Technological advances have made it easier for corporations to combine location data from multiple devices and sources over time.⁷³² This interconnectivity makes location data particularly invasive compared to other types of data, as they are collected continuously and covers a wide range of individuals’ activities in the physical world.

Using algorithmic processing, corporations can analyze location data and identify relationships between data points, such as linking groups of people to specific locations or tracking individual visitation patterns. In addition, using any of the identification techniques described above, corporations can compile detailed mobility patterns for specific entities, creating comprehensive movement records.

Movement records can be categorized into three groups based on the source of the location data: location data generated by a single device and collected by a single corporation; location data generated by a single device but collected by multiple corporations; and location data generated by multiple devices.

First, a corporation may aggregate location data collected by its own technologies, products, or services. These data are typically associated with a unique identifier that allows the corporation to associate the data with a user’s account. Depending on the service, these records

⁷³¹ de Montjoye et al, “Unique in the Crowd”, *supra* note 26 at 4.

⁷³² See Pedreschi et al, “Privacy Protection”, *supra* note 31 at 115.

may provide patterns of movement across the network coverage (e.g., telecommunications services),⁷³³ or indicate when a device is in a particular location (e.g., smart home services).⁷³⁴

The second way that corporations can create movement records is by aggregating the location data generated by a single device but collected by different corporations. In these cases, the location data are collected using the same device identifier (e.g., advertising ID or MAC address), allowing corporations such as data brokers to aggregate the location data from different applications into a single record.⁷³⁵ As Calacci et al. explain:

The different applications on our phones may only collect our location data in limited intervals, such as when they are in use or running in the background, depending on the privacy settings we have set. However, the aggregate of this data reported from these various applications is what the data brokers obtain. The resulting datasets detail the daily movements of hundreds of millions of people.⁷³⁶

Finally, corporations can create a movement record by aggregating location data from multiple sensors and linking them to a common identifier, such as an email,⁷³⁷ or biometric.⁷³⁸ For instance, Amazon's One system uses the uniqueness of palms for identification;⁷³⁹ every time a person scans their palm in a store, a record is created that locates that person in that store. Amazon Inc. can then aggregate these data to create a record of where that person has been.

⁷³³ See Electronic Frontier Foundation, "CSLI", *supra* note 234.

⁷³⁴ In these cases, based on the interaction the user has with a particular device (e.g., smart lock, smart thermostat), the company providing the smart home service can have a record of when a user is at home.

⁷³⁵ For this reason, one strategy that some manufacturers of smart devices used to preserve the privacy of their users is to limit the access that third companies can have to the device's unique identifiers, or to modify or randomize the number to which they have access. See Chapter II-A.2.b, *above*.

⁷³⁶ Calacci et al, "Tradeoff Between the Utility and Risk of Location Data", *supra* note 555 at 2.

⁷³⁷ See Jussi Myllymaki & Stefan Edlund, "Location Aggregation from Multiple Sources"(Paper delivered at the 3rd International Conference on Mobile Data Management MDM, Singapore, January 8-11, 2002) in A. Denise Williams, ed, *Proceedings MDM 2002* (California: IEEE, 2002) 131, DOI:<10.1109/MDM.2002.994393>.

⁷³⁸ See Yunji Liang et al, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective" (2020) 7:9 IEEE Internet of Things Journal 9128.

⁷³⁹ See Amazon, "Amazon One" (last visited 19 December 2023) online: <one.amazon.com> [http://web.archive.org/web/20231219172713/https://one.amazon.com/how-it-works].

The proliferation of wearable devices further expands the range of identifiers available to corporations, such as the MAC addresses of smartphones and smart watches. By collecting multiple MAC addresses from different devices, corporations can create unique fingerprints and more stable identifiers, improving their ability to track individuals across platforms and locations.⁷⁴⁰

4) Location Data as Business Assets

Location data are valuable to corporations with data-driven business models for three main reasons. First, they help bridge the gap between the online and physical worlds. Using algorithms and artificial intelligence techniques, corporations can gain additional insights about individuals based on their interactions with the physical world.⁷⁴¹ These insights allow corporations to find correlations and meanings from the relationship between people and places,⁷⁴² assigning value to where people go to eat or work, and basing decisions on certain aspects of their lives, such as insurance premiums or marketing campaigns.⁷⁴³

Second, location data serves as key identifiers of individual uniqueness, as “two unique individuals cannot occupy the same space, and, by the same token, an individual cannot simultaneously occupy multiple spaces.”⁷⁴⁴ This uniqueness makes location data particularly valuable for identifying and tracking specific devices or individuals.

⁷⁴⁰ See WP29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 14/EN WP 223 (2014) at 8.

⁷⁴¹ See Herrmann et al, “Privacy in Location-Based Services”, *supra* note 21 at 146.

⁷⁴² See Harrison Smith, “The Locative Imaginary: Classification, Context and Relevance in Location Analytics” (2020) 68:3 *Sociological Review* 641.

⁷⁴³ See Chapter III-I.B., *above*.

⁷⁴⁴ Mark Andrejevic, “Becoming Drones: Smartphone Probes and Distributed Sensing” in Rowan Wilken & Gerard Goggin, eds, *Locative Media* (New York: Routledge, 2014) 193 at 194. See also Marx, *Windows into the Soul*, *supra* note 471 at 105; Leszczynski, “Geoprivacy”, *supra* note 20.

Finally, location data are valuable because they allow inferences to be made across sectors.⁷⁴⁵ For instance, the location data generated by a GPS for navigation can be reused by an insurance provider to offer insurance premiums based on the places people travel to.⁷⁴⁶

The use of location data as a business asset varies from corporation to corporation. Some generate revenue by selling location data to third parties, while others generate revenue from the insights that can be gained from these data.⁷⁴⁷ Some corporations deal only with raw or aggregated location data, while others combine these data with information from other sources, such as online activity. This combination creates a more complete understanding of an individual's activities, allowing corporations to draw additional inferences and raise additional suspicions.⁷⁴⁸

Owing to the value of location data and their different uses in different contexts, there is a complex commercial ecosystem involving various players who participate in the generation, aggregation, analysis, and commercialization of location data.⁷⁴⁹ At the core of this ecosystem are extensive corporate mass dataveillance systems that continuously generate, collect, and process vast amounts of data about individuals and their behaviour, including location data.

⁷⁴⁵ Syagnik Banerjee, "Geosurveillance, Location Privacy, and Personalization" (2019) 38:4 *Journal of Public Policy & Marketing* 484 at 486.

⁷⁴⁶ See Cukier & Mayer-Schönberger, *Big Data*, *supra* note 705 at 106.

⁷⁴⁷ See e.g., Wilken, *Cultural Economies*, *supra* note 509 at 83–84; Banerjee, "Geosurveillance, Location Privacy, and Personalization", *supra* note 745. See also Thomas Walle, "Untangling the Location Data Ecosystem", *Street Fight* (29 October 2018), online: <streetfightmag.com> [<http://web.archive.org/web/20200621205557/https://streetfightmag.com/2018/10/29/untangling-the-location-data-ecosystem/>].

⁷⁴⁸ See Michael & Clarke, "Location and Tracking of Mobile Devices", *supra* note 31 at 219.

See also Rule, *Privacy in Peril*, *supra* note 8.

⁷⁴⁹ See e.g., Stuart A Thompson & Charlie Warzel, "Smartphones Are Spies. Here's Whom They Report To", *The New York Times* (20 December 2019), online: <nytimes.com> [<http://web.archive.org/web/20240102150117/http://web.archive.org/screenshot/https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html>].

This section provided an overview of how digital technologies collect, process, and use location data. It examined three main aspects: location techniques, identification methods, and movement records. It explained how a corporation can use different techniques to determine the location of an entity, associate that data with specific individuals or devices, and compile detailed mobility patterns over time. In essence, this section described the technological capabilities that enable corporations to implement data-driven business models and to profit from location data.

Building on this foundation, the section concluded by explaining the commercial value of location data for corporations. It highlighted that at the heart of the collection, processing, and commercialization of location data are corporate mass dataveillance systems. These systems collect and process vast amounts of data about individuals and their behaviour, and form the backbone of this lucrative industry.

Having established this landscape, the following section will examine the economic context in which corporate mass dataveillance systems operate. It will also explore the potential risks associated with such extensive data collection and processing practices, and provide an analysis of the broader implications of corporate mass data surveillance in society.

B. Corporate Dataveillance Systems and Surveillance Capitalism

Corporate mass dataveillance systems form the basis of an economic model centred on the increased generation, collection, use, and trade of data about individuals and their environment. This economic model, described by Zuboff as surveillance capitalism, can be seen as a facet of the pathological personality of the corporation proposed by Bakan. This section explores the underlying mechanisms of surveillance capitalism, looking at how it incentivizes and enables the creation and maintenance of mass dataveillance systems. It also examines the implication of these systems for individuals and society as a whole.

We begin by examining the source of profit for corporations with data-driven business models, focussing on how they use behavioural data surplus to create predictive products. The discussion then delves into the economic imperatives that drive these corporations, namely the extraction imperative which drives the continuous collection of data, and the prediction imperative, which drives the development of increasingly accurate predictive models.

1) Surveillance Capitalism and Traditional Capitalism

Zuboff argues that surveillance capitalism shares some similarities with traditional capitalism, “such as competitive production, profit maximization, productivity, and growth.”⁷⁵⁰ But it differs significantly in its purpose and methods of data collections.⁷⁵¹ While traditional capitalist corporations collect the data generated by the interaction or use of digital technologies, what Zuboff calls *behavioural data*, with the consent of the individual and only to improve products or services, surveillance capitalist corporations take a different approach. These corporations rely on the generation and collection of additional data, which Zuboff calls *behavioural surplus*,⁷⁵² to predict and influence what individuals will feel, think, and do now, soon, and later.⁷⁵³

For example, Google Inc., initially used behavioural data only to provide accurate search results (traditional capitalism).⁷⁵⁴ However, the corporation shifted its approach and began processing additional data generated by user interactions—data not needed to provide the search

⁷⁵⁰ Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 123.

⁷⁵¹ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 48.

⁷⁵² See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 137.

⁷⁵³ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 174. See also Marion Fourcade & Kieran Healy, “Seeing Like a Market” (2017) 15:1 Socio-Economic Review 9.

⁷⁵⁴ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 104–07.

results. This shift allowed Google Inc. to monetize these interactions by analyzing aggregated data to predict the effectiveness of advertising. These predictions were then sold to corporations that wanted to advertise on Google (surveillance capitalism).⁷⁵⁵

The behavioural surplus, as defined by Zuboff, consists primarily of what Kitchin calls automated data.⁷⁵⁶ As explained earlier, automated data includes the metadata generated as a by-product of using a device or engaging with a service.⁷⁵⁷ By exploiting these behavioural surpluses, surveillance capitalist corporations aim to exert greater control over consumer behaviour and market dynamics.

2) Source of Profit (Predictions Products)

At the heart of surveillance capitalism is the creation of *prediction products*—“calculations that predict what individuals and groups will do now, soon, and later.”⁷⁵⁸ These are similar to those described by privacy scholars as sorting individuals based on data profiles.⁷⁵⁹ Profiles that allow corporations to categorize individuals into specific groups based on algorithmic assumptions in

⁷⁵⁵ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 112–13.

⁷⁵⁶ See Kitchin, *Data Revolution*, *supra* note 25 at 89.

⁷⁵⁷ See the text accompanying note 234.

⁷⁵⁸ Zuboff, “We Make Them Dance”, *supra* note 512 at 11. See also Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 175–76.

⁷⁵⁹ Other terms that scholars have used to conceptualise these profiles include “capta shadow,” “digital persona,” and “data doubles.”

For “capta shadow” see Kitchin & Dodge, *Code/Space*, *supra* note 271.

For “digital persona” see Roger Clarke, “The Digital Persona and Its Application to Data Surveillance” (1994) 10:2 *Information Society* 77.

For “data doubles” see Haggerty & Ericson, “Surveillant Assemblage”, *supra* note 551; David Lyon, “Surveillance as Social Sorting: Computer Codes and Mobile Bodies” in David Lyon, ed, *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (London: Routledge, 2005) 13 at 22.

order to make decisions about (or for) an individual, predicting whether they represent, for instance, a “particular high risk, or conversely, a particular attractive marketing opportunity.”⁷⁶⁰

These data profiles are constructed from the digital information individuals generate and the digital footprints they leave behind as they use digital technologies.⁷⁶¹ Based on these, algorithms within each corporation determine the characteristics or criteria that an individual must meet to be classified into one or other pre-defined group. These classifications allow corporations to categorize individuals into groups that reveal different aspects of their lives.

For example, when using location data, algorithms can analyze the places a person frequently visits or the zones they typically navigate or avoid. From this analysis, the algorithm can assign them to a particular group, defining the type of persons they are. This categorization then influences the type of information, advertising, or services that person receives, tailoring offers to their presumed preferences or behaviour.⁷⁶²

The corporate rhetoric of personalization of services and information can be seen as another example of their manipulative trait. By claiming to provide personalized services, they make users feel special, which in turn makes their service more attractive to the individual. In addition, this rhetoric can also be seen as part of their efforts to present themselves as “good neighbours,” reinforcing the idea that they care about their users and that their data processing operations are designed to provide users with better services. In reality, however, algorithms treat individuals as probabilistic numbers rather than unique individuals, and assign them to categories that maximize

⁷⁶⁰ Gandy, *Panoptic Sort*, *supra* note 9 at 79.

See also Cohen, “What Privacy is For”, *supra* note 314 at 1916.

⁷⁶¹ See e.g., Haggerty & Ericson, “Surveillant Assemblage”, *supra* note 551 at 616.

⁷⁶² See Wood, “Spatial Profiling, Sorting and Prediction”, *supra* note 33 at 225.

profitability for the corporation.⁷⁶³ The personalization of services and information is therefore not in the interests of users, but rather in the interest of corporate profit making.

For example, when an individual uses a mobile phone to find directions to the nearest market, the results take into account various elements, including the location of the device, in order to provide relevant results. However, because the primary goal of the corporation providing the navigation service is to maximize its profits, its algorithms are often programmed to prioritize content or recommendations that increases the corporation's revenue. This could mean, for example, favouring certain brands or corporations that have paid for advertising placement.

If a particular market pays the corporation providing the navigation service to promote its brand, the algorithm may prioritize that market's location over others, even if they are less relevant to the user. This profit-driven approach applies broadly to different types of information and products recommendations, influencing how individuals interact with and perceive the options presented to them.

Predictions products are not limited to internal use within the corporation that creates them, or even within its specific industry. As Zuboff explains, external actors—whether individuals, governments, or other corporations—can access these predictive insights by participating in markets where the actions of individuals, groups, organizations, and objects are monitored and traded.⁷⁶⁴ These markets allow anyone interested to buy and use probabilistic information to understand and influence future behaviour, effectively commodifying human activity.

⁷⁶³ See e.g., Gandy, *Panoptic Sort*, *supra* note 9; Oscar H Gandy, "Statistical Surveillance: Remote Sensing in the Digital Age" in Kirstie Ball, Kevin Haggerty & David Lyon, eds, *Routledge Handbook of Surveillance Studies* (Routledge, 2012).

⁷⁶⁴ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 175–76.

To improve the quality and effectiveness of their prediction products and maintain their revenue streams, corporations must continually expand their behavioural data collection effort.⁷⁶⁵ The underlying belief is that larger and more diverse datasets can improve the accuracy of predictions, prompting corporations to expand their data repositories and refine their predictive algorithms.⁷⁶⁶

This data imperative, Fourcade and Healy argue, drives corporations to “believe [that] they should be in the data collection business, even [if] they do not yet know what to do with what they collect.”⁷⁶⁷ Because, as Cukier and Mayer-Schönberger explain, data are “Like a magical diamond mine that keeps on giving long after its principal value has been tapped.”⁷⁶⁸

3) Economic Imperatives

Zuboff attributes this need for expansion to two specific economic imperatives of surveillance capitalism: the extraction imperative and the prediction imperative.⁷⁶⁹ These imperatives drive corporations to constantly seek new sources of data and to refine their predictive capabilities. The following sections examine how these imperatives manifest themselves in the actions and business practices of Meta Inc. and Uber Inc.

⁷⁶⁵ See Bakan & Abbott, “New Corporation Documentary”, *supra* note 166 at 41:00.

⁷⁶⁶ See Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, (London: Amnesty International, 2019) online: <amnesty.org> [<http://web.archive.org/web/20231218123100/https://www.amnesty.org/en/documents/pol30/1404/2019/en/>]; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170.

⁷⁶⁷ Fourcade & Healy, “Seeing Like a Market”, *supra* note 753 at 16.

⁷⁶⁸ Cukier & Mayer-Schönberger, *Big Data*, *supra* note 705 at 104.

⁷⁶⁹ See Zuboff, “We Make Them Dance”, *supra* note 512 at 16. See also Cukier & Mayer-Schönberger, *Big Data*, *supra* note 705.

(a) Extraction Imperative: Expanding Behavioural Surplus

The extraction imperative refers to the need to increase the amount of behavioural surplus for corporations to create services and products that would attract more people to use and engage with them. This has motivated the development of an “extraction architecture”⁷⁷⁰—a network of interconnected, ubiquitous technologies designed to capture and analyze behavioural surplus.⁷⁷¹ Corporations can increase their behavioural surplus in three main ways.

First, corporations may develop new technologies or services that produce unprecedented types of data. Such innovations may result from a corporation’s entry into a new market, or they may be the result of acquisitions of established corporations in other sectors or markets.

To illustrate the first approach, Meta Inc. introduced satellite Internet and expanded Wi-Fi in developing areas to connect users who lacked reliable Internet access.⁷⁷² This move, as reported by Amnesty International, gave the corporation the opportunity to harvest new data from these regions.⁷⁷³

The second approach is exemplified by Meta Inc.’s strategic acquisitions to expand of its location database. Wilken notes that Meta Inc.’s acquisitions of Gowalla⁷⁷⁴, Instagram,⁷⁷⁵

⁷⁷⁰ See Zuboff, “We Make Them Dance”, *supra* note 512 at 16. This is similar to the concept of “surveillance assemblage” proposed by Haggety and Ericsson. Haggerty & Ericson, “Surveillant Assemblage”, *supra* note 551 at 611.

⁷⁷¹ See Zuboff, “We Make Them Dance”, *supra* note 512 at 16.

⁷⁷² See Scheck, Purnell & Horwitz, “Facebook Employees Flag Drug Cartels and Human Traffickers”, *supra* note 604.

⁷⁷³ See Amnesty International, *Surveillance Giants*, *supra* note 766.

⁷⁷⁴ Gowalla was an early location-based mobile social networking platform. Although the platform was closed soon after the acquisition, Meta Inc gained access to the expertise of Gowalla's staff, who worked on building Facebook's location services. See Wilken, *Cultural Economies*, *supra* note 509 at 79; John Letzing, “Facebook Buys More Talent With Gowalla Deal”, *Wall Street Journal* (5 December 2011), online: <wsj.com> [<http://web.archive.org/web/20240102120405/https://www.wsj.com/articles/BL-DGB-23623>].

⁷⁷⁵ Instagram was a popular photo-sharing platform. This acquisition allowed Meta Inc to address its weakness in mobile photo sharing and gain access to a highly engaged user base. See Wilken, *Cultural Economies*, *supra* note 509 at 79; “Facebook Buys Instagram For \$1 Billion, Turns Budding Rival into Its Standalone Photo App”,

Glancee,⁷⁷⁶ and WhatsApp⁷⁷⁷ played a critical role in developing of the geolocation capabilities of its platforms, enabled it to become a major player in the location-based services industry and to significantly increased the quantity and quality of its geolocation data set.⁷⁷⁸

The second way in which corporations can increase their behavioural surplus is by opening up their Application Programming Interfaces (APIs) to third-party developers.⁷⁷⁹ For instance, Wilken argues that Meta Inc.'s geolocation database grew exponentially as a result of its decision to open the Facebook place editing API and geocoding service to a limited number of third-party developers to create location-based services on top of Facebook. As a corporation without a first-mover advantage in the area of geolocation services, this decision allowed Meta Inc. to access and aggregate location data generated by the other applications.⁷⁸⁰

Similarly, corporations can also increase their behavioural surplus by using technologies such as Software Development Kits (SDKs) to piggyback on others' applications to collect data. In the case of location data, for example, some corporations use SDKs to collect location data from

TechCrunch (9 April 2012), online: <techcrunch.com>

[<https://web.archive.org/web/20190501061701/https://techcrunch.com/2012/04/09/facebook-to-acquire-instagram-for-1-billion/>].

⁷⁷⁶ Glancee was a location-based application that tracked a user's location, linked to their social media accounts, and showed their shared interests and Facebook profile picture. See Wilken, *Cultural Economies*, *supra* note 509 at 79–80; Alexia Tsotsis, “Facebook Buys Location-Based Discovery App Glancee”, *TechCrunch* (5 May 2012), online: <techcrunch.com> [<http://web.archive.org/web/20140525172610/http://techcrunch.com/2012/05/04/facebook-buys-location-based-discovery-app-glancee/>].

⁷⁷⁷ WhatsApp was a popular mobile messaging client. One of the primary reasons for this deal was to gain access to WhatsApp's large user base of active users, and to contribute to Meta's mobile and location ambitions. See Wilken, *Cultural Economies*, *supra* note 509 at 81; Matthew Panzarino, “Facebook Buying WhatsApp For \$19B, Will Keep The Messaging Service Independent”, (19 February 2014), online: <techcrunch.com> [<http://web.archive.org/web/20230306013400/https://techcrunch.com/2014/02/19/facebook-buying-whatsapp-for-16b-in-cash-and-stock-plus-3b-in-rsus/>].

⁷⁷⁸ See Wilken, *Cultural Economies*, *supra* note 509 at 75–82.

⁷⁷⁹ See e.g., Anne Helmond, “The Platformization of the Web: Making Web Data Platform Ready” (2015) 1:2 *Social Media + Society* 1.

⁷⁸⁰ See Wilken, *Cultural Economies*, *supra* note 509 at 76.

mobile devices in the background and without the user's full knowledge.⁷⁸¹ A 2018 investigation by the *New York Times* found that at least 75 corporations use SDKs to obtain anonymous and precise location data from mobile applications for consumer surveillance purposes.⁷⁸²

(b) Prediction Imperative: Enhancing Predictive Capabilities

The prediction imperative, on the other hand, drives the need to improve the quality of the behavioural surplus in order to increase the accuracy of their prediction products. This has led to the diversification of extraction architectures to address both economies of scope in surplus accumulation and economies of action.⁷⁸³

(i) Economies of Scope: Expanding the Reach of Dataveillance

Under economies of scope, corporations recognize that their future wealth depends on improving their predictions about individuals by expanding the reach of their data collection practices to include as many real-world scenarios and locations as possible, and by generating,

⁷⁸¹ See Calacci et al, "Tradeoff Between the Utility and Risk of Location Data", *supra* note 557 at 2.

See also The New York Times, "How The Times Analyzed Location Tracking Companies", *The New York Times* (10 December 2018), online: <nytimes.com> [<http://web.archive.org/web/20190101020451/https://www.nytimes.com/2018/12/10/technology/location-tracking-apps-privacy.html>]; MightySignal, "Location SDK Category Apps and Analytics" (last visited 8 February 2021) online: <mightysignal.com> [<http://web.archive.org/web/20230130123541/https://mightysignal.com/sdk-category/12/location>]; MightySignal, "Beacon SDK Category Apps and Analytics" (last visited 8 February 2021) online: <mightysignal.com> [<http://web.archive.org/web/20230130105723/https://mightysignal.com/sdk-category/46/beacon>].

⁷⁸² See Jennifer Valentino-DeVries et al, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", *New York Times* (10 December 2018), online: <nytimes.com> [<http://web.archive.org/web/20240102115358/https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?smid=nytcore-ios-share#>].

See also Fédération Romande Des Consommateurs, *Allo, mon téléphone m'écoute!*, by Jean Busché & Sandra Imsand, (2023) online: <enquetes.frc.ch> [<http://web.archive.org/web/20231219172359/https://enquetes.frc.ch/data>].

⁷⁸³ See Zuboff, "We Make Them Dance", *supra* note 512 at 17.

collecting, and processing more intimate or self-related data, such as personality, mood, and emotions.⁷⁸⁴

Consider the evolution of Meta Inc. Originally a social media platform, Meta Inc. strategically expanded to the virtual and augmented reality market by acquiring Oculus and partnering with Ray-Ban.⁷⁸⁵ The corporation also moved from being a desktop-centric platform to mobile devices and even in the home with its “Portal” series.⁷⁸⁶ Similarly, Uber Inc. expanded beyond its original ride-hailing service to include scooters,⁷⁸⁷ food delivery,⁷⁸⁸ trucks,⁷⁸⁹ alcohol delivery,⁷⁹⁰ and same-day parcel delivery.⁷⁹¹

⁷⁸⁴ See Zuboff, “We Make Them Dance”, *supra* note 512.

⁷⁸⁵ See Meta, “Facebook to Acquire Oculus” (25 March 2014) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221152403/https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/]; Josh Constine, “Facebook’s \$2 Billion Acquisition of Oculus Closes, Now Official”, *TechCrunch* (21 July 2014), online: <techcrunch.com> [https://web.archive.org/web/20240115092722/http://web.archive.org/screenshot/https://techcrunch.com/2014/07/21/facebooks-acquisition-of-oculus-closes-now-official/]; Meta, “Introducing Ray-Ban Stories: First-Generation Smart Glasses” (last visited 15 March 2023) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221153854/https://about.fb.com/news/2021/09/introducing-ray-ban-stories-smart-glasses/].

⁷⁸⁶ See Meta, “Introducing Portal From Facebook: New Video Calling Devices to Connect You With Friends and Family” (8 October 2018) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221153652/https://about.fb.com/news/2018/10/introducing-portal/]; Meta, “Meet the New Portal Family: Smart Video Calling on Your TV and Anywhere in Your Home” (18 September 2019) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20230921195319/https://about.fb.com/news/2019/09/meet-the-new-portal-family/].

⁷⁸⁷ See Uber, “Uber’s Lime Scooter Partnership” (last visited 2 November 2023) online (Help): <https://help.uber.com/riders/article/ubers-lime-scooter-partnership?nodeId=80c4aa93-02b6-4a56-af22-d20ff487b8ac>.

⁷⁸⁸ See Daniel Danker, “Arriving Now: The New Uber Eats” (7 October 2020) online (Newsroom): <uber.com> [http://web.archive.org/save/https://www.uber.com/newsroom/arriving-now-the-new-uber-eats/].

⁷⁸⁹ See Uber Freight, “About us” (last visited 2 November 2023) online: <uberfreight.com> [http://web.archive.org/web/20231219172124/https://www.uberfreight.com/about-us/].

⁷⁹⁰ See Uber, “Cheers! Uber Completes Acquisition of Drizly” (13 October 2021) online (Press Release): <investor.uber.com> [http://web.archive.org/web/20231220122715/https://investor.uber.com/news-events/news/press-release-details/2021/Cheers-Uber-Completes-Acquisition-of-Drizly/default.aspx].

⁷⁹¹ See Uber, “Uber Connect” (last visited 2 November 2023) online: <uber.com> [http://web.archive.org/web/20231111214123/https://www.uber.com/us/en/item-delivery/].

These expansions gave each corporation access to greater volume, diversity, and granularity of data. With these new data, each corporation was also able to move beyond extracting surplus from individuals' search, purchase, and browsing behaviour to programming algorithms that analyze every aspect of human behaviour as individuals interact with their service.⁷⁹²

This need to generate, collect, and process large and personalized amounts of data has motivated corporations to promote the proliferation of smart technologies. Equipped with sensors, processors, and network connections, these devices serve not only as a commodity but also as sophisticated data-producing tools.⁷⁹³ As a result, smart devices have evolved beyond their primary function to become an integral part of corporate mass dataveillance systems.

(ii) Economics of Action: Shaping User Behaviour

Under economies of action corporations learned that the most reliable way to predict the individual behaviour was to intervene at its source and shape it.⁷⁹⁴ Corporations moved from relying on automated machine processes to monitor individuals' actions and produce behavioural surplus, to developing algorithms to manipulate individuals' actions according to the corporations'

⁷⁹² See Zuboff, "We Make Them Dance", *supra* note 512 at 17.

⁷⁹³ See Jathan Sadowski, "When Data is Capital: Datafication, Accumulation, and Extraction" (2019) 6:1 Big Data & Society 1 at 7. See also Zuboff, "We Make Them Dance", *supra* note 512 at 9.

⁷⁹⁴ See Zuboff, "We Make Them Dance", *supra* note 512 at 18; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 353.

These economies of action are similar to what some academic have called digital nudging and dark patterns.

See e.g., Frederik von Briel & Per Davidsson, "Digital Platforms and Network Effects: Using Digital Nudges for Growth Hacking" (Paper delivered at the 40th International Conference on Information Systems, Munich, 2019) [unpublished] online: <https://aisel.aisnet.org/icis2019/innov_entre/innov_entre/8> ; Gregory Day & Abbey Stemler, "Are Dark Patterns Anticompetitive?" (2020) 72:1 Alabama Law Review 1; Veronika Fabricius, Tim Kollmer & Andreas Eckhardt, "Instances of Digital Dark Nudging: Findings of a Systematic Literature Analysis" (Paper delivered at the AMCIS 2023, Panama City, August 10-12, 10 August 2023) [unpublished] online: <http://web.archive.org/web/20240906165031/https://aisel.aisnet.org/amcis2023/sig_adit/sig_adit/12/> ; Sünje Clausen et al, "From Dark Patterns to Digital Sludging: Mapping the Ethical Debate on Controversial Persuasive System Design" (Paper delivered at the 43th International Conference on Information Systems, Copenhagen, December 2022) [unpublished] online: <https://aisel.aisnet.org/icis2022/soc_impact_is/soc_impact_is/11> .

economic interests.⁷⁹⁵ These manipulation techniques are the result of systematic experimentation that began with simple A/B testing of webpage design elements and gradually progressed to more complex experiments.⁷⁹⁶

A/B testing is the process of presenting contrasting options, such as design, colour, or advertising, to different groups to determine which one is most effective in achieving a specific goal. A/B testing has always played a vital role in the design process, but digital technologies, have made this type of testing more affordable, efficient, and effective for businesses. Not only does it allow corporations to adapt technological artefacts to the people who use them, but it also allows them to decide which metric to test for in the first place. This decision is made by a manager or executive of the corporation, who decides what the engineering team should test for.⁷⁹⁷ Given the pathological nature of corporations, it is not surprising that engagement is typically prioritized as the primary metric. This choice is practical for corporations because engagement is often a key indicator of revenue generation. Corporations have effectively translated behavioural insights into user engagement by using A/B testing to determine the optimal combination of colours, fonts, design, and timing.⁷⁹⁸

Some academics have coined the terms “dark patterns” or “digital sludging” to describe intentional design elements that manipulate user behaviour, ultimately leading them to make

⁷⁹⁵ See Zuboff, “We Make Them Dance”, *supra* note 512 at 20.

⁷⁹⁶ See Zuboff, “We Make Them Dance”, *supra* note 512 at 18; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 353.

⁷⁹⁷ See Waldman, *Industry Unbound*, *supra* note 15 at 197–205.

⁷⁹⁸ See Arvind Narayanan et al, “Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces” (2020) 18:2 Queue 67 at 77.

decisions that are not in their best interests. Although there are differences between these two terms, they both refer to design elements that prioritize the interests of the designer over the user.⁷⁹⁹

Corporations use dark patterns to manipulate user behaviour and increase revenue. This can be done by encouraging users to spend more than they would otherwise, persuading them to share more data, or making the service more addictive. The latter is particularly important, as users who spend more time on a platform are more likely to buy more products, share more personal information, and view more ads. In addition, by keeping users on the platform for longer, corporations can collect more behavioural surplus.⁸⁰⁰

One of the most notable examples is Meta Inc.'s manipulation of Facebook users in two situations: one to influence their voting behaviour and the other to influence their emotions. In the first experiment Meta Inc. demonstrated that its algorithms could alter voter turnout by hundreds of thousands of votes simply by encouraging people to vote through experimentally manipulated get-out-to-vote messages.⁸⁰¹ In the second experiment, Meta Inc. showed that its algorithm could create an emotional contagion, causing people to experience the same emotions without their knowledge, and found that users tended to respond more strongly to negative posts.⁸⁰²

Uber Inc. has also been known to use technology design to “nudge” drivers and consumers towards certain behaviours.⁸⁰³ For instance, Uber Inc. has tested various techniques, such as video

⁷⁹⁹ For a literature review of both concepts see Clausen et al, “From Dark Patterns to Digital Sludging”, *supra* note 794.

⁸⁰⁰ See Narayanan et al, “Dark Patterns”, *supra* note 798 at 77–78; Day & Stemler, “Are Dark Patterns Anticompetitive?”, *supra* note 794.

For an analysis of Dark Patterns in LBS apps see Jerome Dreyer et al, “‘Informed’ Consent in Popular Location Based Services and Digital Sovereignty” (2022) 16:4 *Journal of Location Based Services* 312.

⁸⁰¹ See Robert M Bond et al, “A 61-Million-Person Experiment in Social Influence and Political Mobilization” (2012) 489 *Nature* 295.

⁸⁰² See Kramer, Guillory & Hancock, “Massive-Scale Emotional Contagion”, *supra* note 589.

⁸⁰³ See e.g., Barns, “Joining the Dots”, *supra* note 577 at 98.

game graphics and low-value non-cash incentives, to motivate drivers to work longer and harder, even when it is less profitable for them.⁸⁰⁴ The corporation has also taken advantage of the behaviour of some drivers, who tend to set earnings targets and feel motivated when they are close to achieving them, by sending them notifications about their next fare opportunity before their current trip is over, encouraging them to keep working.⁸⁰⁵

This section has introduced surveillance capitalism as the economic model at the heart of mass dataveillance systems. It represents a significant shift from traditional capitalist practices, exploiting surpluses of behavioural data to create predictive products that shape and commodify human behaviour. The imperatives of extraction and prediction drive corporations to continually expand their data collection efforts and refine their predictive capabilities. This has led to the development of sophisticated extraction architectures and manipulation techniques, exemplified by the strategies of corporations such as Meta Inc. and Uber Inc.

The next and final section of this part analyzes the risks associated with corporate mass dataveillance systems, highlighting three main concerns: the vulnerability of the data collected to third-party access, the increasing economic and social power of corporations, and the potential for direct manipulation of individual behaviour.

C. Risks of Corporate Mass Dataveillance Systems

In addition to the risks and harms associated with surveillance systems outlined in Chapter III, including interference with human rights such as privacy, freedom of expression,

⁸⁰⁴ See Noam Scheiber, “How Uber Uses Psychological Tricks to Push Its Drivers’ Buttons”, *The New York Times* (2 April 2017), online: <nytimes.com> [<http://web.archive.org/web/20240102120103/https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?smid=pl-share>]; von Briel & Davidsson, “Digital Platforms and Network Effects”, *supra* note 794.

⁸⁰⁵ See Scheiber, “How Uber Uses Psychological Tricks”, *supra* note 804; von Briel & Davidsson, “Digital Platforms and Network Effects”, *supra* note 794.

freedom of association, and the impact on the foundation of democracy,⁸⁰⁶ corporate mass dataveillance systems pose three additional risks. These systems pose a constant risk of their data being accessed by third parties and governments, they increase the economic and social power of corporations, and by giving corporations direct access to individuals, these systems facilitate social control.

First, as with government-led systems, there is a constant risk that the vast amount of data about individuals and their behaviours that are collected, processed, and stored by these systems will be accessible not only to the corporation collecting the data but also to hackers.⁸⁰⁷ Given that these corporations are generally not constrained by the same constitutional restrictions as governments, and that these data are considered as a business asset, there is an additional risk that these data will be accessible to anyone willing to pay the price.

In addition, the data that corporations collect and process are also a goldmine for governments,⁸⁰⁸ providing them with easy access to a vast amount of data that they previously had to generate, collect, and process,⁸⁰⁹ and on a scale never before available.⁸¹⁰ This is particularly

⁸⁰⁶ See Chapter III-III., *above*.

⁸⁰⁷ See Chapter III, *above*.

⁸⁰⁸ See e.g., Jane Bailey, “Systematic Government Access to Private-Sector Data in Canada” (2012) 2:4 International Data Privacy Law 207; CDT, “The Project on Systematic Government Access to Data Held by the Private Sector” (2013) online: <govaccess.cdt> [<http://web.archive.org/web/20231220133800/https://govaccess.cdt.info/about.php>]; Lisa M Austin, “Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints” (2016) 17:2 Theoretical Inquiries in Law 451; Lyon, “Surveillance, Snowden, and Big Data”, *supra* note 224; Lyon, Marmura & Peroff, *Location Technologies*, *supra* note 30; Bennett et al, *Transparent Lives*, *supra* note 277 at 55–68.

⁸⁰⁹ For example, when law enforcement needed location and/or movement of a specific suspect. This is especially problematic, as the legal protections and standards to access privately held information are usually lower than if the public agency will have to generate and collected the data by themselves. See e.g., Scassa & Sattler, “Location-Based Services and Privacy”, *supra* note 102 at 113.

⁸¹⁰ See e.g., Leszczynski, “Spatial Big Data”, *supra* note 261; Rob Kitchin, “Continuous Geosurveillance in the ‘Smart City’” (last visited 2 May 2018) online (blog): <dismagazine.com> [<http://web.archive.org/web/20231221151522/http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data->

true of location data, as it is cheaper to ask corporations for location data on a particular device or number associated with a person than it is to follow that person or install a tracking device.⁸¹¹ This is problematic because the limits previously put in place to reduce the abuse of power by governments are easily circumvented, and it could act as an incentive for government not to properly regulate these systems, regardless of the risks and harms they create.

Governments can access these data in two ways. On the one hand, governments can request a corporation to provide them with the data they need, which would be more cost-effective than conducting surveillance themselves and could also eliminate the need for judicial authorization.⁸¹² According to Meta Inc's Transparency Report, between 2013 and 2023 the total number of requests they received to provide certain data to government authorities worldwide increased from 25.6k to 272k requests.⁸¹³ On the other hand, governments can also buy access to some of these data. In the US, for example, there are corporations that offer a "subscription-based" service for direct access to location data. These services are available not only to government agencies, but also to anyone interested in buying access to a particular set of data.⁸¹⁴

and-geosurveillance/]; Moritz Büchi et al, "The Chilling Effects of Algorithmic Profiling: Mapping the Issues" (2020) 36 Computer Law & Security Review 1 at 5.

⁸¹¹ See e.g., Banksto & Soltani, "Tiny Constables and the Cost of Surveillance", *supra* note 255.

⁸¹² See e.g., *PIPEDA*, *supra* note 66 at 7(3); Scassa & Sattler, "Location-Based Services and Privacy", *supra* note 102 at 113.

⁸¹³ See Meta, "Government Requests for User Data" (last visited 21 May 2024) online (Transparency Center): <transparency.meta.com> [https://web.archive.org/web/20240521145546/http://web.archive.org/screenshot/https://transparency.meta.com/reports/government-data-requests/].

⁸¹⁴ See e.g., Dell Cameron, "The FBI Just Admitted It Bought US Location Data", *Wired* (8 March 2023), online: <wired.com> [http://web.archive.org/web/20240617124304/https://www.wired.com/story/fbi-purchase-location-data-wray-senate/]; Bennett Cyphers, "How the Federal Government Buys Our Cell Phone Location Data" (13 June 2022) online (Blog): <eff.org> [http://web.archive.org/web/20240625023350/https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data].

Second, corporations have always had a significant influence on society and democratic governments.⁸¹⁵ However, the implementation of mass dataveillance systems has given corporations with data-business models greater economic and social power. On the one hand, these systems are highly profitable, providing corporations with more financial resources to lobby for regulations that benefit their business model,⁸¹⁶ to settle cases without having to take responsibility for wrongdoing or change their business model,⁸¹⁷ to pay fines for failing to comply with existing regulations, or to acquire other corporations either to kill off the competition or to further expand the data they hold.⁸¹⁸

On the other hand, these systems allow corporations to collect vast amounts of data on individuals and social trends, which they can use to gain actionable knowledge and further exacerbate power imbalances. Thus, corporate dataveillance systems are problematic because they give corporations greater control over information, which they use to maximize profits (and thus increase their economic power).⁸¹⁹

⁸¹⁵ See e.g., Bakan, *New Corporation*, *supra* note 5; Bakan, *The Corporation*, *supra* note 1.

See also Barnali Choudhury & Martin Petrin, *Corporate Duties to the Public*, (Cambridge: Cambridge University Press, 2019) c 2.

⁸¹⁶ See the text accompanying note 523 and 1086. See also Adam Satariano & Matina Stevis-Gridneff, “Big Tech Turns Its Lobbyists Loose on Europe, Alarming Regulators”, *The New York Times* (14 December 2020), online: <nytimes.com> [<http://web.archive.org/web/20210827182626/https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html>].

⁸¹⁷ As previously discussed, both Uber and Meta have settled a number of complaints by paying millions of dollars and without having to accept responsibility. See Part II-C.3, *above*.

⁸¹⁸ Further discussion of this can be found in Section B-3.a, *above*.

See also Michael L Katz, “Big Tech Mergers: Innovation, Competition for the Market, and the Acquisition of Emerging Competitors” (2021) 54 *Information Economics and Policy* 1; Juho Lindman, Jukka Makinen & Eero Kasanen, “Big Tech’s Power, Political Corporate Social Responsibility and Regulation” (2023) 38:2 *Journal of Information Technology* 144 at 149.

⁸¹⁹ See e.g., Bart W Schermer, “The Limits of Privacy in Automated Profiling and Data Mining” (2011) 27 *Computer Law & Security Review* 45; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170.

This concentration of wealth and power also leads to a concentration of power over individuals, society, and democratic institutions. For example, as their services and technologies become an essential part of people's daily lives, used by millions of people in different countries,⁸²⁰ they gain additional power to threaten governments with repercussions if they try to pass regulations they do not like.⁸²¹ As shown by Meta Inc's threats after the Australian and Canadian parliaments passed laws requiring it to pay news publishers,⁸²² or Uber Inc.'s threat to leave Minneapolis after the city council voted to raise minimum wages.⁸²³

Furthermore, this concentration of power extends into the lives of individuals, including how they access information and communicate.⁸²⁴ For instance, as people become more dependent on digital platforms to access information of all kinds, the algorithms that corporations design to meet their own goals and profits determine the flow of the information that people access. This

⁸²⁰ See e.g., Wil van der Aalst, Oliver Hinz & Christof Weinhardt, "Big Digital Platforms: Growth, Impact, and Challenges" (2019) 61:6 Business & Information Systems Engineering 645–648.

⁸²¹ See e.g., Martin Moore & Damian Tambini, "Conclusion: Without a Holistic Vision, Democratic Media Reforms May Fail" in Martin Moore & Damian Tambini, eds, *Regulating Big Tech: Policy Responses to Digital Dominance* (New York: Oxford University Press, 2021) 338.

⁸²² See e.g., Easton, "Changes to Facebook's Services in Australia", *supra* note 662; Nick Clegg, "Meta's position on Canada's Online News Act" (8 May 2023) online (Meta): <about.fb.com> [http://web.archive.org/web/20240414202125/https://about.fb.com/news/2023/05/metas-position-on-canadas-online-news-act/]; Meta, "Changes to News Availability on Our Platforms in Canada" (2 June 2023) online (Newsroom): <about.fb.com> [http://web.archive.org/web/20240430235328/https://about.fb.com/news/2023/06/changes-to-news-availability-on-our-platforms-in-canada/]; Geist, "Why Is Meta Blocking All News Links?", *supra* note 663.

See also Matthew Chapman, "Revealed: Mark Zuckerberg Threatened to Pull UK Investment in Secret Meeting with Matt Hancock", *The Bureau of Investigative Journalism* (8 December 2020), online: <thebureauinvestigates.com> [http://web.archive.org/web/20240329192300/http://www.thebureauinvestigates.com/stories/2020-12-08/revealed-mark-zuckerberg-threatened-to-pull-uk-investment-in-secret-meeting-with-matt-hancock/]; Mel Silva, "Update on the News Media Bargaining Code in Australia" (6 January 2020) online (Google): <about.google> [http://web.archive.org/web/20240414152147/https://about.google/google-in-australia/jan-6-letter/].

⁸²³ See e.g., Yiwen Lu, "Uber and Lyft Threaten to Pull Out of Minneapolis After City Council Vote", *The New York Times* (15 March 2024), online: <nytimes.com> [http://web.archive.org/web/20240315192545/https://www.nytimes.com/2024/03/15/technology/uber-lyft-minneapolis-minimum-wage.html].

⁸²⁴ See e.g., Michael Karanickolas & Toby Mendel, *Stand Up for Digital Rights: Recommendations for Responsible Tech*, (Halifax: Centre for Law and Democracy, 2016).

raises questions about freedom of expression and access to information, as well as concerns about content moderation practices.⁸²⁵ The challenges raised in these areas are also influenced by the psychopathic qualities of these corporations, such as their lack of empathy, their manipulation, and their drive for profit, which can be seen in Meta Inc.’s decision to take selective action against the presence of hate speech on its platforms, depending on who created the content, as explained above.⁸²⁶

Third, and closely related to the previous risk, corporate mass dataveillance is problematic because corporations have direct access to individuals. The same technologies that corporations use to generate and collect data give them the ability to directly influence the behaviours of individuals. Through these digital technologies, corporations are able not only to generate and collect data about individuals, but also to create and send them various inputs directly to them. These inputs can be “personalized” on the basis of the profiles that the corporation has categorized the user into, and can take the form of information, access to or offer of certain services, and certain

⁸²⁵ De Gregorio explains that these cases represent a “content moderation paradox,” as social media companies promise to protect free speech while restricting content in order to maintain control over their user base, raising questions about how these companies balance their private interests with public values. Giovanni De Gregorio, “Democratising Online Content Moderation: A Constitutional Framework” (2020) 36 Computer Law & Security Review 1.

See also, Karanicolas & Mendel, *Stand Up for Digital Rights*, *supra* note 824; Evelyn Douek, *The Rise of Content Cartels*, (Columbia University: Knight First Amendment Institute, 2020); Michael Karanicolas, “Squaring the Circle Between Freedom of Expression and Platform Law” (2020) 20:1 Journal of Technology Law & Policy 177; Kate Klonick, “The New Governors: The People, Rules, and Processes Governing Online Speech” (2018) 131 Harvard Law Review 1598.

⁸²⁶ See Part II-C.2, and Part II- C.4., *above*.

prices or charges.⁸²⁷ This type of access is also problematic because it is personalized and non-transparent.⁸²⁸

This direct access facilitates social control, not to impose behavioural norms, such as conformity or obedience, “but rather to produce behaviour that reliably, definitively, and certainly leads to desired commercial results.”⁸²⁹ This means manipulating user behaviour to increase revenue, by encouraging users to spend more money than they would have otherwise, persuading them to share more data, or making the service more addictive in order to collect more data about them.⁸³⁰ For corporations that rely on advertising revenue, for example, this manipulation is aimed at getting more clicks or engagement with ads.⁸³¹ The content of these ads can range from clothing to targeted political messages. This raises concerns about the impact of these systems on the ability of individuals to form and develop their own opinions,⁸³² as well as their right to freely access and share information without fear of manipulation or censorship.⁸³³

Furthermore, this increased personalization can have an impact on an individual’s sense of self. According to Hildebrandt, the application of different group profiles to the same individual

⁸²⁷ See Section B-2, *above*.

For an analysis of algorithmic personalized pricing practices under the Canadian legal system see e.g., Pascale Chapdelaine, “Algorithmic Personalized Pricing” (2020) 17:1 *Journal of Law and Business* 1; Pascale Chapdelaine, “Algorithmic Personalized Pricing: A Personal Data Protection and Consumers Law Perspective” (2024) 102:1 *The Canadian Bar Review* 1.

⁸²⁸ See e.g., Tufekci, “Algorithmic Harms Beyond Facebook and Google”, *supra* note 15.

⁸²⁹ Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 355.

⁸³⁰ The techniques used for the manipulation of the user are Section B-3.b, *above*.

⁸³¹ See e.g., *Meta Platforms Inc., Meta 10-K 2022*, *supra* note 532 at 56–64.

⁸³² See e.g., UN, *Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by Irene Khan, HRC, 47th Sess, UN Doc A/HRC/47/25 (2021); Zeynep Tufekci, “We’re Building a Dystopia Just to Make People Click on Ads” (September 2017) online: <https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads>.

⁸³³ See e.g., UN, *SR Right to Freedom of Opinion and Expression (2021)*, *supra* note 832.

enables a type of personalization that can paradoxically lead to de-individualization. This occurs when a person's inferred preferences, derived from groups based on their online and offline behaviour, are fed back to them, causing them to normalize these preferences even if they do not accurately reflect their true preferences in the first place.⁸³⁴

The ability of corporations and their algorithmic systems to access individuals directly, combined with the corporations' pathological trait of lack of empathy, and their radical indifference,⁸³⁵ creates a situation where user engagement is prioritized, even if it contributes to the promotion of sensationalist content and the reinforcement of polarizing trends.⁸³⁶ This can lead to personal harm, such as suggesting that survivors of violence befriend their perpetrators, which can put them at risk,⁸³⁷ as well as physical harm, when targeted information is combined with location data.⁸³⁸ It also poses risks to society and democracy by giving corporations the power to design algorithms that manipulate people's worldviews and behaviours, such as voting.

IV. Conclusions

Bakan describes the corporation as having a psychopathic personality—characterized by singular self-interest, inability to feel genuine concern for others, and a focus solely on maximizing shareholder wealth. This personality leads to externalization of costs and damages to various

⁸³⁴ See Mireille Hildebrandt, "Profiling and Aml" in Kai Rannenberg, Denis Royer & André Deuker, eds, *The Future of Identity in the Information Society* (Berlin: Springer, 2009) 273 at 285.

See also Mireille Hildebrandt, "The Dawn of a Critical Transparency Right for the Profiling Era" in Jacques Bus et al, eds, *Digital Enlightenment Yearbook 2012* (Amsterdam: IOS Press BV, 2012) 41 at 49.

⁸³⁵ See the text accompanying note 643, *above*.

See also Zuboff et al, "Surveillance Capitalism", *supra* note 641 at 262; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 671–82.

⁸³⁶ See e.g., OHCHR, *Right to Privacy (2021)*, *supra* note 315; UN, *SR Right to Freedom of Opinion and Expression (2021)*, *supra* note 832 at para 66.

⁸³⁷ See OHCHR, *Right to Privacy (2021)*, *supra* note 315.

⁸³⁸ See Leszczynski, "Geoprivacy", *supra* note 20.

groups, including workers, consumers, communities, and the environment. Despite recent corporate movements towards a commitment to stakeholders beyond shareholders, Bakan argues that because the legal structure of the corporation remains unchanged, its pathological personality and primary goal of generating profit at all costs will continue to exist.

This chapter has examined corporate mass dataveillance systems as a manifestation of this psychopathic personality of the corporation. Specifically, it has shown how corporations with data-driven business models, such as Uber Inc. and Meta Inc., exhibit traits such as irresponsibility, superficial relationships, refusal to take responsibility, lack of empathy, asocial tendencies, and deceptive image building. These traits, combined with the economic imperatives of surveillance capitalism, have led to the implementation of extensive mass dataveillance systems that continuously generate, collect, and process vast amounts of data about individuals and their behaviours.

The risks posed by these systems are significant and multifaceted. They include vulnerability to third-party access, concentration of corporate power, and the potential for direct manipulation of individual behaviour. Given the scale and impact of these systems, there is an urgent need for robust regulation to protect individual rights and societal interests.

An adequate regulatory framework must take into account the pathological personality of corporations and set limits to their profit motive. Without adequate regulation, even those technologies that are described as privacy-friendly will respond to the interests of corporations and their interpretation of privacy.⁸³⁹ Therefore, effective regulation must directly address the mass dataveillance capabilities and business models that enable and incentivize such practices.

⁸³⁹ See Bakan, *New Corporation*, *supra* note 5 at 96.

As the next chapter will argue, current data protection frameworks are inadequate to effectively regulate these corporate mass dataveillance systems because they do not take into account the current socio-technical context or the pathological personality of the corporation.

Chapter V. Regulation of Corporate Dataveillance Practices and International Human Rights Framework

There have been various attempts and proposals to regulate corporations in order to reduce their power, and to address some of the risks and harms created by the digital technologies, products, and services that they sell, such as online harms and speech.⁸⁴⁰ Different models and tools have been proposed to achieve these goals, which can be divided into three main areas of regulation: competition and antitrust regulation, content regulation and consumer protection, and sharing economy related issues such as labour and contracting.⁸⁴¹ Efforts in each of these areas aim to address a specific issue, such as negative externalities in the market caused by a monopoly position of some corporations,⁸⁴² providing a balanced protection of freedom of expression and access to information,⁸⁴³ or protecting the working conditions of people working in the “sharing economy.”⁸⁴⁴

⁸⁴⁰ See e.g., “Digital Markets Act” (last visited 3 May 2024) online (European Commission): <https://digital-markets-act.ec.europa.eu/index_en>; “The Digital Services Act package” (16 February 2024) online (European Commission): <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>>; *Investigation of Competition in Digital Markets*, by Jerrold Nadler & David N. Cicilline, CP 117-8 (Washington: Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives, 2022); *Digital Platform Services Inquiry: Interim Report No. 5-Regulatory Reform*, by Australian Competition and Consumer Commission, (Australia: 2022); House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, (December 2018) (Chair: Bob Zimmer).

⁸⁴¹ This division is based on the work of Gleiss, Dengen & Pousttchi, whom did a review of the existing efforts and literature in the area of digital platform regulations. See Alexander Gleiss, Konrad Degen & Key Pousttchi, “Identifying the Patterns: Towards a Systematic Approach to Digital Platform Regulation” (2023) 38:2 *Journal of Information Technology* 180 at 183.

See also Martin Moore & Damian Tambini, “Introduction” in Damian Tambini & Martin Moore, eds, *Regulating Big Tech: Policy Responses to Digital Dominance* (New York: Oxford University Press, 2021) 1.

⁸⁴² See e.g., Lina M Khan, “The Separation of Platforms and Commerce” (2019) 119:4 *Columbia Law Review* 973.

⁸⁴³ See e.g., De Gregorio, “Democratising Online Content Moderation”, *supra* note 825.

⁸⁴⁴ See e.g., *Regulatory Approaches to the Sharing Economy*, by Diego Zuluaga, (UK: Institute of Economic Affairs, 2016).

As discussed in Chapter III, the right to privacy—recognized, among others, in Article 17 of the ICCPR and Article 8 of the ECHR—has often been invoked to regulate surveillance practices and limit government abuse of power.⁸⁴⁵ Building on this framework, this chapter examines how privacy regulation, more specifically data protection frameworks, have been used to regulate the dataveillance capabilities of corporations.

Within the international human rights framework, there are two main approaches to regulating the impact of corporations on human rights. The first approach emphasizes the responsibility of states to regulate corporations in order to prevent, protect, and remedy interference of human rights by corporations, as set out in the International Covenant on Civil and Political Rights (ICCPR). The second approach takes into account the power and impact of corporations in society, and emphasizes the responsibilities that corporations have (or should have) under the international human rights framework.

This chapter examines both these approaches, focussing mainly on the duty of states to regulate. The first part examines the general duty of states under Article 2(1) of the ICCPR. As stated by the UN General Assembly, states have a responsibility to develop and implement effective legislation, with appropriate sanctions and remedies, to protect individuals against human rights violations and abuses, including, in the case of privacy, protection against unlawful and arbitrary collection, processing, retention, or use of personal data by various entities, including corporations.⁸⁴⁶

Given that most states have adopted data protection frameworks to regulate the processing of personal data by corporations, this first part assesses the effectiveness of these regulations in

⁸⁴⁵ See Chapter III-II, *above*.

⁸⁴⁶ See UN, *The Right to Privacy in the Digital Age*, GA, 71st Sess, UN Doc A/RES/71/199 (2017) GA Res 71/199 at art 5(f).

fulfilling states' obligations to protect individuals from corporate mass dataveillance systems, which are comparable to government-led mass dataveillance, and pose significant threats to privacy. This part argues that data protection regulations are insufficient to effectively regulate corporate mass dataveillance because they were enacted under two flawed assumptions that do not take into account the current socio-technical context. As a result, these regulations should not be considered adequate for states to fulfil their ICCPR responsibilities.

The second part of the chapter examines corporate responsibility in the context of international human rights frameworks, in particular under the UN Guiding Principles on Business and Human Rights (UNGPs).⁸⁴⁷ The UNGPs are relevant because they have had a significant impact on the debate on corporate responsibility for the protection of international human rights. This part first presents the UNGPs and their application to the technology sector, as interpreted by the B-Tech Project of the UN Office of the High Commissioner for Human Rights (OHCHR).⁸⁴⁸

The discussion in this second part engages with existing critiques by academics and NGOs that the UNGPs are an inadequate mechanism for regulating or constraining corporate harm. It also argues that this framework fails to effectively limit corporations' mass dataveillance capabilities. This is because the UNGPs primarily position corporations as guardians of individuals' privacy rights in relation to governments. This approach is problematic because it portrays corporations as benevolent actors who care about others. This allows them to cultivate a "good neighbour" image while diverting attention away from their own mass data surveillance practices.

⁸⁴⁷ SRSG, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, by John Ruggie, HRC, 17th Sess, UN Doc A/HRC/17/31 (2011). [UN Guiding Principles]

⁸⁴⁸ OHCHR, "B-Tech Project" (last visited 22 December 2023) online: <<https://www.ohchr.org/en/business-and-human-rights/b-tech-project>>.

I. States' Duty to Regulate Corporate Mass Dataveillance and Data Protection Regulations

Article 2 of the ICCPR establishes two types of obligations on states: one to adopt appropriate measures to ensure the domestic protection of ICCPR rights,⁸⁴⁹ and one to provide effective domestic remedies for persons whose ICCPR rights are violated.⁸⁵⁰ Since the ability to enjoy most ICCPR human rights would be undermined if states had no obligations to prevent human rights abuses by the private sector, the general obligation in Article 2(1) for states to “ensure” ICCPR rights includes an obligation to protect individuals from abuse of all ICCPR rights by individuals and other private entities within their jurisdiction.⁸⁵¹

In the case of the right to privacy guaranteed by Article 17 of the ICCPR, the UN Human Rights Committee (CCPR) stated that it should be protected not only against the acts of the government (or its agents), but also against legal persons such as corporations.⁸⁵² In addition, the CCPR explained that States parties have an obligation to establish a legal framework prohibiting interferences by natural and legal persons that are inconsistent with Article 17 of the ICCPR.⁸⁵³ This obligation has been reaffirmed by the OHCHR in the context of the right to privacy in the

⁸⁴⁹ ICCPR, *supra* note 16 at art 2(2).

⁸⁵⁰ ICCPR, *supra* note 16 at art 2(3).

⁸⁵¹ See UN, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR, 18th Sess, UN Doc CCPR/C21/Rev.1/Add/13 (2004) at para 8. See also Joseph & Castan, *ICCPR Commentary*, *supra* note 307 at 1.115. This duty is also reflected in pillar I of the *UN Guiding Principles*.

⁸⁵² See OHCHR, *General Comment No. 16*, *supra* note 362 at para 1. See also UN, *General Comment No. 31*, *supra* note 851 at para 8.

⁸⁵³ See OHCHR, *General Comment No. 16*, *supra* note 362 at para 9.

Although there is no explicit provision in the text of Article 8 of the ECHR, a corresponding obligation has been recognised in the case law of the ECtHR, where the Court has stated that States also have a positive obligation to ensure effective respect for Article 8 rights, including in interactions between individuals and private actors. See e.g., Richard Clayton & Hugh Tomlinson, eds, *The Law of Human Rights*, 2nd ed (New York: Oxford University Press, 2009) at 1088, 1095; Walter Kälin & Jörg Künzli, “Protection of Private Life” in *The Law of International Human Rights Protection*, 2nd ed (Oxford: Oxford University Press, 2019) 376 at 395–96.

digital age. The OHCHR stated that Article 2(1) of the ICCPR also implies an obligation to adopt legislative and other measures to give effect to the prohibition of, and protection against, unlawful or arbitrary interference and attacks, whether they emanate from state authorities or from natural or legal persons.⁸⁵⁴

Since the adoption of the ICCPR, the States that have ratified the ICCPR have implemented different legal and regulatory frameworks in their own systems to protect to the right to privacy under the ICCPR. Some have enacted a general protection of privacy in their constitution, such as Spain⁸⁵⁵ and India.⁸⁵⁶ Others have enacted laws that protect privacy in specific contexts, such as criminal proceeding, the introduction of new identification systems, or the processing of information by governments and legal persons (e.g., Sweden).⁸⁵⁷

In the context of the collection and storage of personal data in computers, databases and other devices, the CCPR elaborated on the implication of Article 17 of the ICCPR. In particular the CCPR emphasizes that states have an obligation to take effective measures to ensure that the data relating to a person's private life "is never used for purposes incompatible with the Covenant."⁸⁵⁸ In response to these requirements, many states have chosen to establish data protection frameworks as the primary legal instrument for regulating the data processing practices of corporations.⁸⁵⁹ These frameworks aim to protect the privacy rights of individuals while balancing the need for legitimate data use in different sectors.

⁸⁵⁴ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 23.

⁸⁵⁵ See UN, *Report of the Human Rights Committee*, GA, 46th Sess, UN Doc A/46/40 (1991) Supplement No 40 at para 171.

⁸⁵⁶ See UN, *Report CCPR (1991)*, *supra* note 855 at para 293.

⁸⁵⁷ See UN, *Report CCPR (1991)*, *supra* note 855 at paras 338-40.

⁸⁵⁸ OHCHR, *General Comment No. 16*, *supra* note 362 at par 10.

⁸⁵⁹ For a list of international standards for the procession of personal data see OHCHR, *Right to Privacy (2018)*, *supra* note 17 at para 28; UNCTAD, "Data Protection and Privacy Legislation Worldwide", *supra* note 17.

The limitations of data protection frameworks have been highlighted from various perspectives.⁸⁶⁰ Despite these limitations, there has been considerable reliance on data protection frameworks as tools to protect individuals' right to privacy and other human rights vis-à-vis corporations.⁸⁶¹ For example, the CCPR has emphasized that with the emergence of data-driven AI systems, the importance of such framework in providing effective legal protection will continue to grow.⁸⁶² Similarly, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has highlighted the key role of data protection in “reorienting the advertisement-driven business model of the digital economy, which drives the information disorder and related human rights abuses.”⁸⁶³ The Special Rapporteur also noted that “states should adopt strong data protection laws and update electoral and other relevant laws to limit the pervasive tracking and targeting of individuals and their activities online.”⁸⁶⁴

In order to assess the adequacy of data protection regulation in fulfilling states' obligations to protect individuals from corporate mass dataveillance, this part examines two data protection frameworks. First, given its importance and influence,⁸⁶⁵ it analyzes the European Union's General Data Protection Regulation (GDPR).⁸⁶⁶ Second, to provide a national perspective, it examines the Canadian context, specifically the Personal Information Protection and Electronic Documents Act

⁸⁶⁰ See Chapter II-I.B, *above*.

⁸⁶¹ See OHCHR, *Right to Privacy* (2018), *supra* note 17 at paras 28-30.

⁸⁶² See OHCHR, *Right to Privacy* (2021), *supra* note 315 at para 41.

⁸⁶³ UN, *SR Right to Freedom of Opinion and Expression* (2021), *supra* note 832 at para 92.

⁸⁶⁴ UN, *SR Right to Freedom of Opinion and Expression* (2021), *supra* note 832.

⁸⁶⁵ See Stephen Gerard Coughlan et al, *Law Beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization*, (Toronto: Irwin Law, 2014) at 220–35.

⁸⁶⁶ *GDPR*, *supra* note 66.

(PIPEDA) as the federal statute that regulates data processed in the course of commercial activities.⁸⁶⁷

The GDPR and PIPEDA, like many other data protection regulations and international documents,⁸⁶⁸ are based on the Fair Information Principles (FIPs).⁸⁶⁹ These principles establish norms for the processing of personal information, and aim to give individuals greater control over their data collected and processed by corporations.⁸⁷⁰

As a result of this common ground, these regulations share some similarities. For example, they both contain provisions that limit the overcollection of data,⁸⁷¹ and their material scope is limited to the protection of personal information.⁸⁷² However, they also differ in certain respects, for example, because the GDPR was enacted eighteen years after PIPEDA, it contains provisions that PIPEDA does not, such as provisions that take into account automatic processing,⁸⁷³ the right to portability,⁸⁷⁴ and the recognition of location data as personal data.⁸⁷⁵

⁸⁶⁷ PIPEDA, *supra* note 66.

Canada also has three provincial laws that are substantially similar to PIPEDA: *Personal Information Protection Act*, BC Reg 473/2003 [*PIPA BC*]; *Personal Information Protection Act*, Alta Reg 366/2003 [*PIPA Alberta*]; *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-391 [*Québec Act*].

See also Office of the Privacy Commissioner of Canada, “Provincial Laws that May Apply instead of PIPEDA” (May 2020) online: <priv.gc.ca> [http://web.archive.org/web/20231219174406/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/].

⁸⁶⁸ See e.g., OECD, *Guidelines Privacy and Transborder Flows of Personal Data*, *supra* note 354; *Convention 108*, *supra* note 355.

⁸⁶⁹ For a history of the FIPs, and their codification in different data protection instruments See Bennett & Raab, *Governance of Privacy*, *supra* note 319.

⁸⁷⁰ See Bennett & Raab, *Governance of Privacy*, *supra* note 319 at 8.

⁸⁷¹ For instance, limits to the processing of the data through data minimization and appropriateness of the purpose. See PIPEDA, *supra* note 66 at art 5(3), schedule 1 art 4.4; GDPR, *supra* note 66 at arts 5(b)-(c), recital 39.

⁸⁷² See PIPEDA, *supra* note 66 at art 4(1); GDPR, *supra* note 66 at art 2(1).

⁸⁷³ See GDPR, *supra* note 66 at arts 21-22.

⁸⁷⁴ See *supra* note 66 at art 20.

⁸⁷⁵ See *supra* note 66 at art 4(1).

Laws and regulations are created based on assumptions about feasible outcomes in the world. They are designed to function within an assumed socio-technical environment.⁸⁷⁶ Thus, regulations aimed at governing the generation, collection, and processing of the data about the behaviour of individuals and their surroundings by corporations should take into consideration the practical constraints imposed by technology. These technological constraints dictate the scope of corporations' actions, the range of objects they can generate, and the nature of the relationships they can establish with their users and customers.⁸⁷⁷

For this reason, in order to assess the adequacy of current regulations, it is crucial to examine the assumptions on which they were based and how the technological advances discussed in Chapter III and IV have changed these assumptions.⁸⁷⁸ This assessment should also consider whether the regulations take into account the pathological personality of the entities they seek to regulate,⁸⁷⁹ in particular corporation with data-driven business models.

One of the main assumptions underlying these regulations is that privacy is protected by ensuring that individuals have the opportunity to give their consent.⁸⁸⁰ The limitations of this approach, which is based on the idea of privacy as control and self-determination, have been extensively highlighted by other researchers.⁸⁸¹ This thesis agrees with these limitations,

⁸⁷⁶ See Chapter II-II, *above*.

⁸⁷⁷ The customers are not necessarily the same people as the user of their services or devices. In the case of Meta Inc., for instance, their customers are mainly the corporations paying for advertising space on its platforms.

⁸⁷⁸ See Chapter III-I and Chapter IV-III, *above*.

⁸⁷⁹ See Chapter IV-I, *above*.

⁸⁸⁰ See e.g., Policy and Research Group, *Consent and Privacy*, *supra* note 109 at 2; Timothy M Bank, *Guide to the Personal Information Protection and Electronic Documents Act: 2016 Edition*, (Toronto: LexisNexis Canada, 2015) at 7; WP29, *Guidelines on Consent under Regulation 2016/679*, WP259 rev.01 (2018); WP29, *Opinion 15/2011 on the Definition of Consent*, 01197/11/EN WP187 (2011).

⁸⁸¹ For critics and limits of conceptualizing privacy as control see e.g., Waldman, *Industry Unbound*, *supra* note 15; Paul M Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52:6 *Vanderbilt Law Review* 1607; Reiman, "Driving to the Panopticon", *supra* note 31; Daniel J Solove, "Conceptualizing Privacy" (2002) 90:4 *California Law Review* 1087, online: <<https://www.jstor.org/stable/3481326?origin=crossref>> at 1115; Bennett & Raab, *Governance of Privacy*, *supra* note 319 at 20.

particularly because in many cases individuals have no real choice about how their data should be used or when it should be collected. In such a context, reliance on consent as a cornerstone of data protection regulation is not only problematic but also counterproductive.⁸⁸²

This thesis shifts the focus away from the assumptions these regulations make about individuals, and instead concentrates on the assumptions they make about the technological capabilities and personality of the organizations they seek to govern. More specifically, it focusses on two assumptions, one about the technological capabilities of corporations with data-driven business models, and the other about the personality of these corporations.

A. Assumption 1: Data Must Be (Are) Collected and Processed by Corporations

The main purpose of data protection frameworks is to build trust in the technologies that enable the collection and processing of data, which is essential for a thriving data-based economy, by protecting the privacy of individuals. Thus, the first assumption of these regulations is that data about individuals will be collected and processed by corporations,⁸⁸³ which is seen as desirable practices for countries to remain competitive in a digital global economy. As Geller and Gutwirth argued, “data protection by default accepts the processing of personal data; otherwise its aim would be void (how can one regulate a practice if it is not for granted that it takes place?)”⁸⁸⁴

While promoting trust and confidence in an industry and economy is a legitimate regulatory objective, it has limited the scope of the regulatory debate to after the data has been collected,

See also Chapter II-I.B.2., *above*.

⁸⁸² See Strandburg, “Monitoring, Datafication, and Consent”, *supra* note 105 at 85; Jones, “The Internet of Other People’s Things”, *supra* note 53 at 245.

⁸⁸³ See Raphaël Gellert & Serge Gutwirth, “The Legal Construction of Privacy and Data Protection” (2013) 29 Computer Law & Security Review 522 at 525.

⁸⁸⁴ Gellert & Gutwirth, “Legal Construction of Privacy and Data Protection”, *supra* note 883.

excluding the consideration of whether it should be collected in the first place. As a result, data protection regulations focus on setting rules for the management of data by corporations and ensuring that individuals have rights over their data. However, this approach fails to provide regulatory tools for assessing the desirability of, and societal benefits of, data collection and processing, leaving these decisions entirely to corporations.

This regulatory approach is problematic for two main reasons. First, it normalizes data collection and processing as desirable practices. This is particularly worrying given that corporations with data-driven business models not only collect and process data, but also develop and market the technologies, products, and services that enable them to systematically and continuously generate, collect, and process vast amounts of data about individuals and their behaviours. Second, it assumes that corporations are benevolent and capable of changing their behaviour, including the design of technologies, products, and services, to accommodate user's rights, even at the expense of profit. However, corporations behave in the opposite way, they are self-interested and prioritize profit above all else.⁸⁸⁵

The following subsections demonstrate how the intention to foster trust in technologies that facilitate the collection and processing of data, and the corresponding assumption that data must be collected, are evident from the inception of both the EU and Canadian data protection frameworks. These principles have been maintained through ongoing modernization efforts and even as the socio-technological landscape has changed significantly.

⁸⁸⁵ This point is further developed in Section I-B, *below*.

1) Beginning of Data Protection Regulations

Thirty-one years after the ECHR was signed, and with the advance of data processing technologies, the Council of Europe saw the need to establish detailed rules to protect individuals by safeguarding their personal data. To this end the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was opened for signature in 1981.⁸⁸⁶ Convention 108 was (and still is) the only legally binding international agreement in the field of data protection, and it laid the foundations for the data protection regulation in Europe.⁸⁸⁷

Convention 108 recognized the need to reconcile the fundamental values of the free flow of information between peoples with respect for privacy, particularly in the context of automated processing of personal data.⁸⁸⁸ It therefore introduced the concept of data protection as a distinct element.⁸⁸⁹ In particular, it sought to establish rules on “how individuals can be enabled to exercise control over information relating to themselves which [are] collected and used by others.”⁸⁹⁰

As Valerie Steeves pointed out, Convention 108 represented a significant shift at the international level, as the focus shifted from protecting privacy as a human right, as embodied in the ICCPR and ECHR, to facilitating the flow of personal information as a means of promoting

⁸⁸⁶ *Convention 108*, *supra* note 355.

⁸⁸⁷ See Council of Europe et al, *Handbook on European Data Protection Law: 2018 Edition*, (Luxembourg: Publications Office of the European Union, 2018) at 24.

⁸⁸⁸ See *Convention 108*, *supra* note 355 at preamble.

⁸⁸⁹ See *Convention 108*, *supra* note 355 at art 1 (“his right to privacy, with regard to automatic processing of personal data relating to him [“data protection”]).

⁸⁹⁰ Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No 108 (1981) at para 3.

free technological innovation and trade.⁸⁹¹ The approach established in the ECHR, which was based on “a general prohibition of interference with the right of privacy, [allowing] exceptions only under strictly defined conditions,”⁸⁹² changed to one that allowed the processing of data as long as they were “obtained and processed fairly and lawfully.”⁸⁹³ The Article 29 Working Party (WP29)⁸⁹⁴ explained that at the time when Convention 108 was adopted, the prevailing view was that the processing of personal data should not necessarily be considered an “interference with privacy,” but rather that it should always be done in a way that protects everyone’s fundamental rights and freedoms, and in particular their right to privacy, by fulfilling certain conditions.⁸⁹⁵

When Convention 108 was adopted in 1981, the technological capabilities of corporations to generate, collect, and process data were significantly different from today. For instance, computing and storage capabilities were limited, mobile phones and GPS-enabled devices were not widely available, and the World Wide Web had not yet been invented.⁸⁹⁶ Despite these differences, the view that data processing should not be seen as an interference with privacy, but

⁸⁹¹ See Steeves, “Now You See Me”, *supra* note 24 at 468–71. See also *Convention 108*, *supra* note 355 at art 12(2) (“A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party”).

⁸⁹² WP29, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 844/14/EN WP 217 (2014) at 6.

⁸⁹³ *Convention 108*, *supra* note 355 at art 5(a).

⁸⁹⁴ The Article 29 Working is an independent European advisory body on data protection and privacy until 25 May 2018. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. With the entry into application of the GDPR, it was later replaced by European Data Protection Board (EDPB).

⁸⁹⁵ See WP29, *Opinion 06/2014*, *supra* note 892 at 6–7.

⁸⁹⁶ See Clarke, “Person Location and Person Tracking”, *supra* note 29; Computer History Museum, “Timeline of Computer History” (last visited 22 November 2023) online: <computerhistory.org> [<http://web.archive.org/web/20231220140300/https://www.computerhistory.org/timeline/1981/>]; History, “The Invention of the Internet” (28 October 2019) online: <history.com> [<http://web.archive.org/web/20231220140502/https://www.history.com/topics/inventions/invention-of-the-internet>]; Barry M Leiner et al, “Brief History of the Internet: Internet Timeline” (last visited 19 July 2016) online: <internetsociety.org> [<http://web.archive.org/web/20231220135850/https://www.internetsociety.org/internet/history-internet/brief-history-internet/>]; “The Way We Were in 1981: Technology”, *BBC News* (19 November 2010), online: <bbc.com> [<http://web.archive.org/web/20150703031841/https://www.bbc.com/news/uk-11789191>].

rather that rules should be put in place to allow such processing, is reflected in the European data protection regulations that follow Convention 108 and PIPEDA. Moreover, as will be discussed in the following paragraphs, both the EU data protection framework and PIPEDA were established to promote trust and confidence in the data processing practices by corporations in a data-driven economy.

The principles set out in Convention 108 were then refined in Directive 95/46/EC,⁸⁹⁷ which became the cornerstone of data protection law in the EU prior to the GDPR.⁸⁹⁸ Directive 95/46/EC was the result of a long process in which the EU sought to strengthen its position in the data processing industry, to compete with US corporations, and at the same time to ensure the protection of its citizens data as more and more databases containing their personal data were being created across different sectors.⁸⁹⁹

The journey from the European Commission's adoption of the proposal for a Directive in 1990 to its approval in 1995⁹⁰⁰ was driven by one main objective: to ensure the confidence of individuals in the development of the technological infrastructure and a data-based industry. This objective is evident, for instance, in the 1990 proposal, where the European Commission

⁸⁹⁷ EU, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, [1995] OJ, L 281/31 [*Directive 95/46/EC*].

⁸⁹⁸ See WP29 & WPPJ, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 02356/09/EN WP 168 (2009) at para 4.

⁸⁹⁹ See e.g., Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, (Cham: Springer, 2014) at 111; Paul M Schwartz, "European Data Protection Law and Restrictions on International Data Flows" (1994) 80:3 Iowa Law Review 471; Spiros Simitis, "From the Market to the Polis: The EU Directive on the Protection of Personal Data" (1995) 80:3 Iowa Law Review 445; Commission of the European Communities, *Community Policy on Data Processing*, SEC (73) 4300 final (21 November 1973,) online: <<http://aei.pitt.edu/6337/1/6337.pdf>> .

⁹⁰⁰ For a legislative history of this directive see EUR-Lex, "Procedure 1990/0287/COD COM (1990) 314 - 2: Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data" (last visited 22 November 2023) online: <eur-lex.europa.eu> [<http://web.archive.org/web/20231220134505/https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex%3A31995L0046>].

emphasized that an EU-wide approach to the protection of individuals' personal data was essential for the development of the data processing industry and value-added data communications services.⁹⁰¹

As the proposed text was being debated by the European Council in 1994, two significant White Papers were published. One was initiated by the European Commission,⁹⁰² while the other was requested by the European Council.⁹⁰³ Both reports emphasized the importance of an EU-wide data protection framework to increase consumer confidence in the introduction of more digital technologies in the EU. The first report highlighted that the creation of an information area would depend primarily on private sector investment. It stressed the importance of having a legal environment that would stimulate such investment, including data and privacy protection, in particular to ensure the reliability of data transfer systems.⁹⁰⁴ Building on this, the second report warned that the absence of a EU-wide legal framework would lead to a lack of consumer confidence and potentially hinder the rapid development of the information society.⁹⁰⁵

This focus on consumer confidence through regulatory frameworks was not limited to the EU. In Canada, following the adoption of Directive 95/46/EC in the EU, a similar approach was

⁹⁰¹ See European Commission, *Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*, COM(90) 314 final (13 sept 1990) CELEX:51990DC0314 at para 7.

⁹⁰² See European Commission, *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century*, White Paper (Luxembourg: Official Publications of the European Communities, 1994) (This white paper was authored by the European Commission and initiated by its President Jacques Delors).

⁹⁰³ See European Commission, *Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council*, by High Level Group on the Information Society, Bulletin of the European Union Supplement No. 2/94 (1994). In response to the Commission's white paper, the Council requested a group of prominent individuals, led by the Commissioner for the Internal Market and Industrial Affairs, to prepare a report outlining measures to be considered in relation to the European Union's support of infrastructure and information.

⁹⁰⁴ See European Commission, *Growth, Competitiveness, Employment*, *supra* note 902 at 94.

⁹⁰⁵ See European Commission, *Bangemann Report*, *supra* note 903 at 22.

taken.⁹⁰⁶ In 1998, a Task Force on Electronic Commerce composed of members of the Government of Canada's Departments of Industry and Justice, published a discussion paper outlining the main issues that needed to be addressed by private sector data protection legislation and outlining some options for the legislation.

In this paper, the Task Force echoed the EU's concerns, stating that the objective of the legislation would be to set a federal standard for how corporations should process data in order to build consumer confidence and market certainty, and to provide Canada's, "trading partners from around the world with the reassurance they need to engage in transactions that require cross-border transfers of personal information."⁹⁰⁷

Building on this premise, the paper argued that for Canada "to become the most connected country in the world by the turn of the century," consumers, businesses, and governments needed to feel confident about how their personal information was being collected, stored, and used.⁹⁰⁸ To that end, the Task Force proposed that federal legislation should balance two needs: "the business need to gather, store, and use personal information and the consumer need to be informed about how that information will be used and assured that the information will be protected."⁹⁰⁹ Consequently, from the government's perspective, the primary purpose of federal regulation was to build consumer confidence in data processing, with the main concern regarding individuals

⁹⁰⁶ The paper emphasized that ensuring effective protection of personal information is vital for Canada to maintain its competitiveness in the global information economy, especially when exchanging data with European Union member states. It noted that the Directive 95/46/EC could create significant non-tariff trade barriers with Canada if personal information is not adequately protected, which may lead to data flows being blocked. See Industry Canada and Justice Canada, *The Protection of Personal Information: Building Canada's Information Economy and Society*, by Task Force on Electronic Commerce, (Ottawa: IC, 1998) online: <e-com.ic.gc.ca> [<http://web.archive.org/web/20001012101540/http://www.e-com.ic.gc.ca/english/privacy/acroeng.pdf>] at 6–8.

⁹⁰⁷ Industry Canada and Justice Canada, *Building Canada's Information Economy and Society*, *supra* note 906 at 3.

⁹⁰⁸ Industry Canada and Justice Canada, *Building Canada's Information Economy and Society*, *supra* note 906 at 2.

⁹⁰⁹ Industry Canada and Justice Canada, *Building Canada's Information Economy and Society*, *supra* note 906 at 2–3 [emphasis added].

centered on their right to be informed about when their data were being collected and how they were being used.⁹¹⁰

This premise has been carried over into PIPEDA. Its aim is not to reduce the amount of data generated and collected by corporations, but to impose rules on corporations to ensure that data processing takes place within certain limits. As Décarý J.A. explained in *Englander v Telus Communications Inc.*, based on the reading of the four substantial principles set out in Schedule 1 (i.e., identifying purposes, consent, limiting collection, and limiting use, disclosure, and retention), the focus of PIPEDA is not on preventing the collection of the data, which is almost taken for granted. Instead, the focus is on establishing the elements that the purposes for which the data that are collected, used, or disclosed must have.⁹¹¹

2) Modernization Efforts: 2010–2023

Fourteen years after the adoption of the Directive 95/46/EC, and in view of the challenges posed by new technologies and globalization, the European Commission launched a consultation in July 2009 to assess whether the existing legal framework was adequate to meet the growing challenges, and what future action would be needed to address these challenges.⁹¹² In response to this consultation, a joint paper by the Working Party 29 (WP29),⁹¹³ and the Working Party on

⁹¹⁰ See Steeves, “Now You See Me”, *supra* note 24 at 463.

⁹¹¹ See *Englander v Telus Communications Inc.*, 2004 FCA 387 at para 42 [*Englander*].

⁹¹² See WP29 & WPPJ, *The Future of Privacy*, *supra* note 898 at 2.

⁹¹³ This was established by Directive 95/46/EC and that dealt with issues relating to the protection of privacy and personal data until 25 May 2018. With the entry into application of the GDPR it was replaced by the EDPB (European Data Protection Board). See EDPB, “Legacy: Art 29 Working Party” (last visited 14 November 2023) online: <edpb.europa.eu> [http://web.archive.org/web/20231220132132/https://edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en].

Police and Justice (WPPJ) highlighted that the core principles of data protection remained valid, but that the EU framework would benefit from a better application of these in practice.⁹¹⁴

Two years later, the European Commission proposed a comprehensive reform to update the Directive 95/46/ECEC.⁹¹⁵ One reason for the reform was that technological progress and globalization had changed the way in which individuals' data were processed. The Commission explained that in this "brave new data world," the ubiquity of technologies such as social networking sites, cloud computing, location-based services, and smart cards, meant that individuals would leave digital traces with every move they made.⁹¹⁶ It was therefore necessary to establish a robust set of rules to protect individuals' fundamental right to data protection.

In justifying this reform, the European Commission, echoing the conclusions of the WP29 and WPPJ paper, emphasized that the existing framework was effective in terms of its objectives and principles.⁹¹⁷ However, the Commission argued that this framework had not prevented inconsistencies in the way personal data protection is implemented across the EU, leading to legal uncertainty and a general public perception that there are significant risks associated with online activities.⁹¹⁸ It was therefore essential to create a more robust and consistent data protection framework in the EU. This framework would need to be backed up by rigorous enforcement,

⁹¹⁴ See WP29 & WPPJ, *The Future of Privacy*, *supra* note 898.

⁹¹⁵ See European Commission, "Commission Proposes a Comprehensive Reform of the Data Protection Rules" (25 January 2012) online (Newsroom): <ec.europa.eu> [https://web.archive.org/web/20120129011210/http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm].

⁹¹⁶ European Commission, "Why Do We Need an EU Data Protection Reform?" (25 January 2012) online (PDF): <ec.europa.eu> [https://web.archive.org/web/20120227154845/http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf].

⁹¹⁷ See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, proposal for a regulation, COM(2012) 11 final (2012) at 2, 18.

⁹¹⁸ See European Commission, *COM(2012) 11 final*, *supra* note 917 at 2.

allowing the digital economy to flourish across the EU single market, empowering individuals to control their data, and providing legal and practical clarity for corporations and public authorities.⁹¹⁹

Despite the Commission's assessment of how the technological landscape had changed, and the risks posed by this change, the claim that the objectives and principles of the existing framework were still valid was flawed.⁹²⁰ In the period between the adoption of Directive 95/46/EC and the time when European regulators began the process of reforming the EU data protection framework, technological advances in the generation, collection, and processing of data about individuals and their behaviours evolved significantly. This period saw the introduction of the first iPhone, which revolutionized the mobile phone industry and the internet economy,⁹²¹ the commercial availability of GPS technology in mobile phones and in-car navigation systems,⁹²² and the development of the technologies and techniques needed to process large amount of data.⁹²³

⁹¹⁹ See European Commission, *COM(2012) 11 final*, *supra* note 917.

⁹²⁰ See e.g., European Parliament, Protection of Individuals with regard to the Processing of Personal Data ***I European Parliament Legislative Resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Legislative resolution, OJ, C 378/399 (2014) at 401; Council of the European Union, Position (EU) No 6/2016 of the council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Position, OJ, C 159/1 (2016) at 2; GDPR, *supra* note 66 at recital 9.

⁹²¹ See Kalle Lyytinen, "Understanding the Real Innovation Behind the iPhone" (27 June 2017) online: <theconversation.com> [<http://web.archive.org/web/20231221120051/https://theconversation.com/understanding-the-real-innovation-behind-the-iphone-79556>]; Dan Farber, "When iPhone Met World, 7 Years Ago Today", *CNET* (9 January 2014), online: <cnet.com> [<http://web.archive.org/web/20220705220307/https://www.cnet.com/tech/tech-industry/when-iphone-met-world-7-years-ago-today/>].

⁹²² See Mark Sullivan, "A Brief History of GPS" (9 August 2012) online: <pcworld.com> [<http://web.archive.org/web/20231219171822/https://www.pcworld.com/article/461346/a-brief-history-of-gps.html>].

⁹²³ See Rubén Casado & Muhammad Younas, "Emerging Trends and Technologies in Big Data Processing" (2015) 27:8 *Concurrency and Computation* 2078.

These and other technological advances significantly expanded the capabilities to collect and process data. As a result, corporations gained the ability to collect and process categories of data to which they previously had no access, such as the more precise location data on individuals thanks to the widespread availability of GPS, and to do so with greater ease. Given that regulation should be designed to take into account what is technologically feasible in the world, in the light of these socio-technical changes, regulators should have reconsidered and adapted the core principles of data protection regulation during the modernization process to ensure a balance between these new technological capabilities and the rights of individuals.⁹²⁴

However, despite these technological changes, the objective of the new regulation, the GDPR, remains the same as that of Directive 95/46/EC: to build trust in the digital economy, to facilitate its growth, and to enable the various EU economies to be competitive in the global market.⁹²⁵ This approach maintains the assumption that data about individuals and their behaviour must be collected and processed. Furthermore, the GDPR continues to frame the data operations of corporations as mere data processing, even though the nature of the processing that corporations can carry out has evolved significantly since 1995. This framing fails to take account of the increased sophistication and potential impact of modern data processing techniques.

A difference between the Directive 95/46/EC and the GDPR is the fundamental right upon which each is based. The Directive 95/46/EC explicitly referred to Article 8 of the ECHR as the basis for the right to privacy it aimed to protect.⁹²⁶ In contrast, the GDPR is rooted in the Charter

⁹²⁴ See Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152.

⁹²⁵ See *GDPR*, *supra* note 66 at recital 7.

⁹²⁶ See e.g., *Directive 95/46/EC*, *supra* note 897 at Recital 10.

of Fundamental Rights of the European Union,⁹²⁷ particularly Article 8, which recognises the right to the protection of personal data as a distinct and independent right.⁹²⁸

Drafted in 2000, the EU Charter was granted binding legal effect in 2009—fifty years after the adoption of the ECHR and long after the ECtHR recognised that processing personal information relating to private life constitutes interference with the right to privacy under Article 8 of the ECHR. Consequently, the ECHR forms an important basis for the specific provisions of the Charter. For instance, based on the ECtHR’s extensive interpretation of Article 8 of the ECHR, the rights it enshrines are reflected in various Charter provisions, including Article 8 of the EU Charter (right to data protection).⁹²⁹

Although the European legislator could have chosen to base the GDPR on other provisions in the EU Chart, such as Article 7 (Respect for private and family life), the Regulation's explicit grounding in Article 8 alone highlights that, much like its predecessor Directive 95/46/EC, the objective of the GDPR remains specifically centred on regulating the control over personal data and consent rather than addressing the broader right to privacy.⁹³⁰

In the case in Canada, there have been repeated calls for the modernization and reform PIPEDA since 2005, yet none of these efforts have been successful.⁹³¹ Critics argue that the

⁹²⁷ EU, *Charter of Fundamental Rights of the European Union*, [2012] OJ, C316/26 [*EU Charter*].

⁹²⁸ The main legal basis for the GDPR are Article 8(1) of the EU Charter and Article 16(1) of the Treaty on the Functioning of the European Union which “provide that everyone has the right to the protection of personal data concerning him or her.” *GDPR*, *supra* note 66 at Recital 1.

⁹²⁹ Other provisions include Article 3 (right to the integrity of the person), Article 7 (Respect for private and family life), Article 24 (rights of the child), and the principles contained in Article 33 CFR (family and professional life) and Article 37 CFR (environmental protection). See Manuel Kellerbauer et al, eds, “Article 7 CFR” in *The EU Treaties and Charter of Fundamental Rights: A Commentary* (Oxford, UK: Oxford University Press, 2024) 446 at 447.

⁹³⁰ See e.g., Manuel Kellerbauer et al, eds, “Article 8 CFR” in *The EU Treaties and Charter of Fundamental Rights: A Commentary*, 2nd ed (Oxford, UK: Oxford University Press, 2024) 453.

⁹³¹ See e.g., Office of the Privacy Commissioner of Canada, “PIPEDA Reform: Submissions, Recommendations and Research” (last visited 23 November 2023) online: <priv.gc.ca> [<http://web.archive.org/web/20231220101342/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the->

regulation needs to be updated because it no longer reflects technological and social realities,⁹³² particularly with respect to its consent and control regime⁹³³ and its enforcement model.⁹³⁴ Additionally, concerns have been raised about ensuring adequacy with respect to the GDPR in order to maintain uninterrupted data transfers between the EU countries and Canada.⁹³⁵

In response to these concerns, the Canadian government has taken steps to address the need for updated privacy legislation. For instance, a proposal was tabled in Parliament in June 2022, which the government claims takes important steps to ensure that Canadians can trust that their privacy is protected and that AI is used ethically, while fostering innovation that promotes a thriving economy.⁹³⁶ The proposal includes some positive changes, such as granting the Office of the Privacy Commissioner of Canada (OPC) stronger enforcement powers.

However, the proposal still falls short of protecting individuals from corporate dataveillance practices. This is because, like the GDPR, the primary objective of the proposed

personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/]; Office of the Privacy Commissioner of Canada, *Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report*, by Ignacio Cofone, (2020) online: <priv.gc.ca> [http://web.archive.org/web/20231219145750/https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011].

⁹³² See Innovation, Science and Economic Development Canada, “Strengthening Privacy for the Digital Age” (21 May 2019) online: <ised-isde.canada.ca> [http://web.archive.org/web/20231220102053/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/strengthening-privacy-digital-age].

⁹³³ See House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*, (February 2018) (Chair: Bob Zimmer) at 14–35.

⁹³⁴ See e.g., Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat*, *supra* note 840 at 73; Standing Committee on Access to Information, Privacy and Ethics, *Towards PbD*, *supra* note 933 at 52–57.

⁹³⁵ See e.g., Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat*, *supra* note 840 at 72; Standing Committee on Access to Information, Privacy and Ethics, *Towards PbD*, *supra* note 933 at 62–69.

⁹³⁶ The proposed Digital Charter Implementation Act, 2022 (Bill C-27), aims to modernize PIPEDA, and introduce new rules for the development and deployment of artificial intelligence (AI). See Innovation, Science and Economic Development Canada, “Canada’s Digital Charter” (13 March 2023) online: <ised-isde.canada.ca> [http://web.archive.org/web/20231220101549/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world].

regulation remains focussed on building trust in digital technologies, fostering innovation in emerging technologies such as AI, and supporting a digital and data-driven economy.⁹³⁷ Consequently, the proposal continues to assume that the generation, collection, and processing of data about individuals is a desirable practice that must be permitted.

While some regulators in the EU and Canada, as part of their efforts to modernize the data protection framework, have acknowledged the advances in digital technologies have increased the ability of corporations to collect and process large amounts of data about individuals and their surroundings, they have not changed the primary objective of the regulations—to build trust in the digital economy, promote its growth, and enable countries to compete in the global market.

As a result, current data protection regulation continues to be based on the assumption that the collection and processing of data about individuals and their behaviour by corporations is a desirable practice. This approach, however, fails to provide regulatory tools for assessing the desirability of, and societal benefits of, data collection and processing, effectively leaving these decisions entirely to corporations. This is problematic because corporations, by their pathological nature, will prioritize the collection and processing of data at all costs.

B. Assumption 2: Corporations are Benevolent

Under data protection regulations, corporations must meet certain requirements when processing personal data. These include having a valid legal basis,⁹³⁸ collecting and processing only the necessary data for the intended purpose, and clearly defining and communicating the

⁹³⁷ See Innovation, Science and Economic Development Canada, “Consumer Privacy Protection Act” (13 March 2023) online: <ised-isde.canada.ca> [<http://web.archive.org/web/20231220101915/https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act>].

⁹³⁸ See *GDPR*, *supra* note 66 at art 5; OPC, “PIPEDA Fair Information Principles” (May 2019) online: <priv.gc.ca> [http://web.archive.org/web/20231219174928/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/].

purpose for which personal data are collected and processed.⁹³⁹ In addition, corporations must appoint a data protection officer (DPO)⁹⁴⁰ and, in some cases, carry out Data Protection Impact Assessments (DPIAs),⁹⁴¹ and consult with the supervisory authority before processing data.⁹⁴²

These regulations also entrust corporations with the responsibility of defining and implementing important aspects of these requirements. This approach, which Margot Kaminski calls “collaborative governance,” involves using broad legal standards to outline the responsibilities of corporations and filling in the details through collaborative mechanisms such as codes of conduct, guidance from data protection authorities, and interactions between corporate data protection officers and regulators.⁹⁴³

Because of this aspect of the frameworks, it can be argued that the second assumption underpinning data protection regulations is that all corporations with data-driven business models are capable of changing their behaviour to comply with the regulation and respect the rights of their users, even if this has a negative impact on their profits. This assumption is problematic because it overlooks the pathological nature of corporations.

Collaborative governance in data protection regulation means that the process of creating, interpreting, and translating laws takes place in the workplaces of privacy professionals and lawyers working within or with the same corporations that seek to profit from data collection and processing.⁹⁴⁴ As explained in Chapter IV, this is problematic because the pathological tendency

⁹³⁹ See *GDPR*, *supra* note 66 at art 6(1); *PIPEDA*, *supra* note 66 at schedule 1, 4.3.

⁹⁴⁰ See e.g., *GDPR*, *supra* note 66 at art 36; *PIPEDA*, *supra* note 66 at schedule 1, 4.1.

⁹⁴¹ See e.g., *GDPR*, *supra* note 66 at art 35.

⁹⁴² See e.g., *supra* note 66 at art 36.

⁹⁴³ See Margot E Kaminski, “Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability” (2019) 92 Southern California Law Review 1529 at 1596.

See also Waldman, *Industry Unbound*, *supra* note 15 at 108.

⁹⁴⁴ See Waldman, *Industry Unbound*, *supra* note 15 at 111.

of corporations to prioritize profits above all else is reflected in their management and organizational structures. As a result, individuals working on privacy within or for these corporations are likely to adopt a pro-corporate perspective on privacy when interpreting these requirements.⁹⁴⁵

This section illustrates the collaborative governance aspects of data protection regulation and the challenges it poses given the pathological personality of corporations. To do this, this section takes as examples three responsibilities that the regulations impose on corporations: to carry out DPIAs, to choose the appropriate legal basis, and to integrate Privacy by Design (PbD) into their technologies, products, and services. The section concludes by highlighting the problem of relying on fines to ensure compliance.

1) Carry Out Data Protection Impact Assessments (DPIAs)

Under the GDPR, corporations are required to carry out a DPIA prior to generating data in cases where the processing operations are “likely to result in a high risk to the rights and freedoms of natural persons.”⁹⁴⁶ Although there is no similar requirement in PIPEDA, the OPC recommends that organizations conduct a DPIA as part of their responsibilities under the accountability principle.⁹⁴⁷ The idea of the DPIA is to serve as an additional step in assessing the risks associated with technologies and processing operations before data are generated.

⁹⁴⁵ See Chapter IV-I.B.2, *above*.

⁹⁴⁶ *GDPR*, *supra* note 66 at art 35(1).

⁹⁴⁷ See Office of the Privacy Commissioner of Canada, “PIPEDA Fair Information Principle 1: Accountability” (August 2020) online: <priv.gc.ca> [http://web.archive.org/web/20231219174547/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/].

In theory, a DPIA can help corporations to assess and mitigate some of the risks posed by digital technologies, such as the use of data to infer information about individuals and make automated decisions based on that information, as well as unlawful access to data.⁹⁴⁸ Similarly, depending on the level of detail and availability of the DPIA, it could also benefit data protection authorities and consumers by providing greater transparency about the corporation's processing operations, the relationship between the purpose and the processing, and the risks that the corporation has identified as being posed by the processing (or technology).⁹⁴⁹

In practice, however, the potential of DPIAs is limited. Since it is the same corporation that wants to process the data that carries out the entire process,⁹⁵⁰ their real value depends on the framework and definition provided by the corporation's DPO.⁹⁵¹ It is the DPO who identifies the risks, the rights and freedoms that are potentially affected, and the scope of those rights and freedoms.⁹⁵² It is also the same corporation that decides whether or not to make the DPIA public.⁹⁵³

The assumption behind DPIAs is that the corporation will use them as a means to guide the development of its data processing practices and technology, including making the necessary

⁹⁴⁸ See e.g., *Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems*, by Expert Group 2 of the Commission's Smart Grid Task Force, (2014) online: https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf .

⁹⁴⁹ See e.g., Office of the Privacy Commissioner of Canada, "Accountability", *supra* note 947; Irish DPC, "Data Protection Impact Assessments" (last visited 24 November 2023) online (Data Protection Commission): <http://web.archive.org/web/20231220115011/https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments>].

⁹⁵⁰ Another limit is the lack of an appropriate methodology and process that would make the analysis meaningful to protect the rights and freedoms of individuals. See Dara Hallinan & Nicholas Martin, "Fundamental Rights, the Normative Keystone of DPIA" (2020) 6:2 European Data Protection Law Review 178.

⁹⁵¹ See e.g., Niels van Dijk, Raphaël Gellert & Kjetil Rommetveit, "A Risk to a Right? Beyond Data Protection Risk Assessments" (2016) 32 Computer Law & Security Review 286.

⁹⁵² See e.g., David Wright & Paul De Hert, "Introduction to Privacy Impact Assessment" in David Wright & Paul De Hert, eds, *Privacy Impact Assessment* (Dordrecht: Springer, 2012) 3; David Wright & Emilio Mordini, "Privacy and Ethical Impact Assessment" in David Wright & Paul De Hert, eds, *Privacy Impact Assessment* (Dordrecht: Springer, 2012) 397.

⁹⁵³ See Irish DPC, "DPIA", *supra* note 949.

adjustments to minimize potential risks to individuals, even if this results in a reduction in profitability. Given their pathological personality and how this pathological personality affects the privacy professionals working with or within the corporations,⁹⁵⁴ it is expected that the DPIAs will focus on data quality and security of the data processing operations, as well as control and consent requirements, but will not include any of the social consequences that these processes may have on society.⁹⁵⁵ It is also expected that corporations will use them mainly as paper trails to demonstrate compliance,⁹⁵⁶ and if they decide to publish the DPIAs, it will be only those that improve their public image.

2) Choosing the Legal Ground

Data protection regulations require corporations to have a legal basis for their processing activities.⁹⁵⁷ The GDPR sets out six legal grounds: consent, necessary for the performance of a contract, necessary to comply with a legal obligation, necessary to protect the vital interests of the data subject or another natural person, necessary for the performance of a task carried out in the public interest, and necessary for legitimate interest.⁹⁵⁸ In contrast, PIPEDA relies primarily on consent as the basis for data processing. However, in recognition of the need for corporations to process data, PIPEDA includes exceptions to the knowledge and consent requirement,⁹⁵⁹ such as

⁹⁵⁴ See Chapter IV-I.B.2., *above*.

⁹⁵⁵ See e.g., Alessandro Mantelero, “AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment” (2018) 34 Computer Law & Security Review 754.

⁹⁵⁶ See e.g., Ari Ezra Waldman, “Privacy Law’s False Promise” (2020) 97 Washington University Law Review 773; WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679*, WP 248 rev.01 (2017) at 4.

⁹⁵⁷ See Irish DPC, “DPIA”, *supra* note 949.

⁹⁵⁸ See *GDPR*, *supra* note 66 at art 6(1).

⁹⁵⁹ See *PIPEDA*, *supra* note 66 at schedule 1, 4.3. See also Office of the Privacy Commissioner of Canada, “Applying Paragraphs 7(3)(d1) and 7(3)(d2) of PIPEDA” (17 March 2017) online: <priv.gc.ca> [http://web.archive.org/web/20231219173548/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-

conditions of service,⁹⁶⁰ and situations where consent may be inadequate, for instance, because seeking consent may interfere with an ongoing investigation.⁹⁶¹

Corporations must choose the most appropriate basis, clearly identify it, and be prepared to explain their choice.⁹⁶² It is their responsibility to ensure compliance with the requirements of the chosen legal basis, including maintaining a balance between the rights of individuals rights and their business interests. For instance, when relying on contractual necessity, corporations must “examine carefully the perspective of an average data subject in order to ensure that there is a genuine mutual understanding on the contractual purpose.”⁹⁶³ Similarly, when relying on legitimate interest, corporations must “decide whether it has a legitimate interest to justify certain data processing or whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject.”⁹⁶⁴

The fact that the regulation leaves it up to the corporation to consider the rights of individuals is another example of how data protection regulation ignores the pathological personality of the corporation. Instead, it assumes that corporations are benevolent and caring enough to prioritise the rights of individuals, even at the potential expense of their own revenue interests.

personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/gd_d1-d2_201703/]; *Wansink v TELUS Communications Inc*, 2007 FCA 21 at para 23 [*Wansink*].

⁹⁶⁰ See *PIPEDA*, *supra* note 66 at schedule 1, 4.3.3; Office of the Privacy Commissioner of Canada, “Guidelines for Obtaining Meaningful Consent” (13 August 2021) online: <priv.gc.ca> [http://web.archive.org/web/20231219174731/https://priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/].

⁹⁶¹ See *PIPEDA*, *supra* note 66 at art 7(1)(a).

⁹⁶² See e.g., *GDPR*, *supra* note 66 at recitals 39-40; Office of the Privacy Commissioner of Canada, “Consent Guidelines”, *supra* note 960.

⁹⁶³ EDPB, *Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (2019) at 10.

⁹⁶⁴ WP29, *Opinion 08/2012 Providing further Input on the Data Protection Reform Discussions*, 01574/12/EN WP199 (2012) at 13.

As a control mechanism, under the GDPR, individuals have the right to lodge a complaint with a Data Protection Authority (DPA) if they believe that a corporation has not complied with its obligations under the regulation,⁹⁶⁵ such as lacking a valid legal basis for processing personal data.⁹⁶⁶ As a result, the corporation's choice of legal basis and whether it meets the necessary criteria may be subject to review.⁹⁶⁷ It is important to note, however, that this review is neither immediate nor certain and may take place after the data of millions of individuals have been processed.

If the DPA finds that the corporation is not relying on a proper legal basis or is not complying with all the requirements, it can order the corporation to bring its processing practices in line with the GDPR.⁹⁶⁸ In such cases, given the pathological personality of corporations, it is likely that they will adjust their processing to comply with the new legal basis, but they will do so in a way that minimizes any impact on their profits. In particular, if there is revenue to be made from the collection, processing, and generation of personal data, the adjustments will be made in a way that preserves those activities as much as possible.

A good example of this dynamic can be seen in the cases brought against Meta Inc. before the Irish Data Protection Commission (Irish DPC), and Meta Inc.'s subsequent response to those

⁹⁶⁵ Data Protection Authorities are independent bodies responsible for consistently enforcing the GDPR. Among their responsibilities is the handling of submitted complaints, as well as investigating the matters surrounding these complaints to the appropriate extent.

⁹⁶⁶ See *GDPR*, *supra* note 66 at arts 77-82. See also Gloria González Fuster et al, *The Right to Lodge a Data Protection Complaint: OK, but Then What? An Empirical Study of Current Practices under the GDPR*, (Data Protection Law Scholars Network, 2022) online: <accessnow.org> [<https://web.archive.org/web/20231218161747/https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-Complaint-study.pdf>].

⁹⁶⁷ See WP29, *Opinion 06/2014*, *supra* note 892 at 14.

⁹⁶⁸ See *GDPR*, *supra* note 66 at art 58(2).

decisions.⁹⁶⁹ In May 2018, the Irish DPC received two complaints challenging the lawfulness and transparency of Meta Inc.’s data processing practices for behavioural advertising on its Facebook and Instagram platforms.⁹⁷⁰

The complainants argued that Meta Inc. had wrongly relied on “contractual necessity” as a legal basis for processing the data.⁹⁷¹ After a lengthy dispute resolution process involving other EU supervisory authorities and the European Data Protection Board (EDPB),⁹⁷² the Irish DPC published its decisions in January 2023. These decisions found that Meta Inc. had improperly relied on “contractual necessity” as a legal basis for processing personal data for behavioural advertising, as such processing did not constitute a core element of the services provided by the platforms, as set out in Facebook’s Terms of Service,⁹⁷³ and Instagram’s Terms of Use.⁹⁷⁴ The Irish DPC ordered Meta Inc. to bring its data processing practices into compliance with Art. 6(1)

⁹⁶⁹ The OPC ruling on the Aylo platform, formerly known as Mindgeek, is another example of the pathological characteristics of corporations. In this situation, the corporation’s response to a data protection authority shows its unwillingness to accept responsibility and its efforts to maintain its current business model, which is crucial to its profitability.

See Office of the Privacy Commissioner of Canada, *PIPEDA Findings #2024-001: Investigation into Aylo (formerly MindGeek)’s Compliance with PIPEDA* (2024) online: <priv.gc.ca> [https://web.archive.org/web/20240301212628/https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2024/pipeda-2024-001/] at para 183,186,188.

⁹⁷⁰ The Irish Data Protection Commission is the European regulatory body responsible for processing all data protection complaints directed towards Meta Inc, as the company has its registration in Ireland.

⁹⁷¹ See Irish DPC, *Decision Concerning a Complaint Directed Against Meta Platforms Ireland Limited in Respect of the Instagram Service Made Pursuant to Section 113 Of the Data Protection Act 2018*, DPC Inquiry Reference: IN 18-5-7 (12 January 2023) at para 14; Irish DPC, *Decision Concerning a Complaint Directed Against Meta Platforms Ireland Limited in Respect of the Facebook Service Made Pursuant to Section 113 of the Data Protection Act 2018*, DPC Inquiry Reference: IN 18-5-5 (31 December 2022) at para 2.10.

⁹⁷² See *GDPR*, *supra* note 66 at arts 60, 65.

See also See EDPB, “Facebook and Instagram Decisions: ‘Important Impact on Use of Personal Data for Behavioural Advertising’” (12 January 2023) online (Press Release): <edpb.europa.eu> [http://web.archive.org/web/20231220115357/https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural_en].

⁹⁷³ See Irish DPC, *Facebook Case*, *supra* note 971 at para 4.56. See also EDPB, *Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service* (5 December 2022).

⁹⁷⁴ See Irish DPC, *Instagram Case*, *supra* note 971 at para 49. See also EDPB, *Binding Decision 4/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Instagram Service* (5 December 2022).

of the GDPR within three months.⁹⁷⁵ It is important to note that it took more than four years for the Irish DPC to publish its final decisions in both cases. During this lengthy period, Meta Inc. continued its data processing practices on both services unchanged.

Meta Inc.’s response to these rulings reveals its narrow and selective interpretation of the GDPR. It also provides insight into some of its pathological traits, in particular its constant efforts to maintain profitability by refusing to take responsibility and manipulative behaviour.

Meta Inc. tried to downplay its responsibility by emphasizing that it had not broken any rules. For example, the corporation gradually changed its legal basis for processing data, first shifting from “contractual necessity” to “legitimate interest,”⁹⁷⁶ and later to “consent.”⁹⁷⁷ In each case, the corporation was careful to emphasize that although it was changing its legal basis, it was not doing so because it was wrong, as its previous approach was also GDPR compliant.⁹⁷⁸

Meta Inc. also tried to present its practices as the industry standard.⁹⁷⁹ By comparing its actions with those of other corporations,⁹⁸⁰ Meta Inc. sought to normalize its behaviour, deflect criticism, and reaffirm that it had done nothing wrong. In addition, by insisting that other

⁹⁷⁵ See Irish DPC, *Facebook Case*, *supra* note 971 at para 8.5; Irish DPC, *Instagram Case*, *supra* note 971 at para 209.

⁹⁷⁶ See Meta, “EU Legal Bases for Ads”, *supra* note 536 at update March 30, 2023.

⁹⁷⁷ Meta, “EU Legal Bases for Ads”, *supra* note 536 at update August 1, 2023.

⁹⁷⁸ For instance, when Meta Inc. announced that it will be shifting to “consent,” it pointed out that “the GDPR states that there is no hierarchy between legal bases, and non should be consider more valid than other.” Meta, *supra* note 536.

⁹⁷⁹ On this point, Meta Inc. may have been right. For instance, as of November 14, 2023, Uber relies on “legitimate interest” to process data, including metadata and location related data, for various purposes such as marketing, research and development, and security. Its privacy policy does not specify whether, for instance, marketing is personalized, but given its recently investment in advertising and the fact that it sells its product as having “first hand data” to enable personalized marketing, it is possible to assume that these data are (or will be) used to deliver personalized content. See Uber, “Privacy Overview”, *supra* note 538.

⁹⁸⁰ See Meta, “EU Legal Bases for Ads”, *supra* note 536 at initial post, updates March 30 and August 1, 2023.

corporations relied on a similar basis, it implied that the Irish DPC’s interpretation was flawed, further demonstrating its reluctance to accept responsibility.

This refusal to take responsibility has been accompanied by a manipulative behaviour from the outset. In its initial response, Meta Inc. expressed disappointment with the conclusions reached by the Irish DPC, and announced its intention “to appeal both the substance of the rulings and the fines.”⁹⁸¹ It insisted that personalized experiences, including advertising, were essential to its services, and noted that “it would be highly unusual for a social media service not to be tailored to the individual user.”⁹⁸² It also stated that the suggestion that personalized advertising can no longer be offered by Meta Inc. across Europe without first obtaining the consent of each user was incorrect.⁹⁸³ Although the corporation ultimately chose to rely on consent, these statements can be read as an attempt to minimize the impact of the Irish DPC decision on its business model.

In addition, throughout its communications, Meta Inc. sought to reassure its investors and advertisers (its primary customers) that its profitable advertising business model would continue.⁹⁸⁴ Meta Inc. consistently emphasized that the Irish DPC’s decisions concerned only the legal basis for certain advertising practices and not the practice of personalized advertising itself.⁹⁸⁵ This approach allowed the Corporation to maintain its positions while appearing cooperative with the regulatory requirements.⁹⁸⁶

⁹⁸¹ Meta, “EU Legal Bases for Ads”, *supra* note 536 at initial post (Business Lack Regulatory Certainty Around Appropriate Legal Bases).

⁹⁸² Meta, “EU Legal Bases for Ads”, *supra* note 536 at initial post (What is a Legal Basis?).

⁹⁸³ See Meta, “EU Legal Bases for Ads”, *supra* note 536 at initial post (Business Lack Regulatory Certainty Around Appropriate Legal Bases).

⁹⁸⁴ See Meta, “EU Legal Bases for Ads”, *supra* note 536 at initial post, and updates March 30 and August 1, 2023. 3

⁹⁸⁵ See e.g., Meta, “EU Legal Bases for Ads”, *supra* note 536 at initial post (Business Lack Regulatory Certainty Around Appropriate Legal Bases).

⁹⁸⁶ For instance, in its last update, Meta Inc. concluded by saying that it would provide further information over the coming months ahead, as it would take time “to constructively engage with regulators to ensure that any proposed

In response to regulatory pressure, in October 2023 Meta Inc. introduced a subscription-based option for users in the EU, EEA, and Switzerland who did not want their data to be processed for behavioural advertising.⁹⁸⁷ This announcement also illustrates Meta Inc.’s attempt to normalize its behaviour and deflect criticism by justifying its decision by comparing it to what other corporations are doing. It described it as “the best compliance solution” because subscription as an alternative to viewing advertising is a well-established and economically viable business model in many other industries. It stressed that it believed, “like countless other businesses,” that this option would allow it, “to meet changing regulatory obligation while offering users a clear choice.”⁹⁸⁸

Meta Inc’s framing of the change as regulatory compliance and a choice for individuals is also an example of its manipulative behaviour, as the decision to offer a subscription option is ultimately about securing profits. From 1 March 2024, European users who opt for the subscription option had to pay €12.99 per month for the mobile version and an additional €8 per month for each additional account. As a result, users who accessed both Facebook and Instagram had to pay €20.99 per month and €251.88 per year.⁹⁸⁹ Although this pricing model may deter some users from subscribing and opting for behavioural advertising instead, it could also lead to increased revenue per person for Meta. In Q3 2023, Meta Inc.’s global average revenue per person was \$8.71,⁹⁹⁰

solution addresses regulatory obligations in the EU.” Meta, “EU Legal Bases for Ads”, *supra* note 536 at update August 1, 2023.

⁹⁸⁷ See Meta, “Facebook and Instagram to Offer Subscription for No Ads in Europe” (30 October 2023) online (Newsroom): <[about.fb.com/news](https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/)> [<http://web.archive.org/web/20231221152119/https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>] at initial post.

⁹⁸⁸ See Meta, “No Ads in Europe”, *supra* note 987 at update December 4, 2023.

⁹⁸⁹ See Meta, “No Ads in Europe”, *supra* note 987.

⁹⁹⁰ See Meta Platforms Inc, *Quarterly Report Q3 (Form 10-Q)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2023) at 39.

which is higher than this fee. In addition, the average revenue under the behavioural advertising model can fluctuate from month to month and it is influenced by various factors; however, the subscription fee will provide Meta Inc. with a steady revenue stream.

In November 2024, Meta Inc. announced a 40% reduction in its subscription plan. In doing so, it highlighted that while the previous prices were “Firmly in line with peers, this lower pricing means that [its] subscription service will be one of the cheapest across [its] peers.”⁹⁹¹ It also noted that despite its “concerted efforts to comply with EU regulations, [it has] continued to receive additional demands from regulators that go beyond what is written in the law.”⁹⁹² In response to this feedback, and in order to continue to provide its services free of charge to as many EU citizens as possible, the corporation announced that it would be introducing a new option for EU users who choose to use its platforms for free. Users would be able to choose to see “less personalized ads,” which will be based on limited data, including session context, and basic user information such as age, location, and gender.⁹⁹³

It remains to be seen whether European regulators will accept this solution. In 2023, the CJEU suggested that a subscription model could be a valid alternative option for users who do not want their data to be processed.⁹⁹⁴ However, as this aspect was not the main focus of the case, the

⁹⁹¹ See Meta, “No Ads in Europe”, *supra* note 987 at update November 12, 2024 (Significantly Lowering the Price of Subscription for No Ads).

⁹⁹² See Meta, “No Ads in Europe”, *supra* note 987 at update November 12, 2024 (What to Expect From Less Personalized Ads).

For an example of complaint filed against Meta Inc see e.g., Noyb, “Noyb Files GDPR Complaint Against Meta over ‘Pay or Okay’” (28 November 2023) online (News): <noyb.eu> [<http://web.archive.org/web/20231220140812/https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay>] (alleging that their newly introduced subscription option violates the GDPR as the consent given in these cases cannot be deemed as freely given).

⁹⁹³ See Meta, “No Ads in Europe”, *supra* note 987 at update November 12, 2024 (What to Expect from Less Personalized Ads).

⁹⁹⁴ See *Meta Platforms Inc and Others v Bundeskartellamt* [GC], C-252/21, [2023] ECLI:EU:C:2023:537 at para 150 [*Meta Platforms Inc*].

Court did not provide further details on the conditions under which this might be applicable. It therefore remains uncertain whether Meta Inc.'s approach will be accepted as it stands, or whether modifications such as further reduction in the subscription price or a complete change of approach will be required.

While the decisions of the Irish DPC have prompted Meta Inc. to adjust its legal basis for data processing, potentially demonstrating that data protection regulation can be an adequate tool to regulate corporate dataveillance practices, the extent of these changes remains uncertain. Based on the corporation's reactions described above, it is clear that Meta Inc. is not seeking to radically change its business model, but is simply trying to find a more appropriate legal basis that will allow it to continue its current practices and maximize its profits.

Meta Inc's reluctance to change its data processing practices highlights the limitations of data protection regulations, which presuppose corporate empathy and the prioritization of individual rights over financial gain. As a result, the effectiveness of such regulations in encouraging significant changes in data collection and processing practices by corporations with data-driven business models such as Meta Inc. remains questionable.

3) Integrate Privacy by Design (PbD) into their technologies, products, and Services

Privacy by design (PbD) is one of the concepts that represents the idea of engineering privacy from the outset,⁹⁹⁵ recognizing that policy and regulation alone are not enough to protect privacy.⁹⁹⁶ This approach requires technologies, products, and services to be designed in such a

⁹⁹⁵ For a literature review of the different conceptual lenses used to discuss the regulatory effects of technology see Bennett Moses & Zalnieriute, "Dimension of Time", *supra* note 156 at 317–20.

See also Chapter II-A.2.c, *above*.

⁹⁹⁶ See Cavoukian & Prosch, *Roadmap for PbD*, *supra* note 83 at 114–15.

way that personal control, transparency, data collection limits, and data minimization can be easily exercised throughout the data lifecycle.⁹⁹⁷

Although PbD is generally seen as complementary to data protection regulations,⁹⁹⁸ in the case of the GDPR, it is part of the corporation's compliance responsibilities.⁹⁹⁹ As part of their data protection compliance efforts, corporations must also use appropriate technical tools to help them meet some of their obligations, such as ensuring that the data are processed using techniques such as pseudonymization.¹⁰⁰⁰

One of the limitations previously reported in the literature is that there are no clear guidelines on how PbD should be operationalized, leading to a lack of consistency in the level of privacy that is “baked in” to technologies. This creates ambiguity about what it means to operationalize PbD. As Waldman explained, it “could mean anything from following the FIPPs to making technological changes to platforms to integrating lawyers into more diverse design teams.”¹⁰⁰¹ Despite various attempts by commentators to provide guidelines or examples of the practical implementations of PbD,¹⁰⁰² these ambiguities remain.

⁹⁹⁷ See e.g., Cavoukian & Prosch, *Roadmap for PbD*, *supra* note 83; Cavoukian, *PbD in Law, Policy, and Practice*, *supra* note 83.

⁹⁹⁸ See 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on PbD*, *supra* note 82; Office of the Privacy Commissioner of Canada, *2019-20 Departmental Plan*, *supra* note 82.

⁹⁹⁹ See e.g., *GDPR*, *supra* note 66 at art 25.

In the case of PIPEDA, for example, the ETHI Committee argued that “that privacy by design is an effective way to protect the privacy and reputation of Canadians,” and therefore, they recommended that PIPEDA be amended to make privacy by design a central principle, see Standing Committee on Access to Information, Privacy and Ethics, *Towards PbD*, *supra* note 933 at 52.

¹⁰⁰⁰ See e.g., *GDPR*, *supra* note 66 at art 25(1).

¹⁰⁰¹ Ari Ezra Waldman, “Privacy’s Law of Design” (2019) 9:5 UC Irvine Law Review 1239 at 1257.

¹⁰⁰² See e.g., Kirsten Martin & Katie Shilton, “Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices” (2016) 32:3 Information Society 200; Waldman, “Privacy’s Law of Design”, *supra* note 1001; Information and Privacy Commissioner Ontario, *Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design*, by Ann Cavoukian & Drummond Reed, (Toronto: IPC-ON, 2014) online: <ipc.on.ca> [<http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>].

As a result, the definition of how PbD is to be materialized is based on the judgment of the corporations that develop and profit from data-driven technology, products, and services, or the corporations that act as gatekeepers to certain markets. This aspect of PbD has turned these corporations into ethical agents.¹⁰⁰³

In the context of mobile applications, for instance, Daniel Green and Katie Shilton argue that the definition of privacy and the design of the features and settings that fit such a definition differ between the iOS and Android ecosystems, in part because of the different roles that Apple Inc. and Google Inc. play in regulating the marketplace and their participation in the overall data chain.¹⁰⁰⁴ Green and Shilton found that each marketplace sets the parameters of what is allowed and what is not allowed, exercising not only “negative power (hiding or blocking content or users) but also positive power: training [developers about] what privacy means and why it is important.”¹⁰⁰⁵ Therefore, application developers, relying in part in each marketplace’s community blog, materialized these requirements in their applications. They argued that PbD in this context might be better described as “privacy by permitted design” or “privacy by platform.”¹⁰⁰⁶

Considering the concept of PbD as an adequate means to protect the privacy of individuals is another example of how data protection regulations fail to take into account the pathological personality of corporations to prioritize self-interest above all else. By imposing a requirement without providing clear and easily verifiable guidelines, PbD as a regulatory requirement gives corporations the opportunity to interpret it in a way that benefits them and does not affect their profits. Moreover, this approach allows corporations with data-driven business models to enhance

¹⁰⁰³ See Daniel Greene & Katie Shilton, “Platform Privacies: Governance, Collaboration, and the Different Meanings of ‘Privacy’ in iOS and Android Development” (2018) 20:4 New Media & Society 1640 at 1643.

¹⁰⁰⁴ See Greene & Shilton, “Platform Privacies”, *supra* note 1003.

¹⁰⁰⁵ Greene & Shilton, “Platform Privacies”, *supra* note 1003 at 1644.

¹⁰⁰⁶ See Greene & Shilton, “Platform Privacies”, *supra* note 1003 at 1655.

their public image by claiming that they are complying with data protection regulation by implementing PbD, while at the same time relying on mass dataveillance practices as a source of revenue.

4) Fines as Deterrents of Deviant Behaviour

A final example of how data protection regulation overlooks the pathological personality of corporations is the use of fines as a deterrent to deviant behaviour. One of the significant “improvements” of the GDPR was the introduction of substantial fines for corporations that fail to comply with the regulation. To ensure compliance, the GDPR allows for fines of up to €20 million or up to 4% of the corporation’s total global annual turnover (whichever is higher).¹⁰⁰⁷ Similarly, the proposed amendment to the Canadian legislation (Bill C-27) includes this approach.¹⁰⁰⁸

However, given their pathological nature, for corporations fines are simple part of a cost-benefit decision. Taking into account their lack of empathy and asocial tendencies,¹⁰⁰⁹ corporations’ decisions to violate laws depend on factors such as the likelihood of getting caught, potential fines and reputational damage, and the risk of stricter regulations. This reasoning, according to Bakan, explains why many corporations repeatedly engage in illegal activities. Such behaviour may not be ethical, but it can be strategic for corporations to succeed.¹⁰¹⁰

¹⁰⁰⁷ See *GDPR*, *supra* note 66 at art 83.

¹⁰⁰⁸ The proposal establishes “significant fines for non-compliant organizations—with fines of up to 5% of global revenue or \$25 million, whichever is greater, for the most serious offences.” Innovation, Science and Economic Development Canada, “Bill C-27 Summary: Digital Charter Implementation Act, 2022” (18 August 2022) online: <ised-isde.canada.ca> [<http://web.archive.org/web/20231220102246/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020>].

¹⁰⁰⁹ See Bakan, *The Corporation*, *supra* note 1 at 57.

¹⁰¹⁰ See Bakan, *New Corporation*, *supra* note 5 at 57; Bakan, *The Corporation*, *supra* note 1 at 152.

As part of this cost-benefit analysis, corporations often anticipate fines and set aside funds to pay them. This practice is illustrated by the way corporations such as Meta Inc. and Uber Inc. frame their legal proceedings in their annual financial reports. For instance, in its annual report, Meta Inc. acknowledged that the corporation is affected by complex and ever-changing regulations, including those related to privacy.¹⁰¹¹ In particular, Meta Inc. noted that the uncertainty surrounding the interpretation and enforcement of the GDPR, as well as the number and imposition of penalties for non-compliance,¹⁰¹² has resulted in a significant amount of loss contingencies being accrued for regulatory compliance.¹⁰¹³ To account for this, in 2022, Meta Inc. allocated \$4,795 million to “legal-related accruals,” which represents approximately 4% of its revenue (\$116,609 million).¹⁰¹⁴

Similarly, in its annual report, Uber Inc. acknowledged that it faces potential risks associated with the handling of its data, including collection, use, transfer, disclosure, and processing. It acknowledged that these risks could result in legal and regulatory actions, fines, investigations, inquiries, negative press coverage, and other consequences.¹⁰¹⁵ Accordingly, in 2022, Uber Inc. set aside \$1,573 million for “accrued legal, regulatory, and non-income taxes,”¹⁰¹⁶ which represents approximately 4.9% of its revenue (\$31,877 million).¹⁰¹⁷

¹⁰¹¹ It also noted that these regulations are subject to change and are open to interpretation, which could result in litigation, changes to Meta Inc.’s products and practices, financial penalties, increased operating costs, or decreased user growth and engagement, ultimately harming the corporation’s business. See Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 37.

¹⁰¹² See Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 111.

¹⁰¹³ See Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 110.

¹⁰¹⁴ Meta Platforms Inc, *Meta 10-K 2022*, *supra* note 532 at 86.

¹⁰¹⁵ See Uber Technologies Inc, *Uber 10-K 2022*, *supra* note 570 at 37.

¹⁰¹⁶ Uber Technologies Inc, *Uber 10-K 2022*, *supra* note 570 at 110.

¹⁰¹⁷ See Uber Technologies Inc, *Uber 10-K 2022*, *supra* note 570 at 94.

Thus, while fines may seem like a strong incentive to ensure compliance with data protection compliance, relying on them alone is misleading, because for corporations it is not just about the size of the fine, but also about how likely they think they are to be caught, and whether they will make more money by complying with the law and avoiding a fine, or by not complying with the law and getting a fine.

This part has examined the obligations of states to regulate corporate mass dataveillance through the use of data protection regulations, using the GDPR and PIPEDA as examples. While these regulations aim to protect individuals' privacy rights, they are based on problematic assumptions about the nature of data processing practices and corporate behaviour. Specifically, they assume that data processing by corporations is a necessary and desirable practice, and that corporations will act benevolently to protect users' rights. However, these assumptions fail to take into account the pathological personality of corporations, which prioritize profit above all else.

The collaborative governance approach of current data protection regulation, which relies on corporations to interpret key aspects of the regulation, is particularly problematic given these pathological traits. Examples such as DPIAs, the choice of legal grounds for processing, and the implementation of PbD illustrate how corporations can interpret and implement requirements in a self-serving manner. In addition, the use of fines as a deterrent has limited effectiveness, as corporations simply see them as part of a cost-benefit analysis. Overall, this analysis suggests that current data protection frameworks are inadequate to protect individuals from corporate mass dataveillance practices because they do not consider or constrain the profit-driven nature of corporate data processing activities.

II. International Human Rights, Corporations, and Surveillance

Traditionally, the international human rights framework has focussed on the responsibility of states to protect human rights. For example, the ICCPR and the ECHR are international treaties signed by states and the obligations created by these treaties apply to the signatory states. This means that states are obliged to respect human rights in their operations and relations with citizens. As explained previously, they are also obliged to protect individuals' privacy from corporations' mass dataveillance capabilities.¹⁰¹⁸

However, the growing power and influence of corporations has called this traditional paradigm into question. Consequently, various arguments have emerged that corporations should have international obligations to respect and protect human rights. While this approach has gained considerable international recognition, it is insufficient for adequately regulating the mass dataveillance capabilities of corporations, as will be discussed below.

This part examines the evolution of corporate responsibility in the context of human rights, with a particular focus on the Guiding Principles on Business and Human Rights (UNGPs). It critically analyzes the application of the UNGPs to corporations with a data-driven business model, and explores how these principles have inadvertently contributed to reinforcing the “good neighbour” image of corporations. This part concludes by highlighting how the framing of corporations and surveillance practices in within UN human rights framework has reinforced the “good neighbour” image of corporations as protectors of their users' right to privacy.

¹⁰¹⁸ See Part I, *above*.

A. Corporate Human Rights Responsibilities and Their Pathological Personality

Historically, the international human rights framework has been state-centred in response to the power imbalance between states and individuals. However, various scholars have highlighted that relying solely on state responsibility for the protection of human rights has become insufficient in light of corporations' growing power and their ability to impact individuals' rights.¹⁰¹⁹ Consequently, there has been an effort by academics and international organizations to effectively recognize that corporations should have certain duties and responsibilities with respect to human rights.¹⁰²⁰

One notable contribution to this discourse came in 2001 when Steven R. Ratner proposed a series of principles for applying international human rights to private actors. He argued that besides states, "Other entities may also pose a threat to human dignity—either acting with the state or alone—so that any contemporary notion of human rights must contemplate duties on those entities as well."¹⁰²¹ For him, this did not entail the recognition or development of new human rights but the identification of new duty holders.¹⁰²²

Later, Professor John G. Ruggie, in his role as the first UN Special Representative on Business and Human Rights (SRSG), proposed the "Protect, Respect and Remedy" Framework,¹⁰²³ and the "Guiding Principles on Business and Human Rights" (UNGPs).¹⁰²⁴ The

¹⁰¹⁹ See Steven R Ratner, "Corporations and Human Rights: A Theory of Legal Responsibility" (2001) 111:3 The Yale Law Journal 443 at 461.

¹⁰²⁰ See Ratner, "Corporations and Human Rights", *supra* note 1019 at 475.

¹⁰²¹ Ratner, "Corporations and Human Rights", *supra* note 1019 at 469.

¹⁰²² See Ratner, "Corporations and Human Rights", *supra* note 1019.

¹⁰²³ SRSG, *Protect, Respect and Remedy: A Framework for Business and Human Rights*, by John Ruggie, HRC, 8th Sess, UN Doc A/HRC/8/5 (2008).

¹⁰²⁴ SRSG, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, by John Ruggie, HRC, 17th Sess, UN Doc A/HRC/17/31 (2011).

first document, the “Protect, Respect, and Remedy Framework” was presented to the HRC in 2008 after multiple consultations and research integrating different stakeholders.¹⁰²⁵ It provided a “conceptual and policy framework to anchor the business and human rights debate, and to help guide all relevant actors.”¹⁰²⁶ In 2011, the second document, the UNGPs which implemented the 2008 framework, was presented.¹⁰²⁷ The UNGPs set out three distinct but complementary pillars:¹⁰²⁸ (I) the state duty to protect against human rights abuses by business enterprises; (II) the moral responsibility of corporate actors to respect human rights; (III) the need for greater access by victims to effective remedies.¹⁰²⁹ As Ruggie explains, each of these three pillars is an essential element of the overall framework.¹⁰³⁰

Both documents were unanimously endorsed by the HRC. This endorsement, combined with the express support of a diverse set of stakeholders, including the private sector, gave the UNGPs authority and legitimacy as a global standard for preventing and addressing human rights harm connected to business activity.¹⁰³¹ The UNGPs were later incorporated into international frameworks, such as the *OECD Guidelines for Multinational Enterprises*,¹⁰³² and have become a

¹⁰²⁵ See SRSF, *Policy Framework*, *supra* note 1023 at para 4.

¹⁰²⁶ SRSF, *Policy Framework*, *supra* note 1023 at 1.

¹⁰²⁷ See Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, by Special Representative of the Secretary General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, John Ruggie, A/HRC/17/31 (UN Human Rights Council, 2011).

¹⁰²⁸ See SRSF, *Policy Framework*, *supra* note 1023 at para 9.

¹⁰²⁹ See SRSF, *Policy Framework*, *supra* note 1023; SRSF, *UNGPs*, *supra* note 1024 at para 6.

¹⁰³⁰ SRSF, *Policy Framework*, *supra* note 1023 at para 9.

¹⁰³¹ See OHCHR, *The Practical Application of the Guiding Principles on Business and Human Rights to the Activities of Technology Companies*, HRC, 50th Sess, UN Doc A/HRC/50/56 (2022) at para 9.

¹⁰³² OECD, *Guidelines for Multinational Enterprises: 2011 Edition*, (OECD, 2011).

See John Gerard Ruggie, Caroline Rees & Rachel Davis, “Ten Years After: From UN Guiding Principles to Multi-Fiduciary Obligations” (2021) 6:2 Business and Human Rights Journal 179 at 196; Michael K Addo, “The Reality of the United Nations Guiding Principles on Business and Human Rights” (2014) 14 Human Rights Law Review 133; René Wolfstetter & Yingru Li, “Business and Human Rights Regulation After the UN Guiding Principles:

popular point of reference for some corporations with data-driven business model setting out their commitments to human rights.¹⁰³³ Given their significance, this thesis will use the UNGPs to illustrate the current understanding of corporations' role within the context of international human rights frameworks.

Despite their widespread adoption, the UNGPs have faced criticism for not addressing the structural issues created by international law that have facilitated the impunity of transnational corporations in human rights violations, and they do not establish (nor propose the creation of) mandatory obligations for corporations, enforcing mechanisms, or overseeing bodies.¹⁰³⁴

In addition to these criticisms, one of the main problems with the UNGPs is their assumption that corporate actors are benevolent and responsible, and will therefore fulfill their moral responsibility to respect human rights, including identifying and addressing risks in their business model. However, similarly to the limitations of data protection discussed above, this assumption is flawed. Corporations are likely to respect human rights only to the extent that their profits are not materially affected, especially in a voluntary system, such as Pillar II of the UNGPs, where there are no fines or real consequences. This lack of enforcement makes the cost-benefit calculation of whether to respect human right or not easier for corporations.¹⁰³⁵

Accountability, Governance, Effectiveness" (2022) 23 Human Rights Review 1.

¹⁰³³ See e.g., Miranda Sissons, "Our Commitment to Human Rights" (16 March 2021) online (Newsroom): <about.fb.com/news> [<http://web.archive.org/web/20221220121005/https://about.fb.com/news/2021/03/our-commitment-to-human-rights/>]; Isabel Ebert & Ana Beduschi, *Regulating Business Conduct in the Technology Sector: Gaps and Ways Forward in Applying the UNGPs*, Research Brief (Geneva Academy, 2022).

¹⁰³⁴ See e.g., Penelope Simons, "International Law's Invisible Hand and the Future of Corporate Accountability for Violations of Human Rights" (2012) 3:1 Journal of Human Rights and the Environment 5; Sara Seck & Kirsten Stefanik, "Business and Human Rights: Challenges in Accessing Remedy and Justice Human Rights" in Gordon DiGiacomo, ed, *Human Rights: Current Issues and Controversies* (Toronto: University of Toronto Press, 2016) 381 at 393; Surya Deva & Harpreet Kaur, "Business and Human Rights: From 'Tokenism' to 'Centring' Rights and Rights-Holders" in Marianna Leite & Matti Kohonen, eds, *Righting the Economy: Towards a People's Recovery from Economic and Environmental Crisis* (Newcastle upon Tyne, UK: Agenda Publishing, 2024) 43.

¹⁰³⁵ See Part I-B, *above*.

See also Bakan, *New Corporation*, *supra* note 5 at 33.

Moreover, not only have the UNGPs failed to effectively constrain corporate behaviour, they have inadvertently contributed to the pathological personality of corporations. They have provided a legitimate basis for corporations to enhance their “good neighbour” image. The unanimous endorsement and subsequent adoption of the UNGPs at various levels have given corporations the legitimacy to use them as a tool to demonstrate that they care about the human rights consequences of their activities.¹⁰³⁶ This credibility, combined with the absence of binding responsibilities, has opened the door for corporations to enhance their “good neighbour” image while shaping the international discourse to their advantage.¹⁰³⁷

B. B-Tech Analysis of the UNGPs

The UNGPs have been criticized for being too lenient on corporations,¹⁰³⁸ a criticism exemplified by the guidance provided by the OHCHR’s B-Tech project, an initiative designed to provide guidance on the implementation of the UNGPs for corporations in the technology industry. The guidance of the B-Tech project reaffirms that the UNGPs assume that corporations are benevolent and responsible, without a thorough examination of their business practices. This assumption weakens the effectiveness of the framework in addressing the challenges posed by corporate behaviour.

The B-Tech project, launched in 2019, aims to provide authoritative guidance and resources on the implementation of the UNGPs in the technology sector,¹⁰³⁹ and to this end has

¹⁰³⁶ See Addo, “Reality of the UNGP”, *supra* note 1032.

¹⁰³⁷ See Deva, “From Business or Human Rights to Business and Human Rights”, *supra* note 483 at 7 (“Businesses are creating the public impression of being leaders in respecting human rights, but without bringing any fundamental changes to their current business models”).

¹⁰³⁸ See Nicola Jägers, “UN Guiding Principles on Business and Human Rights: Making Headway towards Real Corporate Accountability?” (2011) 29:2 *Netherlands Quarterly of Human Rights* 159; Simons, “International Law’s Invisible Hand”, *supra* note 1034.

¹⁰³⁹ See OHCHR, “B-Tech Project”, *supra* note 848.

published a series of foundational papers on the three pillars of the UNGPs in four key areas.¹⁰⁴⁰

The foundational paper on addressing human rights risks in business models, one of the focus areas, highlights that while the corporate business models used by corporations in the technology sector (e.g., social media, search engines, and the gig economy) have led to remarkable innovations and given many people access to life-changing technologies, they can also perpetuate human rights infringements, undermine democratic values, and widen inequalities.¹⁰⁴¹

The paper highlights that these risks are linked to the design and implementation of the underlying technologies, such as algorithmic systems,¹⁰⁴² pointing out that algorithmic systems can be “legitimately designed” to promote content that increases engagement or keeps users on a site, resulting in more advertising revenue. But the same design can also result in the “unintended” promotion of inflammatory and abusive content.¹⁰⁴³

This example illustrates the problem with the UNGPs as a lenient framework. By framing the design of algorithms that keep users engaged as an acceptable design strategy to increase revenue, the B-Tech project downplays the harmful aspects of corporate data practices, such as profiling and the tailoring of “personalized” services and information,¹⁰⁴⁴ and sidesteps critical questions about their manipulative features, which scholars have argued foster addiction and give corporations disproportionate influence over individuals.¹⁰⁴⁵

¹⁰⁴⁰ These areas are: addressing human rights risks in business models; human rights due diligence and end-use; accountability and remedy; and “a smart mix of measures:” exploring regulatory and policy responses to human rights challenges linked to digital technologies. See OHCHR, *supra* note 848.

¹⁰⁴¹ See B-Tech, *Addressing Business Model Related Human Rights Risks*, OHCHR (2020) B-Tech Foundational Paper online: <ohchr.org> [http://web.archive.org/web/20231218140015/https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf] at 4.

¹⁰⁴² See B-Tech, *Business Model Related HHRR Risks*, *supra* note 1041 at 5.

¹⁰⁴³ See B-Tech, *Business Model Related HHRR Risks*, *supra* note 1041.

¹⁰⁴⁴ See. Chapter IV-III.C., *above*.

¹⁰⁴⁵ See Chapter IV-III.C., *above*.

Moreover, by framing the consequences as “unintended,” the B-Tech project not only fails to adequately analyze the motivations of corporations, but also frames these risks as if they were beyond the control of corporations, helping to build on the “good neighbour” image of corporations. However, given the pathological tendencies and radical indifference of corporations, it is worth asking whether such “unintentional” promotion of harmful content is truly unintentional, or rather a deliberate design choice made in the pursuit of maximizing profit. For instance, if a corporation like Meta Inc. takes a considerable amount of time to remove certain types of content from its platforms, and actively modifies its algorithms to either prevent or promote certain types of content,¹⁰⁴⁶ should we continue to label this as an “unintentional” consequence of technological design?

In addition, the B-Tech report highlighted that even if a business model or strategy has inherent human rights risks, this does not necessarily mean that a corporation cannot operate in a human rights-respecting manner or that the business model must be abandoned altogether. Rather, the corporation must demonstrate that it is taking reasonable steps, in line with the UNGPs, to prevent, reduce, and remedy any harm to people.¹⁰⁴⁷

This lenient approach fails to address the fundamental problems inherent in business models and may allow corporations to continue potentially harmful practices under the guise of compliance with the UNGPs. If corporations are only required to demonstrate that they are taking reasonable steps to minimize the risks associated with the technologies they develop, use, and profit from in order to meet their international obligations, this framework may inadvertently

¹⁰⁴⁶ See e.g., the text accompanying note 645, *above*.

¹⁰⁴⁷ See B-Tech, *Business Model Related HHRR Risks*, *supra* note 1041 at 6.

provide corporations with data-driven business models with the means to normalize and justify their mass dataveillance operations and the potential risks they pose.

C. Enhancing the “Good Neighbour” Image: Corporations as Protectors

The lenient approach of the UNGPs has also allowed corporations to control the discourse and enhance their “good neighbour” image while avoiding scrutiny of their data practices. Corporations with data-driven business models have developed self-regulatory initiatives to demonstrate their commitment to upholding human rights, particularly privacy and freedom of expression, in their operations by presenting themselves as protectors of their users from government surveillance. As Rikke Frank Jørgensen research shows, corporations like Meta Inc. and Google Inc. “see themselves as strongly committed to—and actively promoting—human rights.”¹⁰⁴⁸ However their commitment to human rights focusses on potential human rights violations caused by governments, and pays less attention to areas where their own business practices may negatively impact users’ rights and freedoms.

Initiatives such as the Global Network Initiative (GNI), and Reform Government Surveillance (RGS) coalition are examples of this dynamic. The GNI’s mission is “to protect and advance freedom of expression and privacy in the ICT industry globally.”¹⁰⁴⁹ To achieve this mission, the GNI, a coalition that includes Meta Inc., Google Inc., and Microsoft Inc.,¹⁰⁵⁰ has established a set of principles that assert that privacy—a fundamental human right essential to

¹⁰⁴⁸ Rikke Frank Jørgensen, “What Platforms Mean When They Talk About Human Rights” (2017) 9:3 Policy & Internet 280 at 291.

¹⁰⁴⁹ Global Network Initiative, “GNI Principles”, *supra* note 673 at preamble.

¹⁰⁵⁰ In June 2021, Uber joined the initiative as an observer, but as of 2023, it is no longer part of the initiative in any capacity. Global Network Initiative, “Uber Joins GNI as a Company Observer” (27 June 2021) online: <globalnetworkinitiative.org> [<https://web.archive.org/web/20240116105143/http://web.archive.org/screenshot/https://globalnetworkinitiative.org/uber-joins-gni-as-a-company-observer/>].

human dignity, personal security, identity preservation, and freedom of expression in the digital age¹⁰⁵¹—should only be restricted by governments in narrowly defined situations that comply with internationally recognized laws and standards¹⁰⁵² Participating organizations implement the GNI Principles within their organization, and are independently assessed every two years.¹⁰⁵³

Similarly, the RGS, which includes ten major technology corporations including Meta Inc. and Uber Inc.,¹⁰⁵⁴ calls on the governments around the world to reform the laws and practices that regulate government surveillance systems.¹⁰⁵⁵ By advocating that governments adhere to the ten principles for surveillance outlined by the RGS,¹⁰⁵⁶ these corporations are further reinforcing their role as protectors of their users from government overreach.¹⁰⁵⁷

The narrow focus of corporations with data-driven business models on their human rights responsibilities to respect individuals' right to privacy is not surprising, given that under the UNGPs, corporations are responsible for defining, identifying, and addressing the potential and actual impacts of their business models on specific human rights.¹⁰⁵⁸ Given the incompatibility of

¹⁰⁵¹ See Global Network Initiative, “GNI Principles”, *supra* note 673.

¹⁰⁵² See Global Network Initiative, *supra* note 673.

¹⁰⁵³ See Global Network Initiative, “Company Assessments” (last visited 10 January 2023) online (Global Network Initiative): <globalnetworkinitiative.org> [<http://web.archive.org/web/20231220144913/https://globalnetworkinitiative.org/company-assessments/>].

¹⁰⁵⁴ The other members are Amazon, Apple, Dropbox, Google, Microsoft, Snap Inc, X (formerly Twitter), and Yahoo!. See Reform Government Surveillance, “Purpose and Members” (last visited 24 August 2023) online: <reformgovernmentsurveillance.com> [<http://web.archive.org/web/20231220133513/https://www.reformgovernmentsurveillance.com/about>].

¹⁰⁵⁵ See Meta Inc, “Meta Human Rights Report: Insights and Actions 2020-2021” (July 2022) online (PDF): <https://about.fb.com/wp-content/uploads/2022/07/Meta_Human-Rights-Report-July-2022.pdf> at 40.

¹⁰⁵⁶ See Reform Government Surveillance, “Purpose and Members”, *supra* note 1054.

¹⁰⁵⁷ See also Yael Ronen, “Big Brother’s Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers” (2015) 31:80 *Utrecht Journal of International and European Law* 72.

¹⁰⁵⁸ See SRSRG, *UNGPs*, *supra* note 1024 at principles 10-24.

See also John Sherman III, “Beyond CSR: The Story of the UN Guiding Principles on Business and Human Rights” (2020) Harvard Kennedy School, Working Paper No. 71 at 4.

mass dataveillance practices with the right to privacy and freedom of expression,¹⁰⁵⁹ it is not surprising that these corporations choose to focus the conversation on government surveillance and their efforts to protect these rights in these cases, and exclude from the conversation the broader implications of their own business models.

The framing of corporations as guardians against government surveillance is consistent with a broader trend of prioritizing privacy protection from state actors, especially in the wake of the Snowden revelations.¹⁰⁶⁰ While it is positive that corporations with data-driven business models are taking steps to prevent unlawful government surveillance, these actions do not absolve them of their responsibility for their own mass dataveillance systems.

The narrative that corporations are able to construct and support under the UNGPs, in which governments are portrayed as the primary actor capable of implementing invasive surveillance systems, and corporations are positioned as protectors against such intrusions, overlooks and even obscures the fact that corporations with data-driven business models hold significant amounts of data that governments seek. As a result, this framing allows corporations to hide their active role as intrusive actors, to divert attention away from their own data practices and privacy infringements, and allows them to enhance their “good neighbour” image.

D. UN Perspective on Corporate Data Practices

The narrative that corporations have constructed under the UNGPs is also present in the way that corporate data collection and processing practices have been framed in the UN system. While acknowledging the potential risks to privacy and other rights posed by corporate data practices, these discussions have focussed primarily on two aspects: the role of the states as

¹⁰⁵⁹ See also Amnesty International, *Surveillance Giants*, *supra* note 766.

¹⁰⁶⁰ See Amnesty International, *Surveillance Giants*, *supra* note 766 at 25.

primary surveillance actors and the impact of government-led surveillance on human rights;¹⁰⁶¹ and the responsibilities of corporations, framed in terms of protecting users from other users, such as protecting children from harmful online practices, and from government surveillance, as well as providing users with adequate information about their data practices. This approach has helped corporations with data-driven business models to promote their image as “good neighbours” who care about upholding privacy rights, while continuing their mass dataveillance practices without any real challenge or scrutiny.

The UN has raised concerns about the potential risks of corporate data collection and processing.¹⁰⁶² However, these risks have mainly focussed on government surveillance, emphasizing that corporate data practices are problematic because they feed government surveillance.¹⁰⁶³ For instance, the OHCHR has identified the growing trend of corporations and states exchanging and merging personal data as problematic,¹⁰⁶⁴ and has also noted programs that allow states direct access to corporations’ data streams pose several risks, as they bypass key procedural safeguards and are vulnerable to abuse.¹⁰⁶⁵

This framing is problematic because it overlooks the additional risks posed by corporate dataveillance systems. It also influences the calls for regulatory action and the responsibility of corporations to respect the right to privacy. The OHCHR, for example, has emphasized the need for appropriate legislative action on corporate data practices. However, these calls have primarily

¹⁰⁶¹ See Chapter III-III, *above*.

¹⁰⁶² See UN, *Right to Privacy (GA, 2017)*, *supra* note 846.

¹⁰⁶³ See Chapter III-III, *above*.

¹⁰⁶⁴ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at para 13; OHCHR, *The Right to Privacy in the Digital Age*, HRC, 51st Sess, UN Doc A/HRC/51/17 (2022) at para 42.

¹⁰⁶⁵ See OHCHR, *Right to Privacy (2022)*, *supra* note 1064 at para 41.

focussed on improving the state practices, such as state requests to corporations and access to extraterritorially held information or information sharing with other states.¹⁰⁶⁶

Guided by the UNGPs, the UN framework distinguishes two types of responsibilities for corporations: one relating to their involvement in or facilitation of government surveillance, and the other relating to their responsibilities for their own data processing operations. With respect to the first type, corporations have a duty to protect individuals from government surveillance. This includes assessing the privacy risks associated with potential government requests for access to their user data,¹⁰⁶⁷ assessing the broader human rights impact of how their technologies might be used by governments for surveillance,¹⁰⁶⁸ and implementing human rights policies, including rules to prevent arbitrary or unlawful access to their data.¹⁰⁶⁹

With regard to the second type, corporations have a primary responsibility to protect privacy through transparency. This includes informing users about the collection, use, sharing, and retention of their personal data, as well as establishing transparent data processing policies that allow for informed user consent.¹⁰⁷⁰ This framing of the corporate responsibility with respect to the right to privacy is not only limited in that it does not take into account the broader risks and implications of corporate mass dataveillance, but it is also consistent with the narrow privacy

¹⁰⁶⁶ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at para 36.

¹⁰⁶⁷ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at para 46; OHCHR, *Right to Privacy (2014)*, *supra* note 251 at para 44.

¹⁰⁶⁸ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at para 46. See also UN, *SR Right to Freedom of Opinion and Expression (2019)*, *supra* note 372.

¹⁰⁶⁹ See OHCHR, *Right to Privacy (2018)*, *supra* note 17 at paras 47-48.

¹⁰⁷⁰ See e.g., UN, *Right to Privacy (GA, 2017)*, *supra* note 846 at para 6; UN, *The Right to Privacy in the Digital Age*, HRC, 34th Sess, UN Doc A/HRC/34/L.7/Rev.1 (2017) GA Res 34 at para 5; UN, *The Right to Privacy in the Digital Age*, GA, 75th Sess, UN Doc A/RES/75/176 (2020) GA Res 75/176 at para 8; OHCHR, *Right to Privacy (2018)*, *supra* note 17 at paras 29-31; UN, *The Right to Privacy in the Digital Age*, GA, 73rd Sess, UN Doc A/RES/73/179 (2019) GA Res 73/179 at para 7.

discourse promoted by corporations with data-driven business models that reduce the right to privacy to issues of choice and control.¹⁰⁷¹

While the OHCHR has also recognized the duty of states to protect against abuses of the right to privacy by corporations, it has not specified the nature of the risks posed by such abuses or provided guidance on how they should be regulated,¹⁰⁷² beyond emphasizing the importance of data protection principles.¹⁰⁷³ A shift in this perspective occurred in OHCHR's 2022 report, which highlighted that the widespread tracking of internet users by numerous organizations, including advertisers, financial institutions, and data brokers, called for increased scrutiny in international human rights discussions.¹⁰⁷⁴ This call will hopefully lead to further discussions that take the processing activities of corporations more seriously in terms of their mass dataveillance capabilities, and not just in the context of government surveillance.

This section has shown how the UNGPs, and their interpretation through initiatives such as the B-Tech project, have significant limitations in addressing the complex challenges posed by the mass dataveillance systems of corporations with data-driven business models. While these frameworks aim to promote responsible corporate behaviour, they often fail to adequately address the fundamental problem inherent in mass dataveillance practices.

The lenient approach to corporations, coupled with an emphasis on self-regulation and protection from government surveillance, fails to fully acknowledge the potential harms caused by corporate data practices themselves. This narrow focus not only obscures the active role of

¹⁰⁷¹ See Chapter IV-I.B.1, *above*.

¹⁰⁷² See OHCHR, *Right to Privacy* (2018), *supra* note 17 at Para 61(i) (States Obligations, and Business Enterprises Responsibilities) at par 61(i). (Stated have the duty to protect against abuses of the right to privacy by business enterprises “by taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication”).

¹⁰⁷³ See OHCHR, *Right to Privacy* (2018), *supra* note 17 at paras 28-33.

¹⁰⁷⁴ See OHCHR, *Right to Privacy* (2022), *supra* note 1064 at para 53.

corporations in privacy infringements, but also allows them to position themselves as guardians of users' rights while continuing potentially harmful data collection and processing activities. To effectively address the human rights implications of data-driven business models, a broader and more critical approach is needed, one that scrutinizes corporate practices as closely government surveillance, and holds corporations accountable for the full range of their human rights impacts.

III. Conclusions

Within international human rights frameworks, there are two main approaches to regulating the impact of corporate surveillance capabilities on human rights. First, states have established data protection frameworks to regulate the processing of data by corporations, thereby fulfilling their responsibility to prevent, protect, and remedy corporate interference with human rights, as defined in the ICCPR. Second, the UNGPs have been seen as an attempt to hold corporations with data-driven business models accountable for protecting human rights, such as privacy, through their operations.

This chapter has examined the limitations of both approaches in addressing corporate practices of mass dataveillance. The analysis highlights several key issues. First, data protection regulations such as the GDPR and PIPEDA are based on flawed assumptions about corporate behaviour and technological capabilities. They assume that data collection and processing by corporations are necessary and desirable, and that corporations will act benevolently to protect users' rights. However, these assumptions fail to take into account the pathological nature of corporations, which prioritize profit above all else.

Second, the collaborative governance approach of data protection regulations, which relies on corporations to interpret key aspects, is problematic given the pathological traits of corporations. Examples such as DPIAs, the choice of legal grounds for processing, and the

implementation of Privacy by Design illustrate how corporations can interpret requirements in a self-serving way.

Third, international human rights frameworks such as the UNGPs also make problematic assumptions about corporate empathy and responsibility. Their lenient approach allows corporations to enhance their “good neighbour” image while avoiding scrutiny of harmful data practices. Moreover, the framing of corporations as protectors against government surveillance, both in the corporate initiatives and in the UN perspectives, obscures corporations’ own role in mass dataveillance and allows them to deflect attention from their privacy infringements.

Overall, these regulatory approaches provide inadequate tools for assessing the societal impact and desirability of corporate data collection and processing practices. They fail to meaningfully constrain the profit-driven nature of corporate mass dataveillance and, as such, they should not be considered adequate for states to fulfill their obligations under Article 2(2) of the ICCPR.

As the next chapter will argue, in order for states to adequately fulfill their international responsibility under Article 2(2) of the ICCPR, they need to put in place a regulatory framework that takes into account the pathological personality of corporations and that aims to directly regulate corporations’ mass dataveillance capabilities by limiting the business models that enable and incentivize them implement, maintain, and expand mass dataveillance systems.

Chapter VI. Regulating Corporate Dataveillance in the Face of Socio-technical Change

The psychopathic personality of corporations is becoming increasingly problematic because the institutional character that has given them this personality and their power over democratic institutions and society has not been properly regulated. Since the 1980s, the role of the law as “the main institutional vehicle for policing corporations in aid of public interests” has begun to decline.¹⁰⁷⁵ In its place, various forms of “private regulation,” such as self-regulation, motivated by economic logic and guided by market forces, began to emerge.¹⁰⁷⁶ This shift has created an environment in which corporate power has grown without any major constraints.¹⁰⁷⁷

Three main features contribute to the lack of adequate limits on the power of corporations in general, and those with a data-driven business model in particular. First, the constant lobbying efforts of corporations are aimed at changing the regulatory environment in their favour. In the case of corporations with a data-driven business model, their lobbying power has increased significantly due to the political and economic influence they have gained through their mass dataveillance systems.¹⁰⁷⁸ Second, their transnational nature makes it difficult for a single national government to regulate them effectively,¹⁰⁷⁹ a challenge that is not unique to corporations with a data-driven business model, but applies to multinational corporations across various industries.

¹⁰⁷⁵ See Joel Bakan, “The Invisible Hand of Law: Private Regulation and the Rule of Law” (2015) 48:2 Cornell International Law Journal 279 at 280.

¹⁰⁷⁶ See Bakan, “The Invisible Hand of Law”, *supra* note 1075. See also Bakan, *The Corporation*, *supra* note 1 at 89–90, 161–63; Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 75.

¹⁰⁷⁷ See Bakan, *New Corporation*, *supra* note 5. See also Thomas Linzey, “Killing Goliath: Defending Our Sovereignty and Environmental Sustainability through Corporate Charter Revocation in Pennsylvania and Delaware” (1997) 6:1 Penn State Environmental Law Review 31 at 34–35.

¹⁰⁷⁸ See Chapter IV-III.C, *above*.

¹⁰⁷⁹ See e.g., Lindman, Makinen & Kasanen, “Big Tech’s Power, Political CSR and Regulation”, *supra* note 818.

Finally, their efforts to build a good neighbour image, including promises to look after people's rights such as privacy—what Bakan called the new corporate movement—has led to a push for greater self-regulation.¹⁰⁸⁰

First, in order to fulfill their primary purpose—to generate profit for shareholders—and driven by their pathological personality, corporations have actively attacked and crippled democratic institutions in order to retain more power to operate in ways that better serve their interests.¹⁰⁸¹ For example, regulations tend to make their operations costlier by imposing restrictions that translate into higher financial operating costs.¹⁰⁸² These include the need to pay labour costs, environmental restrictions, and the need to maintain infrastructure for safety reasons. Corporations therefore actively lobby regulators in order to have a direct influence on ensuring that the regulations adopted impose the lowest possible costs on their operations.¹⁰⁸³

To this end, they set up lobby offices or teams in various key regulatory centres, such as Washington D.C., and Brussels, and invest in national or regional policy teams to engage directly with policymakers in the countries where they operate.¹⁰⁸⁴ Moreover, transnational corporations' efforts to shape the regulatory landscape do not stop at the national level; they are also directly

¹⁰⁸⁰ See Bakan, *New Corporation*, *supra* note 5.

¹⁰⁸¹ See Bakan, *The Corporation*, *supra* note 1 at ch 4.

¹⁰⁸² See Bakan & Abbott, "New Corporation Documentary", *supra* note 166 at 57:20.

¹⁰⁸³ See Bakan & Abbott, "New Corporation Documentary", *supra* note 166 at 52:00-54:44. See also Mikkel Flyverbom, "Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations" in Christina Garsten & Adrienne Sörbom, eds, *Power, Policy and Profit: Corporate Engagement in Politics and Governance* (Cheltenham, UK: Edward Elgar Publishing, 2017) 115 (Flyverbom argues that in the case of tech companies in addition to traditional lobby strategies, they also influence governments around the world through other modes of corporate advocacy).

¹⁰⁸⁴ See e.g., Pawel Popiel, "The Tech Lobby: Tracing the Contours of New Media Elite Lobbying Power: Communication, Culture & Critique" (2018) 11:4 Communication, Culture & Critique 566; Flyverbom, "Corporate Advocacy in the Internet Domain", *supra* note 1083.

involved in global economic regulations, either by acting as transnational lobbies, or by setting up rules themselves, within transnational private self-governance or public-private partnerships.”¹⁰⁸⁵

In the case of corporations with data-driven business model, there are several examples of active lobbying to avoid regulations that would affect their profits.¹⁰⁸⁶ A recent report found that in the digital economy sector, the EU is targeted by 651 corporations and associations, with large corporations such as Google Inc., Amazon Inc., and Meta Inc. being the main drivers of the increase in lobbying spending.¹⁰⁸⁷ As of September 2023, when the report was published, the top 10 digital corporations spent a combined €40 million a year on lobbying, accounting for more than a third of the sector’s total spending. In the EU Parliament, four of the top six lobby spenders are large corporations with data-driven business models, with Meta Inc. leading the list.¹⁰⁸⁸

Second, it has become increasingly difficult to regulate transnational corporations because they are not easily tied to a single jurisdiction from a regulatory perspective.¹⁰⁸⁹ This poses

¹⁰⁸⁵ Fabricius, Kollmer & Eckhardt, “Instances of Digital Dark Nudging”, *supra* note 794 at 279.

¹⁰⁸⁶ See e.g., Lomas, “Big Tech Lobbied to Weaken EU Rules”, *supra* note 523; Cadwalladr & Campbell, “Revealed”, *supra* note 523; Natasha Lomas, “Uber Lobbies for ‘Prop 22’-Style Gig Work Standards in the EU”, *TechCrunch* (15 February 2021), online: <techcrunch.com> [<http://web.archive.org/web/20240102171758/http://web.archive.org/screenshot/https://techcrunch.com/2021/02/15/uber-lobbies-for-prop-22-style-gig-work-standards-in-the-eu/>]; Ben Brody & Bill Allison, “Lobbying Group for Facebook and Google to Pitch Self-Regulation of Ads”, *Bloomberg* (24 October 2017), online: <bloomberg.com> [<http://web.archive.org/web/20180509015759/https://www.bloomberg.com/news/articles/2017-10-24/lobby-group-for-facebook-google-to-pitch-self-regulation-of-ads>].

¹⁰⁸⁷ See Corporate Europe Observatory, “Lobbying Power of Amazon, Google and Co Continues to Grow” (8 September 2023) online: <corporateeurope.org> [<http://web.archive.org/web/20231221122155/https://corporateeurope.org/en/2023/09/lobbying-power-amazon-google-and-co-continues-grow>].

¹⁰⁸⁸ See Corporate Europe Observatory, *supra* note 1087.

¹⁰⁸⁹ See Coughlan et al, *Law Beyond Borders*, *supra* note 865 at 131–32; Doris Fuchs & Markus ML Lederer, “The Power of Business” (2007) 9:3 *Business and Politics* 1; Larry Cata Backer, “Regulating Multinational Corporations: Trends, Challenges, and Opportunities Multinational Corporations” (2015) 22:1 *Brown Journal of World Affairs* 153.

See also Rikke Frank Jørgensen, “Human Rights and Private Actors in the Online Domain” in Molly K Land & Jay D Aronson, eds, *New Technologies for Human Rights Law and Practice* (Cambridge, UK: Cambridge University Press, 2018) 243.

challenges because it becomes difficult for a national government to enact regulations that effectively create a framework to address the challenges posed by these corporations.¹⁰⁹⁰ In addition, their transnational structure allows them to locate their activities in states where regulation poses the least or no obstacle to the activity in which the corporation wishes to engage.¹⁰⁹¹

In the case of transnational corporations with a data-driven business model, they have also developed and introduced technological layers that significantly affect how individuals and governments access information and communicate (as in the case of Meta Inc.’s platforms), and have also created value for individuals who depend on them as a source of economic income (as in the case of Meta Inc. and Uber Inc.’ platforms). The combination of the power wielded by these corporations and the growing global dependence on the technologies they develop and market also has a negative impact on the ability of states to exercise their jurisdiction.¹⁰⁹²

Third, as part of the new corporate movement, corporations have successfully created a “good neighbour” image and have used this image to argue that they are socially responsible and public-spirited enough to self-regulate, and that there is no need for external regulation.¹⁰⁹³ In the case of corporations with a data-driven business model, they have gone a step further, arguing that self-regulation is the best option because public regulation would stifle innovation,¹⁰⁹⁴ and that

¹⁰⁹⁰ Deva refers to this as an “asymmetry between territorial laws and extraterritorial business operations.” See Surya Deva, “Business and Human Rights: Alternative Approaches to Transnational Regulation” (2021) 17 Annual Review of Law and Social Science 139 at 144.

¹⁰⁹¹ See Coughlan et al, *Law Beyond Borders*, *supra* note 865 at 131–32.

¹⁰⁹² See Coughlan et al, *Law Beyond Borders*, *supra* note 865. See also Mikkel Flyverbom, Ronald Deibert & Dirk Matten, “The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business” (2019) 58:1 Business & Society 3.

¹⁰⁹³ See Bakan, *New Corporation*, *supra* note 5 at 89; Bakan & Abbott, “New Corporation Documentary”, *supra* note 166 at 55:32-56:09.

¹⁰⁹⁴ See Bakan, *New Corporation*, *supra* note 5 at 139–40. See also Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 189–90.

their innovation is important to society because their technology, products, and services are not just a commodity but the solution to many of today's social problems.¹⁰⁹⁵ While it is true that regulation can limit innovation, this is not necessarily a bad thing. Since the early twentieth century, regulation has been an important tool for democratic societies to balance the benefits and harms of corporate-driven innovation.¹⁰⁹⁶ Moreover, given that corporations are driven by financial self-interest, regulation remains essential to ensure that their actions do not harm society as a whole.¹⁰⁹⁷

These three features highlight the complexity of regulating corporate power. Crucially, there is no single solution for this problem. Effective regulation of corporations requires a variety of measures, including limiting their influence over democratic institutions, increasing their accountability for the harms caused by their services,¹⁰⁹⁸ and ensuring cooperation between national governments to establish regulations and standards that prevent corporations from exploiting favourable legal regimes. However, given that the profitability of corporate mass dataveillance systems is at the root of a number of other problems,¹⁰⁹⁹ this thesis calls for the urgent regulation of these systems.

As explained earlier, governments have chosen to address the regulation of data processing by corporations through data protection frameworks. The previous chapter argued that current data protection frameworks, such as GDPR and PIPEDA, do not fully take into account the pathological nature of corporations, their current technological capabilities, and the risks and harms these

¹⁰⁹⁵ See Bakan, *New Corporation*, *supra* note 5 at 106.

¹⁰⁹⁶ See Bakan, *New Corporation*, *supra* note 5 at 113–14.

¹⁰⁹⁷ See Bakan, *New Corporation*, *supra* note 5.

¹⁰⁹⁸ See e.g., Waldman, *Industry Unbound*, *supra* note 15 at 236.

¹⁰⁹⁹ See Chapter IV-III.C, *above*.

create. For this reason, the previous chapter argued that these frameworks are unable to effectively regulate corporate mass dataveillance systems, and thus fail to fulfill states' responsibilities under Article 2(2) of the ICCPR.¹¹⁰⁰

Given that data protection frameworks are not able to effectively regulate corporate mass dataveillance systems and therefore do not provide an effective protection against the risk they pose to the right to privacy, states have a duty to establish a new regulatory framework that specifically addresses corporate mass dataveillance capabilities, making them specific and exceptional, rather than the *status quo* as is currently the case. It is important to stress that states not only have the responsibility to regulate corporations, but also have the power to do so. After all, corporations are legal institutions whose existence depends on the legal system that gives them their rights.¹¹⁰¹

As a final step in the methodology,¹¹⁰² this chapter proposes a regulatory framework for states to fulfill their international human rights obligations, and adequately regulate corporate mass dataveillance capabilities. To this end, the chapter is divided into two main parts. The first part argues that there is a need for a new regulatory framework, primarily aimed at limiting corporate mass dataveillance capabilities. The second part explains the two key features that the new framework should have: a corporate duty to limit revenue streams, and a mandatory dissolution of the corporation as a measure for non-compliance.

¹¹⁰⁰ See Chapter V-I, *above*.

¹¹⁰¹ See Bakan, *The Corporation*, *supra* note 1 at 166; Waldman, *Industry Unbound*, *supra* note 15 at 233.

See also Beate Sjøfjell, "How Company Law Has Failed Human Rights-and What to Do About It" (2020) 5:2 Business and Human Rights Journal 179.

¹¹⁰² See Chapter II-II.B., *above*.

See also Bennett Moses, "How to Think about Law, Regulation and Tech", *supra* note 18 at 17.

I. The Need for a New Regulatory Framework

Laws and regulations are enacted in a particular socio-technical context with explicit and implicit assumptions about what is possible at the time. As new technological capabilities are enabled, these assumptions may lose their relevance or importance, creating a disconnect between the goals and assumptions of the regulation and the context it seeks to regulate.¹¹⁰³ As argued in the previous chapter, in the case of data protection regulation, there is a disconnect between the assumptions on which it is based and the current socio-technical environment that it seeks to regulate.

In the first place, data protection laws assume that data collection and processing must be undertaken by corporations, which is seen as desirable because it allows countries to remain competitive in the digital global economy. However, the rapid advances in technology that enable the generation, collection, and processing of vast amounts of data have made this assumption problematic. The assumption that data collection and processing is a necessary condition has limited the scope of the regulatory debate to after the data has been collected, excluding consideration of whether it should be collected in the first place. By focussing on setting rules for how corporations should manage data and ensuring that individuals have rights over it, these regulations have left it to corporations to assess and decide whether the collection and processing of data are desirable in the first place.¹¹⁰⁴

The limited scope of these regulations is problematic because of the second assumption on which they are based: that corporations are benevolent and capable of changing their behaviour, including the design of their products and services, to comply with the regulation and respect the

¹¹⁰³ See Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18.

¹¹⁰⁴ This is developed in detail in Chapter V-I.A, *above*.

rights of their users. Data protection regulation is based on a collaborative governance model that relies on corporations to carry out various processes and decisions, such as carrying out DPIAs, choosing the legal grounds for processing, and implementing PbD. However, the pathological personality of corporations means that they will interpret these requirements in a way that minimizes their negative impact on their profits. In other words, they will only consider the rights of their users if it does not affect their profits.¹¹⁰⁵

In light of these limits to data protection regulation, this thesis proposes to regulate corporate mass dataveillance capabilities by modifying existing corporate law to impose limits on the business model and the pathological personality of corporations as the actors responsible for creating and designing technologies with mass dataveillance capabilities, and as the actors deciding to implement them.¹¹⁰⁶ The following section explains the regulatory rationale, objectives, and targets of the proposed regulatory framework.¹¹⁰⁷

A. Regulatory Rationales: Democratic Oversight and Protecting Rights

The regulatory framework that this chapter will propose aims to regulate a socio-technical landscape that can be characterized by the widespread adoption of digital technologies that have facilitated the mass dataveillance of individuals by pathological corporations.¹¹⁰⁸ These systems

¹¹⁰⁵ This is developed in detail in Chapter V-I.B, *above*.

¹¹⁰⁶ In the case of a regulatory disconnection, Bennett Moses argues that it is necessary to determine the appropriate regulatory response, which could be to modify the existing regulations, apply existing laws to a new situation, or enact a new regulation that will better respond to the new socio-technical context. See Bennett Moses, “Why Have a Theory of Law & Tech Change?”, *supra* note 154; Bennett Moses, “Recurring Dilemmas”, *supra* note 156 at 249.

See also Brownsword, “So What Does the World Need Now?”, *supra* note 146.

¹¹⁰⁷ See Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18 at 17; Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152 at 585.

¹¹⁰⁸ See Chapter IV-III, *above*.

have become an important source of revenue for corporations, which often prioritize profit over all else, resulting in significant risks and harms to individual rights and society as a whole. The pervasive nature of these mass dataveillance systems not only interferes with the right to privacy, but also raises serious concerns about wider human rights implications.¹¹⁰⁹

In this context, the new regulatory framework should be based on two interrelated rationales: first, the protection from harm and the protection of privacy, which is internationally recognized as a human right; and second, the pursuit of democratic control to limit the power of corporations in shaping technological developments.¹¹¹⁰

The first rationale—the protection of individual rights—can be understood in terms of two key aspects. The first is the obligation of states to protect human rights, as mandated by national laws and international conventions such as the ICCPR and the ECHR.¹¹¹¹ The second aspect is the need to protect individuals from the harms and risks posed by technological change.¹¹¹²

As explained above, under the international human rights framework, states have a responsibility to take appropriate legislative measures to prevent and protect individuals from interference with their right to privacy, including when such interference is committed by legal persons.¹¹¹³ The proposed regulatory framework is thus rooted in the obligation of states to fulfill their obligations under international human rights law.

¹¹⁰⁹ See Chapter IV-III.C, *above*.

¹¹¹⁰ Bennett Moses identifies four main justifications for regulation in response to socio-technical change: market failure, social solidarity, protection against harm and risk to collectively desired rights, and the pursuit of democratic control. See Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152 at 583.

See also Tony Prosser, *The Regulatory Enterprise*, (New York: Oxford University Press, 2010) c 1.

¹¹¹¹ See Prosser, *The Regulatory Enterprise*, *supra* note 1110 at 13–15.

¹¹¹² See Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152 at 578–81.

¹¹¹³ See ICCPR, *supra* note 16 at art 17; *Pact of San Jose, Costa Rica*, *supra* note 196 at art 11; ECHR, *supra* note 195 at art 8.

See also OHCHR, *Right to Privacy (2018)*, *supra* note 17 at par 23; OHCHR, *General Comment No. 16*, *supra* note 362 at par 1, 9; Alex Conte, “Privacy, Honour and Reputation” in *Defining Civil and Political Rights*, 2d ed

With regard to the second aspect, the proposed regulatory framework is justified by the need to protect privacy against the risks posed by mass dataveillance systems implemented and maintained by corporations. As developed in detail in Chapter IV, these systems pose three main risks: first, the constant threat that the data collected could be accessed by unauthorized third parties or governments; second, the increasing economic and social power of the corporations that use these systems; and third, the facilitation of social control through corporations' direct access to individuals.¹¹¹⁴

The second regulatory rationale—democratic oversight—also has two elements: oversight of socio-technical change, and oversight of corporate power. First, Bennett Moses argues that because technology can be designed in different ways, it is crucial that particular technologies are subject to democratic debate. This process ensures that technological design remains responsive to diverse perspectives and that concerns about potential harm to different community groups are taken into account in shaping technological trajectories.¹¹¹⁵

Second, Bakan highlights the critical role of regulation as the primary mechanism by which governments control corporate behaviour. He emphasizes that regulation serves as the channel through which citizens, through their elected representatives, shape the rules that govern corporate behaviour. When regulation is weakened or rolled back, democratic control over corporations is diminished, which in turn erodes the scope of citizens' democratic rights.¹¹¹⁶ Bakan goes on to

(Routledge, 2009) 201 at 202; Danwood Mzikenge Chirwa, "State Responsibility for Human Rights" in Mashood A Baderin & Manisuli Ssenyonjo, eds, *International Human Rights Law: Six Decades after the UDHR and Beyond* (Abingdon, Oxon: Routledge, 2016) at 405; Kálin & Künzli, "Protection of Private Life", *supra* note 853 at 395–6; Clayton & Tomlinson, *Law of Human Rights*, *supra* note 853 at 1088, 1095.

¹¹¹⁴ See Chapter IV-III.C, *above*.

¹¹¹⁵ See Bennett Moses, "Regulating Sociotechnical Change", *supra* note 152 at 581. See also Winner, *The Whale and the Reactor*, *supra* note 7; Lessig, *Code*, *supra* note 7.

¹¹¹⁶ See Bakan, *The Corporation*, *supra* note 1 at 61.

argue that another rationale for regulation is that corporations are themselves products of regulation. He claims that regulation is necessary as a legal safeguard against the dangers that the law itself creates in the form of corporations.¹¹¹⁷

Democratic oversight in these two areas is an important rationale for the new regulatory framework, as corporations have the power to shape the socio-technical context of individuals by deciding on the design of the technologies that individuals use on a daily basis, and by choosing to use those technologies.¹¹¹⁸ Currently, the design of these technologies is influenced by corporations' need to generate, collect, and process large amounts of data about individuals and their behaviour. As explained in Chapter IV, the design and deployment of corporate mass dataveillance systems can be seen as a facet of the pathological nature of corporations, which prioritize profit above all else. This psychopathic corporate personality has facilitated the rise of surveillance capitalism, and has also contributed to the failure of current privacy rules to adequately limit corporate mass dataveillance and the risks and harms it poses.¹¹¹⁹

Given that the pathological nature of corporate behaviour, coupled with the lack of effective controls, has allowed mass dataveillance of individuals to become both profitable and widespread, by failing to regulate the institutional structures that enable this pathological corporate personality, governments are neglecting their duty to protect individuals from corporate invasions of privacy.

The risks and harms caused by corporations with psychopathic tendencies—whose pathological behaviour is both a product of and perpetuated by corporate law—have not been

¹¹¹⁷ See Bakan, *The Corporation*, *supra* note 1 at 61–62.

¹¹¹⁸ See Chapter IV-III.C, *above*.

See also Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 29 (They argue that companies exercise their power to influence and shape others' desire for technology by deciding where to innovate).

¹¹¹⁹ See Chapter IV-III, *above*.

adequately constrained by external regulations such as data protection.¹¹²⁰ These regulations are often seen by corporations as mere costs to be minimized or avoided in order to maximize profits, reducing compliance to a simple cost-benefit calculation.

Therefore, a regulatory framework that aims to protect individuals from corporate mass dataveillance systems and the risks and harms they created must include a reform of the institutional structures that sustain the psychopathic personality of the corporation. It must also ensure that compliance is transformed from a mere cost into a genuine constraint on corporate existence.

The proposed framework is therefore justified by the need to protect privacy, and to limit the power of corporations in the design and deployment of surveillance technologies. With these two rationales in mind, the next section outlines the regulatory goals and target of the proposed framework.

B. Regulatory Goal and Target

Having established the dual rationale for the proposed regulatory framework—protecting privacy and strengthening democratic control—this section outlines the specific goals and targets that the proposed framework must focus on in order to mitigate the harmful effects of corporate mass dataveillance and uphold democratic values. The regulatory goal refers to the main objective that the regulation seeks to achieve, while the regulatory target can be considered from two perspectives: as the object that the regulation seeks to regulate (e.g., a particular technological

¹¹²⁰ See the text accompanying note 1136, *below*, for an explanation of external and internal regulation.

artifact or conduct/behaviour),¹¹²¹ and as the subject at which the regulation is directed (e.g., the organization that produces a particular technological artifact or the individual who uses it).¹¹²²

1) Regulatory Goal

Under data protection regulations, the processing of personal data is not seen as an interference with privacy *per se*.¹¹²³ As a result, it is not framed as an exceptional practice that should only occur in limited circumstances, as is the case in the international human rights framework in relation to government-led surveillance. In such cases, the ECtHR and OHCHR have made it clear that the collection of data from individuals constitutes an interference with the right to privacy, regardless of whether the data are subsequently processed or used by government officials. Therefore, this practice should only take place in certain exceptional circumstances.¹¹²⁴ In contrast, data protection regulation frames the processing of personal data as an acceptable process that can take place on a regular basis, as long as it meets certain conditions, such as that the data are “obtained and processed fairly and lawfully.”¹¹²⁵

Given that corporations with a data-driven business model can generate and process substantial amounts of data through their mass dataveillance systems, and given the power that these corporations can wield over individuals and society,¹¹²⁶ it is necessary that the proposed

¹¹²¹ See e.g., Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152 at 584; Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18.

See also Clara Iglesias Keller, “Don’t Shoot the Message: Regulating Disinformation Beyond Content” in Carlos Blanco de Moraes, Gilmar Ferreira Mendes & Thomas Vesting, eds, *The Rule of Law in Cyberspace* (Cham: Springer International Publishing, 2022) 309 at 316–17.

¹¹²² See e.g., Lessig, *Code*, *supra* note 7 c 7.

¹¹²³ See WP29, *Opinion 06/2014*, *supra* note 892 at 6–7. See also Chapter V-I.A, *above*.

¹¹²⁴ See Chapter III-II, *above*.

¹¹²⁵ See WP29, *Opinion 06/2014*, *supra* note 892 at 6–7. See also Chapter V-I.A, *above*.

¹¹²⁶ See Chapter IV-III.C, *above*.

framework adopt the approach taken in the case of government surveillance, that is, that the collection and processing of data by corporations should be considered an interference with the right to privacy.¹¹²⁷

By considering these actions as an interference with the right to privacy, the proposed regulatory framework must ensure that the systematic collection and processing of data about individuals and their behaviours by corporations is consistent with international human rights requirements. Under the international human rights framework, any interference with the right to privacy must be exceptional and justified.¹¹²⁸ Therefore, the main regulatory goal of the proposed framework should be to limit the ability of corporations to engage in mass dataveillance.¹¹²⁹

The term “mass dataveillance systems” refers to technological systems that continuously and systematically collect, process, and organize data about individuals and their behaviours, with the aim of providing organizations with a basis for action towards those individuals.¹¹³⁰ In these cases, corporate profits depend on these systems continuously accumulating and collecting metadata that can be used beyond of what is necessary to improve services, which they use to accurately predict the future feelings, thoughts, and actions of individuals.¹¹³¹ Therefore, limiting the ability of corporations to engage in mass dataveillance requires a fundamental reassessment of the underlying business models that drive these practices. In particular, the framework should

¹¹²⁷ See Chapter III-II, *above*.

See also Kälén & Künzli, “Protection of Private Life”, *supra* note 853 at 378.

¹¹²⁸ See e.g., OHCHR, *General Comment No. 16*, *supra* note 362 at para 8; Paul M Taylor, “Article 17: Privacy, Home, Correspondence; Honour and Reputation” in *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee’s Monitoring of ICCPR Rights* (Cambridge: Cambridge University Press, 2020) 458 at 463.

¹¹²⁹ See Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18 at 19.

¹¹³⁰ See Chapter III-I, *above*. See also Rule, *Privacy in Peril*, *supra* note 8 at 14.

¹¹³¹ This is discussed in detail in Chapter IV-III, *above*

constrain business models that rely on mass data collection and predictive analytics by limiting the types of revenue streams available to corporations.

2) Regulatory Object

As noted above, mass dataveillance systems are a facet of the psychopathic personality of corporations, which is characterized by an obsessive focus on profits and share prices, greed, disregard for others and a tendency to break legal rules.¹¹³² Therefore, in order to achieve the goal of limiting corporate mass dataveillance, the proposed framework should focus on the institutional nature of corporations, in particular their legal structures, rather than on the technologies they use or the data they process.

Regulating the technologies directly, such as requiring that they have a certain set of features or functionalities or prohibiting others, may seem like a viable option. For instance, the regulation could require that the location data generated by digital technologies can only be processed internally. However, given the pathological personality of corporations, focussing on specific features of the technologies as the object of the regulation could lead corporations to simply find a new way to generate and process the data. As long as it is profitable, new methods of dataveillance will continue to emerge to replace the current technological methods. This has been illustrated by attempts to regulate corporate dataveillance capability by regulating certain technologies, such as third-party cookies, which have led corporations to adopt alternative technologies, such as fingerprinting, to monitor online behaviour.¹¹³³ A similar scenario may arise,

¹¹³² See Bakan, *The Corporation*, *supra* note 1 at 86. See also Chapter IV, *above*.

¹¹³³ See e.g., Taylor Kay Lively, “The Way the Third-Party Cookie Crumbles: Part 1 EU and UK Developments” (7 December 2021) online (blog): <iapp.org> [http://web.archive.org/web/20230922104837/https://iapp.org/news/a/the-way-the-third-party-cookie-crumbles-part-1-eu-and-uk-developments/]; Taylor Kay Lively, “The Way the Third-Party Cookie Crumble: Part 2 Shifting Industry Practices and Alternatives to Third-Party Cookies” (9 December 2021) online (blog): <iapp.org>

for instance, with regulations on the use of GPS location data, as corporations may switch to using location data collected by Bluetooth or Wi-Fi stations instead of GPS. For this reason, focussing on the specific characteristics of these systems may make the scope too narrow (or too broad) and may also make the regulation quickly outdated.¹¹³⁴

Alternatively, regulation could target the data generated and processed by mass dataveillance systems, focussing on reducing the volume or frequency of data collected about individuals and their behaviour. By limiting the data that corporations can collect and rely on, such regulations would indirectly limit their surveillance capabilities. For example, economist Paul Romer has proposed taxing the revenue generated by targeted digital advertising to reduce the power of corporations with a data-driven business model and to protect the “commons of shared values and norms on which democracy depends.”¹¹³⁵ He argues that such a tax would motivate these corporations to “shift towards a healthier, more conventional business model,”¹¹³⁶ such as charging for subscriptions.

While this approach acknowledges the profit-driven nature of corporations, which motivates them to develop and market data-extracting technologies to increase their profits,¹¹³⁷ it would provide a limited solution. In addition to the well-known challenges posed by corporate tax

[<http://web.archive.org/web/20231218064654/https://iapp.org/news/a/the-way-the-third-party-cookie-crumbles-part-2-shifting-industry-practices-and-alternatives-to-third-party-cookies/>]; Matt Burgess, “The Quiet Way Advertisers Are Tracking Your Browsing”, *Wired* (26 February 2022), online: <wired.com> [<http://web.archive.org/web/20220328060058/https://www.wired.com/story/browser-fingerprinting-tracking-explained/>].

¹¹³⁴ See Bennett Moses, “Recurring Dilemmas”, *supra* note 156 at 265.

¹¹³⁵ Paul Romer, “A Tax That Could Fix Big Tech”, *The New York Times* (6 May 2019), online: <nytimes.com> [<http://web.archive.org/web/20241010054039/https://www.nytimes.com/2019/05/06/opinion/tax-facebook-google.html>].

¹¹³⁶ Romer, *supra* note 1135. See also “Capitalism’t: Why We Should Tax Digital Advertising” (11 March 2021) online (podcast): <chicagobooth.edu> [<http://web.archive.org/web/20240805064608/https://www.chicagobooth.edu/review/capitalisnt-why-we-should-tax-digital-advertising>].

¹¹³⁷ See Chapter IV-III, *above*.

evasion practices,¹¹³⁸ given the pathological nature of corporations, corporations that currently rely on ad targeting and have the necessary infrastructure to collect and process data about individuals and their behaviours will conduct a cost-benefit analysis to determine the profitability of staying in the ad targeting business, repurposing the data to provide services not covered by the tax, or selling the data to other third parties, such as insurance corporations, banks, or government agencies. It would therefore not limit the ability of corporations to engage in mass dataveillance, and could even create new markets (or expand existing ones) for the profitability of data about individuals and their behaviours.

Therefore, this thesis argues for a more fundamental regulatory approach that addresses the structural nature of corporations.

The regulation of corporations can be divided into internal and external regulation.¹¹³⁹ Internal regulation, which refers to corporate law and relates to the governance rules of the corporations, such as the internal structures of the corporations and the establishment of legal obligations such as fiduciary duties of care and loyalty, has been used primarily to protect shareholders.¹¹⁴⁰ External regulation, which refers to regulation that imposes external pressure on corporations to address the harms and risks that corporations create for other stakeholders, has

¹¹³⁸ See e.g., Nick Hopkins, “Why We Are Shining a Light on the World of Tax Havens Again”, *The Guardian* (5 November 2017), online: <theguardian.com> [http://web.archive.org/web/20240415074926/https://www.theguardian.com/news/2017/nov/05/why-shining-light-world-tax-havens-again-paradise-papers]; James Temperton, “Apple Ordered to Pay €13bn in Back Taxes over ‘Illegal’ Deal in Ireland” *Wired* (30 August 2016), online: <wired.com> [http://web.archive.org/web/20240814024236/https://www.wired.com/story/apple-tax-european-commission-ireland-amount/] [http://web.archive.org/web/20240814024236/https://www.wired.com/story/apple-tax-european-commission-ireland-amount/]; Felix Hugger et al, *The Global Minimum Tax and the Taxation of MNE Profit*, OECD Taxation Working Papers, No 68 (Paris: OECD Publishing, 2024); Jonathan Chew, “7 Corporate Giants Accused of Evading Billions in Taxes”, *Fortune* (11 March 2016), online: <fortune.com> [http://web.archive.org/web/20240722162813/https://fortune.com/2016/03/11/apple-google-taxes-eu/]. >.

¹¹³⁹ See e.g., Kent Greenfield, “Proposition: Saving the World with Corporate Law” (2008) 57:4 *Emory Law Journal* 947 at 960.

¹¹⁴⁰ See e.g., Greenfield, “Proposition”, *supra* note 1139.

been used primarily to protect the wider public.¹¹⁴¹ For instance, environmental regulation has been used to control the environmental externalities of corporations, tax law has been used as a means of ensuring the redistribution of wealth, labour law has been used to ensure a fair relationship between employees and corporations, competition law has been used to maintain a competitive market,¹¹⁴² and data protection has been used to protect individuals from the risks and harms created by the data practices of corporations.¹¹⁴³

For most of the history of the corporation, states have relied on external regulation to regulate the power of corporations and the risks and harms that their activities create, rather than requiring changes within the corporation itself.¹¹⁴⁴ This approach has been criticized by some scholars who argue that in order to control the power of corporations, and to protect society from the harms and risks created by their activities, it is necessary to use the internal regulations of corporate law to change certain aspects of the institutional nature of corporations.¹¹⁴⁵

For instance, Barnali Choudhury argues that the root cause of many of the corporate human rights abuses is the way in which corporations operate, which is facilitated by corporate law.¹¹⁴⁶ She argues that the combination of limited liability and a separate legal personality with a corporate purpose that prioritizes shareholders in the governance of the corporation increases the power of

¹¹⁴¹ See e.g., Greenfield, “Proposition”, *supra* note 1139.

¹¹⁴² See e.g., Edward B Rock, “For Whom Is the Corporation Managed in 2020? The Debate over Corporate Purpose Essays” (2020) 76:2 Bus Law 363 at 368.

¹¹⁴³ See Chapter V-I, *above*.

¹¹⁴⁴ For a debate on the role of corporate law to protect society from harm and risk created by corporations see D Gordon Smith, “Response: The Dystopian Potential of Corporate Law” (2008) 57:4 Emory Law Journal 985; Greenfield, “Proposition”, *supra* note 1139.

¹¹⁴⁵ See e.g., Christopher M Bruner & Beate Sjøfjell, “Corporate Law, Corporate Governance and the Pursuit of Sustainability” in Beate Sjøfjell & Christopher M Bruner, eds, *The Cambridge Handbook of Corporate Law, Corporate Governance and Sustainability* (Cambridge: Cambridge University Press, 2019) 713 at 714; Barnali Choudhury, “Corporate Law’s Threat to Human Rights: Why Human Rights Due Diligence Might Not Be Enough” (2023) 8:2 Business and Human Rights Journal 180 at 185; Greenfield, “Proposition”, *supra* note 1139 at 960.

¹¹⁴⁶ See Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 180–81.

corporations and encourages increased risk-taking and a move away from protection of human rights.¹¹⁴⁷ She argues that it is therefore necessary for states to reform corporate law by limiting limited liability, at least in the case where corporations operate as a group corporation,¹¹⁴⁸ and by refocusing corporate purpose by broadening the duties and governance priorities of corporations beyond shareholders.¹¹⁴⁹

Similarly, Beate Sjøfjell argues that a major problem in the debate on how to regulate corporations to improve their social impact is that corporate law has been excluded from the discussion.¹¹⁵⁰ She argues that at the heart of the problem of ensuring corporate respect for human rights and creating of sustainable businesses is the failure of corporate law to specify (or say anything) about the purpose of the corporation and the related concept of the corporation's interests.¹¹⁵¹ This silence, she argues, has left room for a "law-and-economic inspired social norm of shareholder primacy."¹¹⁵² Therefore, she argues that the key to challenging shareholder primacy is to reform corporate law to clearly define the purpose and duty of the corporation.¹¹⁵³

In line with these critiques, this thesis argues for a shift in regulatory focus from external pressures, such as data protection, to internal reforms within corporate law, aimed at addressing the structural factors that contribute to the pathological personality of corporations.

¹¹⁴⁷ See Choudhury, "Corporate Law's Threat to Human Rights", *supra* note 1145 at 185–89. See also Deva, "Alternative Approaches to Transnational Regulation", *supra* note 1090 at 148.

¹¹⁴⁸ See Choudhury, "Corporate Law's Threat to Human Rights", *supra* note 1145 at 190–91.

¹¹⁴⁹ See Choudhury, "Corporate Law's Threat to Human Rights", *supra* note 1145 at 191–96.

¹¹⁵⁰ See Sjøfjell, "How Company Law Has Failed Human Rights", *supra* note 1101 at 182.

¹¹⁵¹ See Sjøfjell, "How Company Law Has Failed Human Rights", *supra* note 1101 at 182–83.

¹¹⁵² See Sjøfjell, "How Company Law Has Failed Human Rights", *supra* note 1101 at 183.

¹¹⁵³ See Sjøfjell, "How Company Law Has Failed Human Rights", *supra* note 1101 at 189.

3) Regulatory Subject

In order to define the particular regulatory subject of the proposed framework, Zuboff's distinction between capitalist corporations and surveillance capitalist corporations is particularly important.¹¹⁵⁴ As explained above, both types of corporations develop or use technologies to collect and use data necessary to provide their services. However, they differ in how they decide to use the metadata generated by interactions with these technologies. This is what Zuboff calls "behavioural data."¹¹⁵⁵

In traditional capitalist models, corporations generate and use only the behavioural data necessary to improve their services or products. In contrast, surveillance capitalism operates on a different principle, as Zuboff explains. Here, corporations rely on collecting and processing of additional metadata beyond what is necessary to improve services—what Zuboff calls "behavioural surplus."¹¹⁵⁶

The operation of surveillance capitalist business models depends on the continuous accumulation and processing of this behavioural surplus, which is then used beyond the scope of service improvement. Profits in this model are generated by using behavioural surplus to accurately predict the future feelings, thoughts, and actions of individuals.¹¹⁵⁷ This harvesting of behavioural surplus is characterized by the routine collection and storage of data about individuals and their behaviours, and the organization of that data to support decision-making processes about those individuals.¹¹⁵⁸ It is this business model and its profitability that has incentivized the

¹¹⁵⁴ This is discussed in detail in Chapter IV-III-B, *above*

¹¹⁵⁵ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 137.

¹¹⁵⁶ See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170.

¹¹⁵⁷ This is discussed in detail in Chapter IV-III-B, *above*

¹¹⁵⁸ This is in line with the definition provided by Rule about the systems of mass surveillance. See Rule, *Privacy in Peril*, *supra* note 8 at 14.

development and deployment of mass dataveillance systems, which the proposed framework seeks to restrict.

Therefore, the regulatory subject of the proposed framework can be defined as any corporation that facilitates or engages in mass dataveillance as part of its business model. That is, any corporation that derives revenue from the sale of technologies, products, or services that either facilitate, are based on, or are informed or improved by the collection or processing of behavioural data surpluses.

This regulatory subject is justified for two main reasons. First, corporations that facilitate mass dataveillance by developing and selling technologies that facilitate the collection and processing of behavioural data surpluses have the power to prioritize certain values in the design of these technologies. By regulating the inherent pathological personality of these corporations and their business models, the framework aims to limit not only their mass dataveillance capabilities, but also the availability of such technologies to other corporations. This approach recognizes that these corporations wield significant power in shaping the norms around these data practices, by designing technologies with sensors or code with the specific purpose of enabling the collection and processing of behavioural data surpluses.

Second, even corporations that do not directly control the design of these dataveillance technologies exert significant influence by choosing to base their business model, in whole or in part, on the mass collection and processing of behavioural data surpluses. This strategic choice drives demand for these technologies and perpetuates the broader ecosystem of mass dataveillance. By basing their profit models on the collection and processing of these behavioural data surpluses, these corporations are normalizing the use of such practices in society, regardless of whether such data are necessary for the product or service they offer.

The proposed regulatory framework, therefore, seeks to address the issue of mass dataveillance capabilities of corporations by targeting both the developers of the technologies that enable corporate mass dataveillance and the corporations that choose to rely on these practices. Through this dual approach, the proposed regulation aims to mitigate the privacy risks posed by the systematic and continuous monitoring of individuals.

II. Limiting Corporate Dataveillance: Essential Features

Building on regulatory rationales, goals, and targets discussed in the previous part, this part will focus on developing key features of the proposed regulatory framework. The proposed regulatory framework has a two-part approach: first, the redefinition of corporate purpose and the introduction of a duty to limit revenue streams, coupled with mandatory dissolution for non-compliance. These two components challenge the traditional view of corporations and corporate law.¹¹⁵⁹

The first component of the framework challenges traditional corporate law by redefining corporate purpose and introducing a duty to limit revenue streams. The framework aims to limit the pathological tendencies of corporations by placing clear limits on how they can generate revenue. It directly challenges the profit maximization rule (or shareholder primacy¹¹⁶⁰), by requiring corporations to ensure that their revenues do not come from certain technological capabilities, even if this results in additional costs or reduced revenues.

¹¹⁵⁹ This is the view of corporations as primarily concerned with the creation of profit for the benefit of shareholders, and of corporate law as primarily concerned with protecting shareholders. See e.g., Greenfield, “Proposition”, *supra* note 1139 at 960.

¹¹⁶⁰ See Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101.

The second component of the framework introduces a mandatory dissolution for non-compliance. This measure embodies the idea that if and when corporations choose to disobey the law and become a danger to society, the government that granted them the right to do business has the power to revoke that right. This approach goes beyond traditional penalties, which corporations see as part of the cost of doing business, and instead introduces a genuine existential threat for non-compliance.

These recommendations should be seen as part of a wider reform of corporate law, which will require corresponding changes to the duties of corporations. The framework aims to dismantle the business model of surveillance capitalism, impacting on the profits of corporations that rely on a surplus of behavioural data.

This part is divided into three sections. The first two sections elaborate on these two key components of the framework and provide a model text for the proposed regulation. The final section explores some of the possible criticisms and limitations of the proposed framework, focussing on how the proposed regulation may affect different types of innovation, the logistical challenges it poses for regulators, and the broader systemic and political factors that may limit its effectiveness.

A. Regulating Self-Interest, Corporate Purpose, and Limiting How Corporations Can Pursue Their Purpose

One aspect of the legal structure of the corporation that has contributed to its pathological personality is the construction of the corporation's purpose as solely focussed on the generation of profit, and the corresponding duty to ensure that the corporation's actions are directed towards the generation of profit at all costs.¹¹⁶¹ This mandate renders the corporation "*singularly* self-interested

¹¹⁶¹ See Bakan, *The Corporation*, *supra* note 1 at 35–9.

and unable to feel genuine concerns for others” because it requires it to put its own interests ahead of the rights and interests of other stakeholders, such as consumers, workers, or the communities directly affected by the corporation’s actions.¹¹⁶² Moreover, because nothing in the legal structure of the corporation limits how it can pursue this purpose,¹¹⁶³ this self-interest has led to the development of other psychopathic traits such as lack of empathy, superficial relationships with others, and manipulative behaviour.¹¹⁶⁴

To counter this self-interest, some scholars have suggested that the purpose of the corporation and the scope of the corporate duties should be broadened beyond shareholders,¹¹⁶⁵ so that the corporation would have to consider issues beyond financial and profit concerns, such as human rights and environmental sustainability.¹¹⁶⁶ Drawing on the contributions of these scholars, this section develops two of the elements necessary to constrain the pathological personality of corporations in order to limit their capacity for mass dataveillance. First, the new regulatory framework must include a reform of the institutional character that creates the self-interested quest of corporations; this is the corporate purpose. Second, this change in purpose must be accompanied by a specific limitation on this self-interested pursuit, by establishing a specific corporate duty to limit the ways in which corporations can fulfill their pursuit of profit.

¹¹⁶² See Bakan, *The Corporation*, *supra* note 1 at 56.

See also Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1142 at 188.

¹¹⁶³ See Bakan, *The Corporation*, *supra* note 1 at 60–69.

¹¹⁶⁴ See e.g., Bakan, *The Corporation*, *supra* note 1 at 56.

¹¹⁶⁵ These will be developed in detail in the Section A.1, *below*.

¹¹⁶⁶ For a comparative law study of the different approach to the director’s duty and the interest of the company see Beate Sjøfjell et al, “Shareholder Primacy: The Main Barrier to Sustainable Companies” in Beate Sjøfjell & Benjamin J Richardson, eds, *Company Law and Sustainability: Legal Barriers and Opportunities* (Cambridge, UK: Cambridge University Press, 2015) 79; European Commission, *Study on Directors’ Duties and Sustainable Corporate Governance: Final Report* (Luxembourg: Publications Office of the European Union, 2020) at annex I and II; Robert McCorquodale & Stuart Neely, “Directors Duties and Human Rights Impacts: A Comparative Approach” (2022) 22:2 *Journal of Corporate Law Studies* 605.

1) Corporate Purpose: Broadening the Scope Beyond Self-Interested Profit Generation

The first element of the proposed framework is to reform the corporate purpose as the legal structure that fosters the self-interest motivation of the pathological corporation.¹¹⁶⁷ It is important to distinguish between two concepts: the corporate purpose that corporations set for themselves and the corporate purpose that is set by the law, i.e., the purpose for which the law allows corporations to be set up as legal entities.

An example of the former—the corporate purpose—is the 2019 public statement by the CEOs of major American corporations announcing that shareholder value is no longer the primary goal of the corporation, but that the corporation also has a fundamental commitment to all its stakeholders.¹¹⁶⁸ As explained earlier, this statement is an example of the “good corporation” movement,¹¹⁶⁹ which did not represent a fundamental change in the profit-driven nature of corporations, but instead provided them with an opportunity to create a positive public image.¹¹⁷⁰

The latter concept of the legal basis of a corporate purpose is the focus here. Traditionally, the main purpose of a corporation has been narrowly defined as the generation of profit for shareholders at all costs, also known as the shareholder wealth maximization rule.¹¹⁷¹ Even in jurisdictions where there is no specific legal mandate to prioritize the interests of shareholders—

¹¹⁶⁷ See e.g., Bakan, *The Corporation*, *supra* note 1 at 180. (He argues that to reform the corporation meaningfully, the legal mandate to pursue its own self-interest must be revised. This revision should focus on restructuring corporations to serve and be accountable to a broader spectrum of society, rather than exclusively prioritising the interests of shareholders and corporations themselves.)

¹¹⁶⁸ Business Roundtable, “Redefinition of Corporations”, *supra* note 482. See also Bakan & Abbott, “New Corporation Documentary”, *supra* note 166 at 6:13; Fitzgerald, “CEOs Said Shareholder Value is No Longer Their Main Objective”, *supra* note 482.

¹¹⁶⁹ See Bakan, *New Corporation*, *supra* note 5 at 57.

¹¹⁷⁰ See Chapter IV-I, *above*.

¹¹⁷¹ See e.g., Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 c 3.

i.e., the interests of profit generation—the shareholder prioritization is often the rule.¹¹⁷² Sjøfjell, for example, distinguishes between “shareholder primacy” as a market norm and the legal norm of “shareholder value” in UK corporate law. She argues that even in jurisdictions where corporate law does not require the maximization of shareholder wealth, various relevant actors in these jurisdictions increasingly assume that shareholder interests are paramount in corporate decision making.¹¹⁷³ Therefore, even if corporate law does not directly mandate profit generation at all costs as the corporation’s sole purpose, its silence on the corporation’s specific purpose may also contribute to their pathological personality, as the absence of a mandatory legal purpose enables corporations to pursue self-interested purposes.

This self-interested purpose has been challenged by scholars and policymakers. They argue that this narrow focus can have detrimental effects on both the economy and society, highlighting the need for a redefinition of corporate purpose.¹¹⁷⁴ As a result, there have been proposals to modify this corporate purpose.

According to Barnali Choudhury and Martin Petrin, alternative perspectives on corporate purpose, such as stakeholderism or pluralist models, tend to reach three conclusions.¹¹⁷⁵ First, corporations need to consider the interests of a wider range of non-shareholder stakeholders. Second, wealth maximization should not be the sole guiding principle in corporate decision-making. Third, corporate decision-making should balance the interests of all stakeholders, including shareholders. Importantly, this means that where there is a conflict between shareholder

¹¹⁷² See e.g., Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815.

¹¹⁷³ See Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 183; Bruner & Sjøfjell, “The Pursuit of Sustainability”, *supra* note 1145 at 715–16. See also Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 183.

¹¹⁷⁴ See e.g., Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 c 3; OECD, *Guidelines for Multinational Enterprises*, *supra* note 1032 at 19.

¹¹⁷⁵ See Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 43.

and non-shareholder interests, the latter should not automatically prevail. They also emphasize, however, that these theories do not provide a definitive answer as to how the conflict of interests should be resolved.¹¹⁷⁶

Building on these considerations, Choudhury and Petrin argue that a redefined general corporate purpose should contribute to the accountability of corporations for their impact on society.¹¹⁷⁷ They argue that a redefined purpose must broaden its focus to include non-shareholder interests and ensure that these interests are given equal weight with shareholder interests.¹¹⁷⁸ Within this framework, they argue, corporate governance mechanisms should seek to balance and, where possible, benefit the full range of corporate stakeholders.¹¹⁷⁹

Similarly, in the area of sustainability, some authors have argued for the need to redefine the overarching purpose of corporations within corporate law, regardless of their sector or industry.¹¹⁸⁰ For example, Sjøfjell, emphasizing the interconnectedness of the protection of human rights and the achievement of sustainability,¹¹⁸¹ suggests that the overarching purpose of corporations should be to create “sustainable value within planetary boundaries respecting the interest of its investors and other involved and affecting parties.”¹¹⁸² Within this overarching purpose, the articles of incorporation could set out a more detailed set of purposes tailored to the particular activities of the corporation.¹¹⁸³

¹¹⁷⁶ See Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815.

¹¹⁷⁷ See Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 58.

¹¹⁷⁸ See Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 59.

¹¹⁷⁹ See Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 83.

¹¹⁸⁰ See e.g., Beate Sjøfjell et al., “Securing the Future of European Business: SMART Reform Proposals” University of Oslo, Research Paper Series No. 2020-11.

¹¹⁸¹ See Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 199.

¹¹⁸² See Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 196. See also Sjøfjell et al., “SMART Reform Proposals”, *supra* note 1180 at 61.

¹¹⁸³ See Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 196.

These proposals have a common goal: to balance the interests of different stakeholders without eliminating the shareholders' interest in making a profit or the role of the corporation as an instrument for making a profit. They propose to make clear that shareholders' economic interests should not take precedence over other stakeholder interests, but should be balanced with other stakeholder interests to achieve specific objectives, such as creating sustainable value within planetary boundaries,¹¹⁸⁴ or to contributing to corporations' responsibility for their social impacts.¹¹⁸⁵

Given that the regulatory framework proposed in this thesis is framed as a reform of corporate law, it is essential that the new corporate purpose is broad enough to apply to corporations in different industries or sectors. Based on the proposals outlined above, the new framework should make the following purpose explicit:

The purpose of corporations is to create value for the benefit of all stakeholders, including shareholders, employees, customers, and communities. In fulfilling this purpose, corporations have a positive duty to adhere to international human rights in all their activities. Corporations must balance the pursuit of profit with their responsibilities to society by ensuring that all aspects of their business model contribute positively to the well-being of all stakeholders.

This purpose would serve as the basis for a broader reform of corporate law aimed at addressing and limiting the pathological features of corporate behaviour. Moreover, such a reform is consistent with the state's duty to protect against business-related human rights abuses by enacting and enforcing regulations that promote respect for human rights.¹¹⁸⁶ As part of this duty, states must ensure that their policies and regulations consistently place respect for human rights at

¹¹⁸⁴ See Sjäfjell et al, "SMART Reform Proposals", *supra* note 1180 at 61. See also Sjäfjell, "How Company Law Has Failed Human Rights", *supra* note 1101 at 196.

¹¹⁸⁵ See Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 58.

¹¹⁸⁶ See SRSRG, *UNGPs*, *supra* note 1024 at principles 1-3.

the heart of the digital economy.¹¹⁸⁷ Therefore, by embedding respect for human rights in the core purpose of corporations, this reform not only addresses some aspects of the pathological behaviour of corporations, but also strengthens the alignment between corporate practices and state regulatory obligations, ensuring that human rights remain a central priority in the evolving digital economy.

As noted above, corporate behaviour is constrained by internal and external regulation.¹¹⁸⁸ The proposed purpose seeks to impose an internal constraint on corporate behaviour, embedding the requirement to consider the wider societal impact of their actions into the very DNA of corporations, and part of the fundamental reason for their legal existence. It seeks to move beyond the traditional focus on maximizing shareholder returns and instead promote a balance between profit generation and responsibility to society. This shift represents an important step in mitigating the pathological personality of corporations by establishing a first layer of restraint.

This reframing of corporate purpose positions international human rights not as a “basic expectation [that] society has of business,”¹¹⁸⁹ but as an essential and non-negotiable component of corporate existence. It could also be seen as the next evolutionary step in the implementation of the UN Guiding Principles on Business and Human Rights (UNGPs). By embedding international human rights obligations within the internal structure of the corporation, these principles become part of the institutional nature of the corporation, transforming human rights from a moral

¹¹⁸⁷ See B-Tech, *Bridging Governance Gaps in the Age of Technology: Key Characteristics of the State Duty to Protect*, OHCHR (2021) B-Tech Foundational Paper online: <ohchr.org> [<http://web.archive.org/web/20240722004358/https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf>] at 6.

¹¹⁸⁸ See Part I-A.2, *above*

¹¹⁸⁹ SRSG, *Policy Framework*, *supra* note 1023 at para 9.

responsibility that corporations should strive to respect into a structural constraint that mitigates the pathological tendencies of corporate behaviour.

Creating value for all stakeholders through respect for international human rights must be an integral part of all aspects of a corporation's business model. This includes decisions about revenue generation through the development and design of technologies, the integration of specific technologies into their business operations, and the use of data. Businesses must carefully consider whether their technological developments are consistent with their obligations to create value for all stakeholders by respecting international human rights, rather than simply pursuing profit or efficiency gains at the expense of fundamental rights.

However, broadening the corporate purpose will not be enough to limit the pathological personality of corporations. This broader purpose must be backed up by specific, enforceable duties.¹¹⁹⁰ Furthermore, given that the regulatory goal of the new framework is focussed on addressing a specific profit-driven, privacy-invasive practice, the proposed framework must also introduce a specific duty aimed at limiting the revenue streams derived from such practices, as the following sections will explain.

2) Corporate Duties: Limiting How Corporations Can Generate Profit

The broader corporate purpose proposed in the previous section will also need to be operationalized through specific corporate duties to ensure that it translates into actionable obligations. Various proposals have emerged to extend corporate duties to include the interests of non-shareholder stakeholders and to introduce a specific duty to protect human rights. As

¹¹⁹⁰ See e.g., Sjäfjell et al, "SMART Reform Proposals", *supra* note 1180 at 59; Sjäfjell, "How Company Law Has Failed Human Rights", *supra* note 1101 at 196. They propose formulating a duty to ensure that the company fulfils its overarching purpose, respecting the interest of its members, other investors, and other involved and affected parties.

discussed below, these proposals have their own merits; however, they alone are not sufficient to limit the pathological personality of corporations, and as such may have a limited effect in limiting corporate mass dataveillance, because they fail to impose restrictions on the characteristics that give corporations their pathological personality.

There are two groups of proposals that are of interests for this thesis. The first group of proposals suggests that the law could impose a duty to consider specific stakeholder interests (e.g., employees)¹¹⁹¹ or to balance the interests of different stakeholders.¹¹⁹² This approach would require directors to explicitly consider the impact of their decisions on different stakeholder groups, potentially leading to more holistic decision making. Within this group, one of the most cited and discussed examples of legislative broadening of corporate duties is the so-called enlightened shareholder value provision in Section 172 (2) of the UK Companies Act of 2006.¹¹⁹³ This statutory provision introduced a “duty to consider” non-shareholder interests.¹¹⁹⁴ This provision has been criticized because the “duty to consider” is an easy standard to meet,¹¹⁹⁵ and

¹¹⁹¹ This is the case in jurisdictions where employees are part of the board (e.g., Germany) and where the regulation specifically includes employees, such as the Canadian law. See *Canada Business Corporations Act*, RSC 1985, c C-44 [CBCA] art s 122 (1.1)(a).

¹¹⁹² See European Commission, *Study on Directors’ Duties*, *supra* note 1166.

¹¹⁹³ See e.g., Sjøffjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 187; Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 187; McCorquodale & Neely, “Directors Duties and Human Rights Impacts”, *supra* note 1166 at 610; Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 c 3.

¹¹⁹⁴ See *Companies Act 2006*, (UK) [UK Companies Act].

See also Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 47.

¹¹⁹⁵ According to the explanatory notes, to comply with this duty, “it will not be sufficient to pay lip service to the factors.” Furthermore, under Section 414CZA of the UK Company Act, companies have a responsibility to report how they have considered the interests of other stakeholders. However, it does not establish the minimum requirements for the manner in which directors should consider those interests.

See Department of Trade and Industry, “Explanatory Notes to Companies Act 2006” (last visited 18 August 2024) online: <legislation.gov.uk> [<http://web.archive.org/web/20240422131159/https://www.legislation.gov.uk/ukpga/2006/46/notes/division/6/2>] at s 328.

that it does not, in the end, abandon the corporate purpose of profit generation above all else.¹¹⁹⁶ These criticisms could be addressed by setting out the minimum requirements that directors must consider, and by linking this duty to a broader corporate purpose, as the one suggested in the previous section.

The second group of proposals is to impose specific duties to protect human rights. For instance, Choudhury suggests that corporate law could impose a duty on directors “to identify, prevent, and mitigate human rights and other related harms.”¹¹⁹⁷ Choudhury argues that this duty could have an impact on corporate governance that could further prevent human rights or environmental harms.¹¹⁹⁸ Similarly, some states are enacting, or proposing to enact, various forms of mandatory human rights due diligence laws as an attempt to integrate societal concerns into corporate decision-making.¹¹⁹⁹ A frequently cited example is the French Duty of Vigilance Law of 2017,¹²⁰⁰ which amended the French corporate law (*Code de Commerce*¹²⁰¹) to impose a duty

See also Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 192–93; Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 48; McCorquodale & Neely, “Directors Duties and Human Rights Impacts”, *supra* note 1166 at 618–20.

¹¹⁹⁶ Under section 172(1) of the UK Company Act directors must act to promote the success of the company for the benefit of its members as a whole, that is the shareholders. By establishing that the decision-making must be for the benefit of its members as a whole, it did not change the outcome in the cases of conflict between stakeholder interests, and profit generation. As long as the directors consider in good faith other interests, they may still decide not to take them into account if that will result into a most advantageous result for shareholders.

See Department of Trade and Industry, “Notes UK Companies Act”, *supra* note 1195 at s 328.

See also Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 192–93; Choudhury & Petrin, *Corporate Duties to the Public*, *supra* note 815 at 48; Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 187.

¹¹⁹⁷ Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 195.

¹¹⁹⁸ See Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145 at 194.

¹¹⁹⁹ See Sjøfjell, “How Company Law Has Failed Human Rights”, *supra* note 1101 at 181.

¹²⁰⁰ *Loi n° 2017-399 du 27 mars 2017*, JO, 28 March 2017, no 0074 [*French Duty of Vigilance Law*].

See e.g., Bruner & Sjøfjell, “The Pursuit of Sustainability”, *supra* note 1145 at 719; McCorquodale & Neely, “Directors Duties and Human Rights Impacts”, *supra* note 1166 at 620.

¹²⁰¹ *Code de commerce* [C com France] at livre II.

of diligence on large French corporations. The law requires corporations to publish an annual “vigilance plan” detailing reasonable measures to identify risks and prevent serious human rights abuses within their groups and supply chains worldwide.¹²⁰² Critics argue that many corporations treat the vigilance plan as a mere tick-box exercise that lacks real transparency and stakeholder engagement, and thus fails to drive meaningful change in corporate behaviour.¹²⁰³

Both of these approaches—the duty to consider non-shareholder interests, and the duty to prevent and protect human rights—offer possible ways of operationalizing the proposed corporate purpose. For instance, the duty to consider non-shareholder interests could serve as a specific duty, creating an enforceable obligation to “balance the pursuit of profit with their responsibilities to society by ensuring that all aspects of their business model contribute positively to the well-being of all stakeholders.”¹²⁰⁴ This duty would ensure that directors explicitly consider how all aspects of their business model contribute to the well-being of stakeholders, potentially promoting more ethically informed decision-making.

Similarly, a duty to identify, prevent, and protect human rights, and to demonstrate reasonable steps taken to comply with this duty, could give effect to the broader corporate purpose to “adhere to international human rights in all their activities.”¹²⁰⁵ This duty could provide a legal

¹²⁰² *French Duty of Vigilance Law*, *supra* note 1200 at art 1.

See Business & Human Rights Resource Centre, “France’s Duty of Vigilance Law” (last visited 19 August 2024) online: <business-humanrights.org> [<http://web.archive.org/web/20240921145006/https://www.business-humanrights.org/en/big-issues/corporate-legal-accountability/frances-duty-of-vigilance-law/>].

¹²⁰³ See Elsa Savourey & Stéphane Brabant, “The French Law on the Duty of Vigilance: Theoretical and Practical Challenges Since its Adoption” (2021) 6:1 Business and Human Rights Journal 141 at 147.

See also Deva & Kaur, “From ‘Tokenism’ to ‘Centring’ Rights and Rights-Holders”, *supra* note 1034; Choudhury, “Corporate Law’s Threat to Human Rights”, *supra* note 1145.

¹²⁰⁴ See the text accompanying note 1182, *above*, for the proposed corporate duty.

¹²⁰⁵ See the text accompanying note 1182, *above*, for the proposed corporate duty.

basis for a corporate purpose focussed on human rights considerations and more conscientious business practices.

However, these proposals alone will not be enough to curb the pathological tendencies of corporations and to limit their dataveillance capabilities. While these duty proposals help to shift the focus of corporations away from purely profit-driven motives, and they encourage consideration of societal and human rights concerns, they do not impose adequate constraints on the way in which corporations can pursue profit. This is important because without clear constraints on profit-seeking behaviour, corporations are likely to continue to prioritize their financial goals at the expense of their human rights and social responsibilities. Limiting the way in which corporations can pursue profit is necessary to address the root causes of their pathological personality, as the unrestricted pursuit of financial gain incentivizes harmful behaviours, such as dataveillance.

As noted earlier,¹²⁰⁶ one of the legal structures that has contributed to the pathological personality of corporations can be described as the combination of three elements: a corporate purpose focussed solely on making a profit,¹²⁰⁷ a duty that compels directors to prioritize profit maximization,¹²⁰⁸ and an internal legal structure that imposes few, if any, restrictions on how that purpose is pursued.¹²⁰⁹

The broader corporate purpose proposed in the previous section addresses the first element by broadening the corporate purpose from profit generation alone to value creation for the benefit of all stakeholders, with an explicit commitment to international human rights. The two sets of

¹²⁰⁶ See the text accompanying note 1158, *above*.

¹²⁰⁷ See Bakan, *The Corporation*, *supra* note 1 at 35–9.

¹²⁰⁸ See Bakan, *The Corporation*, *supra* note 1.

¹²⁰⁹ See Bakan, *The Corporation*, *supra* note 1 at 60–69.

duties described—the interests of stakeholders and the prevention and protection of human rights—could serve to partially address the second element by requiring that corporate actions go beyond profit motives and extend to the interests of other groups, including employees and communities.

However, these proposals do not go far enough to set clear limits on how corporations can pursue profit, which is crucial to addressing the third element that underlies corporate pathology. In particular, these proposals do not prevent corporations from engaging in practices that conflict with societal and ethical concerns in the pursuit of financial goals. Therefore, in order to achieve the regulatory objectives of the proposed framework, and to limit the pathological tendencies of corporations, the duty imposed on corporations should impose strict limits on how corporations can achieve profitability.

(a) Duty to Limit Revenue Streams

In defining the new duty, it is important to recognize that certain technological capabilities that underpin corporate mass dataveillance systems also provide significant value to individuals and society. For example, digital technologies that make it easier to communicate, search for information, share photos, videos, and documents, and locate people in a particular place at a particular time have improved reporting on human rights abuses around the world.¹²¹⁰ Similarly,

¹²¹⁰ See e.g., Richard Pendry, “New Technology, War, and Human Rights Reporting” in Stephen J A Ward, ed, *Handbook of Global Media Ethics* (Cham: Springer, 2021) 1031; Alice Kohli, “Data-Driven Human Rights Investigations” in Oliver Hahn & Florian Stalph, eds, *Digital Investigative Journalism: Data, Visual Analytics and Innovative Methodologies in International Reporting* (Cham: Springer International Publishing, 2018) 67; OHCHR, “Using Social Media to Promote Human Rights” (10 August 2011) online: <ohchr.org> [<http://web.archive.org/web/20240127170700/https://www.ohchr.org/en/stories/2011/08/using-social-media-promote-human-rights>].

location technologies have been instrumental in locating people during natural disasters, and helping rescuers and humanitarians target and deliver aid more effectively.¹²¹¹

The framework must therefore strike a balance between the beneficial use of technology and the regulation of invasive data practices. One way of doing this is to regulate the types of business models that rely on the collection and processing of behavioural data surpluses, as it is the profitability of these data that incentivizes the development and deployment of mass dataveillance systems.¹²¹² As an illustration, it is possible to identify three types of business model among the corporations that will be most affected by this framework. These business models are not mutually exclusive, as some corporations may generate revenue from more than one model.¹²¹³

In the first business model, corporations generate revenue by selling technology that facilitates the collection and processing of behavioural data surpluses. This is part of the business model of corporations that sell on-premise data analytic software, such as Palantir Inc.,¹²¹⁴ or hardware with sensors and connectivity capabilities, such as Amazon Inc.¹²¹⁵ Increasingly, it is also part of the business model of emerging players in the data economy, such as car manufacturers, who are increasingly building technological capabilities into their vehicles to collect and process data about their occupants.¹²¹⁶

¹²¹¹ See e.g., P Gregg Greenough & Erica L Nelson, “Beyond Mapping: A Case for Geospatial Analytics in Humanitarian Health” (2019) 13:1 Conflict and Health 50; Emily Aiken et al, “Machine Learning and Phone Data Can Improve Targeting of Humanitarian Aid” (2022) 603:7903 Nature 864.

¹²¹² See Chapter IV-III, *above*.

¹²¹³ See Table 2, *below*, for an illustration of this point.

¹²¹⁴ See e.g., Palantir Technologies Inc., *Annual Report 2023 (Form 10-K)*, Commission File Number: 001-39540 (United States Securities and Exchange Commission, 2023) at 93.

¹²¹⁵ See e.g., Amazon.com, Inc., *Annual Report 2023 (Form 10-K)*, Commission File No. 000-22513 (United States Securities and Exchange Commission, 2023) at 43.

¹²¹⁶ An example of this is Stellantis N.V. which is discussed in more detail in Part II-A.2.c, *below*.

See also, Jen Caltrider, Misha Rykov & Zoë MacDonald, “*Privacy Not Included: A Buyer’s Guide for Connected Products” (6 September 2023) online: <foundation.mozilla.org>

In the second business model, corporations generate revenue by **selling services that are based on** the collection and processing of behavioural data surpluses. These services are usually business-to-business (B2B) services, where the buyer is usually not the primary user of the product, but a third party interested in the data for its own products and services. This is part of the business model, for example, of corporations that sell personalized advertising services that are based on the collection and processing of behavioural data surpluses, such as Meta Inc.¹²¹⁷

In the third business model, corporations can generate revenue by **selling products or services that are informed or improved by** the use of technology or services that collect and process behavioural data surpluses. This is part of the business model of some clothing retailers, for example, who rely on third-party data collection and processing software as part of their decision-making process for various aspects of their business, from designing their products to driving customer engagement with targeted promotions.¹²¹⁸

Taking all of the above into account, the proposed framework should establish the following duty to limit revenue streams:

All corporations have a duty to ensure that their revenues do not derive from the sale of technologies, products, or services that either facilitate, are based on, or are informed or improved by the collection or processing of behavioural data surpluses.

[<http://web.archive.org/web/20240605142413/https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/>].

¹²¹⁷ See e.g., Meta Platforms Inc, *Annual Report 2023 (Form 10-K)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2024) at 75.

¹²¹⁸ See e.g., Oracle, “Oracle Retail Data Store Cloud Service” (2024) online (PDF): <[oracle.com](http://www.oracle.com/a/ocom/docs/industries/retail/retail-data-store-ds.pdf)> [<http://web.archive.org/web/20230314055028/https://www.oracle.com/a/ocom/docs/industries/retail/retail-data-store-ds.pdf>]; Michael Hickins, “How Data Analytics Informs the Fashion Industry” (24 February 2023) online: <[oracle.com](http://www.oracle.com/retail/fashion/fashion-analytics/)> [<http://web.archive.org/web/20240817234418/https://www.oracle.com/retail/fashion/fashion-analytics/>]; Brandwatch, “Retail” (last visited 8 October 2024) online: <[brandwatch.com](https://www.brandwatch.com/industries/retail/)> [<http://web.archive.org/web/20240927141356/https://www.brandwatch.com/industries/retail/>].

By placing a limit on how corporations can generate revenue, this duty acts as a limit on their pathological personality. Moreover, this corporate duty directly targets the core problem of surveillance capitalism: the exploitation of behavioural data surpluses for profit.

To comply with this duty, corporations must ensure that the business models for all their services and products do not depend on the collection and processing of behavioural data surpluses. These are the data that are generated as a result of the individuals' interactions with technology, beyond what it is necessary to improve products and services.¹²¹⁹ This could include data from online activities (e.g., browsing history, clicks, and social media interactions), offline activities (e.g., location tracking via mobile devices), and data derived from the use of connected devices (e.g., IoT devices, connected cars).

Under this duty, corporations would be required to avoid business models that rely on monetizing data about individuals and their behaviours collected and process through mass dataveillance practices. This includes, for example, the sale of behavioural data surpluses to third parties, or the use of such data internally to generate revenue from targeted advertising or behavioural manipulation.

This duty will have an impact on existing corporations whose business model is based on the collection and processing of behavioural data surpluses, as shown in Table 1. While this could reduce their profitability in the short term, it could also drive innovation towards technologies, services, and products that do not rely on mass dataveillance to deliver societal benefits to society and a good user experience.

¹²¹⁹ This corresponds to Zuboff's definition of behavioural surplus. See Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 at 137.

See also Part-I.B.3 Regulatory Subject, *above*.

	Current business models	Example of how business models could change under the proposed framework
Business Model 1	They generate revenue by selling technology that facilitates the collection and processing of behavioural data surpluses.	They will not be able to sell technologies that facilitate the collection and processing of behavioural data surpluses. They may continue to sell technology (hardware or software) that is designed to limit the intended use of behavioural data surpluses (e.g., removing sensors that are not needed for customer experience; limiting software access to data that may be used to collect or process behavioural data surpluses). They will not be able to sell technology to corporations that operate under business model 2 or 3 (e.g., cross-referencing client list).
Business Model 2	They generate revenue by selling services that are based on the collection or processing of behavioural data surpluses. Predominantly B2B, the buyer is usually not the primary user of the product, but a third party interested in the data for their own products and services.	They will not be able to sell services that are based on behavioural data surpluses. They may continue to sell services based on the same software, hardware, methods, algorithms, infrastructure that can be applied to non-behavioural data or to behavioural data that is not considered to be surplus (e.g., user/customer experience).
Business Model 3	They generate revenue by selling products or services that are informed or improved by the use of technology or services that collect and process behavioural data surpluses.	They will have to stop relying on the insights provided by behavioural data surpluses and only rely on behavioural data that is inherent in the use of the product or service (e.g., user/customer experience). They will not be able to purchase technology or services from corporations that are deemed to be operating under business models 1 or 2.

Table 1. Examples of how current business models could change under the new framework.

(b) Reporting and Regulatory Review

The proper implementation of the proposed duty would require corporations to report on their business models in a way that allows a public authority to verify their compliance with the duty. This will require them to provide a report outlining their business model.

Currently, corporations provide a general description of their business in their annual reports, but this often lacks detail on how they make their profits, and in particular whether data are a significant source of those profits. For example, Meta Inc.’s business description states: “We report our financial results based on two reportable segments: Family of Apps (FoA) and Reality Labs (RL). [. . .] We generate substantially all of our revenue from advertising.”¹²²⁰ Similarly, Uber Inc. describes its business as:

Uber is a technology platform that uses a massive network, leading technology, operational excellence and product expertise to power movement from point A to point B. Uber develops and operates proprietary technology applications supporting a variety of offerings on its platform.¹²²¹

While these descriptions provide a high-level overview, they lack specifics on the role of data in revenue generation. The proposed framework would require corporations to provide detailed revenue reporting and a clear link between data usage and revenue streams. This reporting requirement could act as a bridge between the information corporations already provide in their privacy notices under data protection rules and the financial information that they disclose in their annual reports under corporate law. The process would not require the creation of entirely new documents, but rather the organization and linking of existing internal documents.

¹²²⁰ Meta Platforms Inc, *Meta 10-K 2023*, *supra* note 1217 at 95.

¹²²¹ Uber Technologies Inc, *Annual Report 2023 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2023) at 82.

(i) Detail Revenue Reporting

Under corporate law, corporations are already required to prepare annual financial statements for presentation to their shareholders¹²²² and for filing with the relevant authorities.¹²²³ These financial statements typically include information on profits, costs, liabilities, equity, and assets.¹²²⁴ However, in their current form, these reports are not sufficient to verify compliance with the proposed duty because they do not distinguish between data-driven activities and other revenue-generating activities.

Given this existing reporting requirement, the new reporting requirement could be incorporated into these financial statements with the added specificity that all corporations would be required to provide a detailed breakdown of all their revenue streams, categorized as follows:

1. Revenue from data-driven activities: For example, advertising revenue based on user profiling, revenue from dynamic pricing algorithms, or targeted recommendations.
2. Revenue from non-data-based activities: For example, subscription services, direct sales of products, or standard fees for services.

This breakdown would provide an initial overview of the business model and serve as a starting point for the regulator to verify compliance.

¹²²² See e.g., *CBCA*, *supra* note 1191 at s 155; EU, *Directive 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) (Text with EEA relevance)*, [2017] OJ, L169/46 [*Directive Regarding Company Law*] at art 14 (f); EU, *Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC Text with EEA relevance*, [2013] OJ, L182/19 [*Directive on Corporate Financial Statements*].

See also US Securities and Exchange Commission, “Annual Report” (last visited 22 May 2024) online: <investor.gov> [<http://web.archive.org/web/20240425153855/https://www.investor.gov/introduction-investing/investing-basics/glossary/annual-report>].

¹²²³ See e.g., *CBCA*, *supra* note 1191 at s 160; *Directive Regarding Company Law*, *supra* note 1222 at art 16.

¹²²⁴ See e.g., *Directive on Corporate Financial Statements*, *supra* note 1222 at annex III.

(ii) Mapping of Data to Revenue Streams

The second part of the report would require corporations to link their revenues to the data they collect and process. Data protection rules already require corporations to provide information about their data practices, including what data are collected, how these are collected (e.g., through user interactions, third-party sources), and for what purposes.¹²²⁵ This information, typically provided in privacy policies, is intended to ensure that users have sufficient information to consent to the processing of their data.¹²²⁶

Under the proposed framework, corporations would be required to provide this information to the regulator, with the added requirement that it be directly linked to their business model. This means that corporations would have to demonstrate a clear link between the data they collect and process and the revenue they generate from that data.

For example, a corporation like Meta Inc. would need to detail how user data collected across its various platforms contributes to its advertising revenue, including the processes involved in user profiling and targeted advertising. Similarly, Uber Inc. would need to show how data from user interactions on its platform—such as ride-hailing or food delivery—is used to generate dynamic pricing models or other data-driven revenue streams.

(c) What This Means for Corporations

As outlined above, the proposed framework would require corporations to provide detailed information in two key areas: a breakdown of revenues into data-based and non-data-based

¹²²⁵ See e.g., *GDPR*, *supra* note 66 at arts 12, 13; *PIPEDA*, *supra* note 66 at sch 1, s 4.2; Office of the Privacy Commissioner of Canada, “PIPEDA Fair Information Principle 3: Consent” (August 2020) online: <priv.gc.ca> [http://web.archive.org/web/20240717225530/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/].

¹²²⁶ See e.g., *GDPR*, *supra* note 66 at recital 61; Office of the Privacy Commissioner of Canada, “Consent”, *supra* note 1225.

categories, and a clear link between the data they collect and process and their revenue streams. To illustrate how this reporting requirement could work in practice, this section analyzes four corporations: Meta Inc, Uber Inc, Stellantis N. V. and H&M Group. These corporations were chosen because they represent different business models that demonstrate varying degrees of reliance on data collection and processing for revenue generation.

Meta Inc and Uber Inc, for example, rely heavily on data-based revenue streams through targeted advertising and platform optimization. Stellantis N. V., an automotive manufacturer, illustrates how industries are increasingly integrating data into products and services, such as connected vehicles. H&M Group, a fashion and design corporation, demonstrates the growing importance of data in optimizing customer experience and supply chain efficiency.

The analysis is based on information from each corporation’s most recent annual report and privacy policy. Where specific data required by the proposed framework are not available, these gaps are identified. As detailed in Table 2, each corporation’s business model reflects different levels of engagement with mass dataveillance, making them relevant case studies for examining the potential implementation of the proposed reporting requirement.

	Business Model 1	Business Model 2	Business Model 3
Regulatory Subject	Any corporation that facilitates or engages in mass dataveillance as part of its business model. That is, any corporation that derives revenue from the sale of technologies, products, or services that either facilitate, are based on, or are informed or improved by the collection or processing of behavioural data surpluses.		
Definition	They generate revenue by selling technology that facilitates the collection and processing of behavioural data surpluses.	They generate revenue by selling services that are based on the collection and processing of behavioural data surpluses. Predominantly B2B, the buyer is usually not the	They generate revenue by selling products or services that are informed or improved by the use of technology or services that collect and process

	Business Model 1	Business Model 2	Business Model 3
		primary user of the product, but a third party interested in the data for their own products and services.	behavioural data surpluses.
Meta Platforms Inc.	Revenue generated from the sale of VR and AR Glasses with sensors and connectivity capabilities that facilitates the collection and processing of behavioural data surpluses.	Revenue generated from the sale of advertising services that are based on the collection and processing of behavioural data surpluses in order to profile users.	Revenue generated from the sale of subscriptions to their platforms (e.g., Facebook, and Instagram) which are informed and improved by the processing of behavioural data surpluses.
Uber Technologies Inc.	n/a	Revenue generated from the sale of advertising services that are based on the collection and processing of behavioural data surpluses in order to profile users.	Revenue generated from the sale of mobility and delivery services that are informed by the processing of behavioural data surpluses to profit from real-time dynamic pricing and user profile-based recommendations.
Stellantis N. V.	Revenue generated from the sale of vehicles equipped with sensors and connectivity capabilities that facilitates the collection and processing of behavioural data surpluses.	Revenue generated from the sale of data services that are based on the collection and processing of behavioural data surpluses from their vehicles to third parties for in-car advertising, targeted marketing (e.g., billboards), or other commercial purposes (e.g., insurance).	Revenue generated from the sale of in-car services (or on-demand services) informed by the processing of behavioural data surpluses provided by a third party or collected by the vehicle.
H&M Hennes & Mauritz AB	n/a	n/a	Revenue generated from the sale of clothing and accessories whose transactions are enabled

	Business Model 1	Business Model 2	Business Model 3
			by the processing of behavioural data surpluses by a third-party advertising or recommendation service, or a third-party social media analytics service (e.g., Brand Watch).

Table 2. Examples of how different business models based on the collection and processing of behavioural surplus can be applied to Meta Inc., Uber Inc., Stellantis N. V. and H&M AB.

(i) Meta Platforms Inc. (Meta Inc.)

As previously detailed,¹²²⁷ Meta Inc., formerly Facebook Inc, was founded in 2004 and became a publicly traded corporation in 2012.¹²²⁸ Its products include the platforms Facebook, Messenger, Instagram (including apps such as Threads and Boomerang),¹²²⁹ WhatsApp,¹²³⁰ and a range of hardware such as VR glasses (Meta Quest, formerly Oculus),¹²³¹ and AR glasses in partnership with Ray-Ban.¹²³² The following number and categories are based on the information available in Meta Inc.’s most recent annual report and privacy policy.

	Information that Meta Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
Revenue Breakdown	In its 2023 Annual Report, ¹²³³ Meta Inc. reports the following revenue categories and amounts:	A. Revenue Breakdown ¹²³⁴ In order to comply with the proposed framework, Meta Inc. would need to

¹²²⁷ See Chapter IV-II.B., *above*, for a detail description of Meta Platforms Inc

¹²²⁸ See Facebook Inc, *Facebook IPO*, *supra* note 582.

¹²²⁹ See Facebook, “What are the Meta Products?”, *supra* note 565.

¹²³⁰ See Meta, “WhatsApp”, *supra* note 584.

¹²³¹ See Meta, “Products Definition”, *supra* note 585.

¹²³² See Meta, “Ray-Ban”, *supra* note 586.

¹²³³ Meta Platforms Inc, *Meta 10-K 2023*, *supra* note 1217.

¹²³⁴ Meta Platforms Inc, *Meta 10-K 2023*, *supra* note 1217 at 95–96.

	Information that Meta Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
		provide a more detailed breakdown of its advertising revenues than it currently provides in its annual report. Therefore, the following example provides potential subcategories into which advertising revenues could be broken down.
	• Advertising: \$131,948 million • Other revenues: \$1,058 million • Reality Labs: \$1,896 million • Total revenue: \$134,902 million	1. Data-based Revenue: 97.2%
		1.1. Advertising Revenue: \$131,948 million.
		<u>1.1.1. Data-Driven Advertising</u>
		<i>1.1.1.1 Targeted Ads Based on User Behaviour:</i> For instance, ads targeted using data about users' browsing habits, likes, shares, and interactions across the platform.
		<i>1.1.1.2 Cross-Platform Data Usage:</i> For instance, ads that use and combine data from Instagram, WhatsApp, and Facebook.
		<i>1.1.1.3 Lookalike Audiences:</i> For instance, targeting new users based on similarities to the behaviour of existing users.
		<u>1.1.2. Contextual Advertising:</u>
		<i>1.1.2.1 Revenue from Ads Based on Content, Not User Data:</i> For instance, ads that are served based on the context of the page a user is viewing, rather than their individual data.
		<i>1.1.2.2. Revenue from Event-Based Advertising:</i>

	Information that Meta Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
		For instance, ads linked to specific, non-personalized events such as holidays or product launches.
		2. Non-Data-Based Revenue: 2.1%
		2.1 Oculus and Virtual Reality Products: 1.4% 2.1.1. Sales of VR Hardware, VR Software and In-App Purchases: \$1,896 million.
		2.2. WhatsApp Business Platform: 0.7% 2.2.1. Net fees from developers using the payment infrastructure and revenue from various other sources: \$1,058 million.
Data Processing	According to Meta Inc.’s privacy policy, ¹²³⁵ the corporation collects and processes a wide range of behavioural data to support its advertising business, and to personalize the user experience, including content recommendations and suggestions for people, groups or events.	B. Mapping of Data to Revenue Streams
	These data include, but are not limited to: • Metadata about the content • The types of content users see or interact with, and how they interact with it. • The applications and features that users use, and the actions they take within them.	User profiling and advertising revenue: Meta Inc. would need to explain how data such as content metadata, device signals, and location data are aggregated to create detailed user profiles. And how these profiles are then used to target advertising, significantly increasing ad engagement and therefore advertising revenue.
		Cross-platform data integration: Meta Inc. would need to describe how data

¹²³⁵ Meta, “Privacy Policy” (last visited 28 August 2024) online (Privacy Center): <<https://www.facebook.com/privacy/policy>>.

	Information that Meta Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	• The time, frequency and duration of the users' activities on Meta Inc Products • Device characteristics and device software • What users are doing on their device, such as whether Meta Inc.'s applications are in the foreground or whether the user's mouse is moving (which can help distinguish humans from bots). • Identifiers that distinguish a user's device apart from other users. • Device signals • Information that users have shared through their device settings (such as GPS location). • Location-related information • Information about the network a user connects their device to and their connection, including your IP address. • Reports on the performance of Meta Inc. Products on the user's device • Information from cookies and similar technologies	collected across its various platforms (e.g., Facebook, Instagram, WhatsApp) is integrated to provide advertisers with more comprehensive targeting options, thereby increasing the value of ads and the revenue generated from them. Impact on revenue per ad unit: Meta Inc. would need to correlate the use of behavioural data with specific financial outcomes, such as revenue per ad or total ad sales, to demonstrate how data-driven insights directly contribute to the corporation's bottom line.

Table 3. Meta Inc. reporting under the proposed regulatory framework

(ii) Uber Technologies Inc (Uber Inc.)

As previously detailed,¹²³⁶ Uber s Inc. was founded in 2010 and became a publicly traded corporation nine years later, in 2019.¹²³⁷ Its products include Uber Ride, Uber Eats, Uber Transit, Uber Health, Uber Freight, and Uber for Business.¹²³⁸ The following number and categories are based on the information available in Uber Inc’s annual report and privacy policy.

	Information that Uber Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
Revenue Breakdown	In its 2023 Annual Report, ¹²³⁹ Uber Inc. reports the following revenue categories and amounts:	A. Revenue Breakdown Based on the information currently available in Uber Inc.’s annual report and privacy policy, it is difficult to provide a precise breakdown of revenues related to data-driven activities. However, the following example illustrates how Uber Inc. might report under the proposed regulatory framework:
	• Mobility: \$19,832 million • Delivery: \$12,204 million • Freight: \$5,245 million	1. Data-based Revenue:
		1.1. <u>Advertising revenue</u>:¹²⁴⁰ Uber Inc.’s advertising revenue is currently reported under its delivery segment,¹²⁴¹ making it difficult to extract the exact figure. However, this would be a key area

¹²³⁶ See Chapter IV-II.A, *above*, for a detail description of Uber Technologies Inc

¹²³⁷ See Uber Technologies Inc, *Uber IPO*, *supra* note 567.

¹²³⁸ See Uber, “Apps, Products, and Offerings”, *supra* note 568.

¹²³⁹ Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 94.

¹²⁴⁰ “We derive the majority of our advertising revenue from sponsored listing fees paid by merchants and brands in exchange for advertising on our platform. Advertising revenue is recognized when an end-user engages with the sponsored listing based on the number of clicks. Revenue is presented on a gross basis in the amount billed to merchants and brands as we control the advertisement before it is transferred to the end-user.” Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 89.

¹²⁴¹ Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 94.

	Information that Uber Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	Total Revenue: \$37,281 million	requiring more detailed disclosure under the new framework.
		1.2 <u>Data-Driven Recommendations (delivery segment)</u> : This would include revenues generated from targeted restaurant recommendations based on users' order history and preferences.
		1.3 <u>Dynamic Pricing/Surge Pricing (mobility segment)</u> : This would include additional revenue generated during periods of high demand, directly influenced by real-time data on user behaviour and demand patterns.
		2. Non-Data-Based Revenue:
		2.1. <u>Mobility Revenue</u> : ¹²⁴² \$19,832 million 2.1.1. User Fares 2.1.2. Service fees paid by drivers 2.1.3. Fees charge to end users 2.1.4. Membership subscriptions ¹²⁴³
		2.2 <u>Delivery Revenue</u> : ¹²⁴⁴ \$12,204 million 2.2.1. Services fees paid by Couriers

¹²⁴² “We derive our Mobility revenue primarily from service fees paid by Drivers for use of the platform and related service to connect with Riders and successfully complete a trip via the Platform. [...] Depending on the market where the trip is completed, the service fee is either a fixed percentage of the end-user fare or the difference between the amount paid by an end-user and the amount earned by Drivers.” Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 88.

¹²⁴³ “We offer subscription memberships to end-users including Uber One, Uber Pass, Rides Pass, and Eats Pass (“Subscription”). We recognize Subscription fees ratably over the life of the pass. We allocate Subscription fees earned to Mobility and Delivery revenue on a proportional basis, based on usage for each offering during the respective period” Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 94.

¹²⁴⁴ “We derive our Delivery revenue from service fees paid by Couriers and Merchants for use of the platform and related service to successfully complete meal preparation, grocery and other delivery service on the platform, amounts charged to end-users for Delivery services, and fees charged to end-users for use of the platform in certain markets.” Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 88.

	Information that Uber Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
		2.2.2. Services fees paid by Merchants
		2.3. <u>Freight and Logistics Revenue</u> : ¹²⁴⁵ \$5,245 million
Data Processing	According to Uber Inc.’s privacy policy, ¹²⁴⁶ the corporation collects and processes a wide range of behavioural data to support various aspects of its business, including advertising and personalized services.	B. Mapping of Data to Revenue Streams
	The information collected includes: • Inferred gender information • Location data: Precise or approximate location data collected from users’ devices. • Transaction data: Types of services requested or provided, trip or order details (such as the date and time, pick-up and drop-off addresses, distance travelled and items ordered); and payment transaction information (such as a name and location of a restaurant or merchant, amount charged, and payment method). • Usage data: Access dates and times, application features or pages viewed, browser type, and application crashes and other system activity.	Dynamic pricing: Uber Inc. would need to explain how surge pricing, which is adjusted based on real-time demand data, directly impacts its revenue. This would include an analysis of how behavioural data (e.g., user activity patterns, location data) is used to implement surge pricing.
		Personalized recommendations: Uber Inc. would need to detail how data such as past order history and user preferences are used to provide targeted restaurant recommendations, and how this practice contributes to revenue in the delivery segment.
		Advertising revenue: Uber Inc. would need to clarify how user data are used to generate advertising revenue, particularly in the delivery segment, and what specific data types are used to generate targeted ads.

¹²⁴⁵ “We derive our Freight revenue from freight transportation services provided to Shippers.” Uber Technologies Inc, *Uber 10-K 2023*, *supra* note 1221 at 86.

¹²⁴⁶ Uber, “Uber Privacy Notice (7/17/2024)” (last visited 28 August 2024) online: <<https://www.uber.com/legal/en/document/>>.

	Information that Uber Inc. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	• Device data: Includes the hardware models, device IP address or other unique device identifiers, operating systems and versions, software, preferred languages, advertising identifiers, devices motion data, and mobile network data.	

Table 4. Uber Inc. reporting under the proposed regulatory framework

(iii) Stellantis N. V.

Stellantis N. V. is a multinational automobile corporation with global operations, owning 14 well-known car brands, including Jeep, Chrysler, Peugeot and Fiat. The corporation was incorporated in the Netherlands in April 2014 as a public limited corporation, initially named Fiat Chrysler Automobiles N.V. The current Stellantis N. V. is the result of the consolidation of FCA and PSA, two formerly independent and prominent global automobile groups.¹²⁴⁷ In 2021, Stellantis N. V. launched its strategy “to transform itself to a sustainable mobility tech corporation—emphasizing the electrification and software of its vehicles.”¹²⁴⁸

Stellantis N. V. does not have a centralized privacy policy that applies to all of its vehicles and services. Instead, its privacy policies vary by region and by services provided. For example, in both Canada and Europe, there are two different privacy policies: one applies when accessing the website or applications,¹²⁴⁹ while the other applies to the connected services offered directly in

¹²⁴⁷ See Stellantis N.V., *Annual Report for the Year Ended December 31, 2023* (Stellantis N.V., 2023) at 18.

¹²⁴⁸ Stellantis N.V., *Annual Report Stellantis*, *supra* note 1247 at 190.

¹²⁴⁹ See Stellantis, “Europe’s General Privacy Policy” (30 June 2023) online: <jeep.co.uk> [http://web.archive.org/web/20241015015305/https://www.jeep.co.uk/privacy]; Stellantis, “FCA Canada Inc Privacy Policy” (15 August 2019) online: <fcacanada.ca> [http://web.archive.org/web/20240926114254/https://www.fcacanada.ca/privacy/].

the vehicles.¹²⁵⁰ For the purposes of this analysis, both types of privacy policies are considered as they relate to the handling of behavioural data.

	Information that Stellantis N. V. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
Revenue Breakdown	In its 2023 Annual Report, ¹²⁵¹ Stellantis N. V. reported the following revenue categories and amounts:	A. Revenue Breakdown Based on the information currently available in Stellantis N. V.’s annual report and privacy policy, it is difficult to provide a precise breakdown of revenues related to data-driven activities. This may be due to the fact that data-driven activities are a new business area for the Corporation. However, the following example illustrates how Stellantis N.V. might report under the proposed regulatory framework:
	• Shipments of Vehicles and Sales of Other Goods: €183,230 million • Other Services Provided:¹²⁵² €4,018 million	1. Data-based Revenue:¹²⁵³ 1.1. <u>Revenue from Connected Car Services:</u>¹²⁵⁴ This includes revenues from services or subscription models offered on the basis of data collected by sensors and on-board systems. Services such as real-time

¹²⁵⁰ See Stellantis, “Appendix II : European Connected Vehicles Privacy Policy” (last visited 16 October 2024) online (PDF): <services-store.peugeot.co.uk> [http://web.archive.org/web/20241108155700/https://services-store.peugeot.co.uk/sites/peugeot/files/2024-02/Privacy%20Policy%20UK%2010-23.pdf]; Stellantis, “Brand Connect Powered by SiriusXM Privacy Policy” (22 August 2023) online: <driveuconnect.ca> [http://web.archive.org/web/20240519200318/https://www.driveuconnect.ca/connected-services/privacypolicy.html].

¹²⁵¹ Stellantis N.V., *Annual Report Stellantis*, *supra* note 1247 at 292.

¹²⁵² “Other revenues from services provided are primarily comprised of maintenance plans, extended warranties, and connectivity services, and are recognized over the contract period in proportion to the costs expected to be incurred based on the Company’s historical experience” Stellantis N.V., *Annual Report Stellantis*, *supra* note 1247 at 272.

¹²⁵³ Stellantis plans to double its net revenues to €300 billion. It projects that 20% of total revenues will come from growth in its software and services business. See Stellantis, “Dare Forward 2030: Financials” (last visited 22 October 2024) online: <stellantis.com> [http://web.archive.org/web/20241009105942/https://www.stellantis.com/en/company/dare-forward-2030/financials].

¹²⁵⁴ Currently, a part of this category is recognized under the category of “other services provided”. See Stellantis N.V., *Annual Report Stellantis*, *supra* note 1247 at 272.

	Information that Stellantis N. V. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	• Construction Contract Revenues: €709 million • Lease Instalments from Assets Sold with a Buy-Back Commitment: €896 million • Interest Income of Financial Services Activities: €691 million • Net Revenues: €189,544 million	navigation, remote diagnostics, and vehicle maintenance alerts. ¹²⁵⁵
		1.2 <u>Revenue from Targeted Marketing and personalized offers:</u> With connected cars and customer profiles, Stellantis N. V. can deliver personalized marketing offers (e.g., car upgrades, services) based on user behaviour, location and driving patterns. This category should include revenues from targeted in-car advertising (via infotainment systems) and from services offered.
		1.3 <u>Revenue from Data Monetization:</u>¹²⁵⁶ This should include the revenues from Stellantis N. V.’s data business unit: Mobilisights.¹²⁵⁷
		2. Non-Data-Based Revenue:
		2.1 <u>Vehicle sales and other goods</u> 2.1.1 Sales of non-connected vehicles 2.1.2 Sales of connected vehicles 2.1.3 Other goods

¹²⁵⁵ See Kirsten Korosec, “How Stellantis Plans to Make \$22.5B a Year from Software in its Cars, Trucks and SUVs”, *TechCrunch* (7 December 2021), online: <techcrunch.com> [http://web.archive.org/web/20220103175622/https://techcrunch.com/2021/12/07/how-stellantis-plans-to-make-22-5b-a-year-from-software-in-its-cars-trucks-and-suvs/].

¹²⁵⁶ “In January 2023, Stellantis announced the establishment of Mobilisights, a business unit dedicated to executing the Company’s DaaS strategy globally by serving as the gateway to telematic data from the Company’s connected vehicles. Stellantis targets to have an estimated 34 million connected vehicles on the road globally by 2030.” Stellantis N.V., *Annual Report Stellantis*, *supra* note 1247 at 27.

¹²⁵⁷ See Stellantis, “Mobilisights” (last visited 10 October 2024) online: <mobilisights.com> [http://web.archive.org/web/20241010000049/https://www.mobilisights.com/]; Stellantis, “New ‘Mobilisights’ Business Unit Advances Stellantis’ Growing Data and Connected Services Offer” (5 January 2023) online (Press Release): <stellantis.com> [http://web.archive.org/web/20240430153841/https://www.stellantis.com/en/news/press-releases/2023/january/new-mobilisights-business-unit-advances-stellantis-growing-data-and-connected-services-offer].

	Information that Stellantis N. V. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
		2.2 <u>Aftersales Services</u> :
		2.3 <u>Construction Contract Revenues</u> : €709 million
		2.4 <u>Lease Instalments from Assets Sold with a Buy-Back Commitment</u> : €896 million
		2.5. <u>Interest Income of Financial Services Activities</u> : €691 million
Data Processing	According to Stellantis N. V.’s privacy policies, the corporation collects and processes a wide range of behavioural data to support various aspects of its business. With respect to the data collected through the use of its website and application, some of the purposes include: behavioural advertising, marketing,¹²⁵⁸ for communications, to provide a service, to share data with partners for their own marketing purposes,¹²⁵⁹ and to analyze user preferences and behaviours in order to customize its services and communications.¹²⁶⁰ With respect to the data collected through their connected services, some of the purposes include:¹²⁶¹ to provide the Connected Services and related support, and to evaluate and	B. Mapping of Data to Revenue Streams

¹²⁵⁸ See Stellantis, “Canada Privacy Policy”, *supra* note 1249, s 6.“

¹²⁵⁹ See Stellantis, “EU Privacy Policy”, *supra* note 1249, s 4(h).

¹²⁶⁰ In this case it does not only includes the data collected from website and application, but also “vehicle data.” See Stellantis, “EU Privacy Policy”, *supra* note 1249, s 4(f).

¹²⁶¹ See Stellantis, “Canada Connected Services”, *supra* note 1250; Stellantis, “EU Connected Services”, *supra* note 1250.

	Information that Stellantis N. V. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	improve the vehicles and the Connected Service.	
	The data collected includes, but are not limited to: • Website or application usage data: this may include, but is not limited to, the pages viewed, the search terms entered, IP address, operating systems and browser clients, and geographical location.¹²⁶² • Location data:¹²⁶³ this includes data from the sensors of the device used to access the website or application, or the IP address. • Information inferred from the individual's activity:¹²⁶⁴ this includes, for example, Stellantis N. V. being able to understand driving style, most travelled routes and places of interest based on interactions with the connected services.¹²⁶⁵	Connected car services: Stellantis N. V. would need to detail how data collected from vehicles (e.g., driving patterns, diagnostics, maintenance needs) is translated into revenue through connected car services. For example, they would explain how subscription models for these services are driven by real-time data collection and analysis.
		In-car advertising and personalized offers: Stellantis N. V. would need to demonstrate how in-car advertising or personalized service recommendations are created using data from the car's infotainment system, driving habits and user preferences, and how this contributes to targeted marketing revenues.
		Data Monetization: Stellantis N. V. would need to demonstrate how the telematics data collected across all its different vehicle brands is used to deliver the various services offered by Mobilisights or another business unit, and how this contributes to its data monetization business.

¹²⁶² See Stellantis, “Canada Connected Services”, *supra* note 1250; Stellantis, “Canada Privacy Policy”, *supra* note 1249, s 4.

¹²⁶³ Stellantis, “Canada Privacy Policy”, *supra* note 1249, s 4; Stellantis, “Canada Connected Services”, *supra* note 1250; Stellantis, “EU Privacy Policy”, *supra* note 1249, s 2(d); Stellantis, “EU Connected Services”, *supra* note 1250.

¹²⁶⁴ See Stellantis, “EU Privacy Policy”, *supra* note 1249, s 2(c).

¹²⁶⁵ See Stellantis, “EU Connected Services”, *supra* note 1250.

	Information that Stellantis N. V. Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	• Vehicle data:¹²⁶⁶ this is all technical, diagnostic and real-world data that can be collected via the sensors and devices installed on the vehicle. Such as location, speed and distances, engine running time and turning off time; if the battery cable is cut, battery diagnostics, movements with the key removed, suspected collision, as well as diagnostic data such as, but not limited to, oil and fuel levels, tire pressure, and engine status.¹²⁶⁷	

Table 5. Stellantis N. V. reporting under the proposed regulatory framework.

(iv) H&M Hennes & Mauritz AB (H&M Group)

H & M Hennes & Mauritz AB (H&M Group) is a global fashion and design corporation headquartered in Stockholm, Sweden. Founded in 1947, the corporation now operates more than 4,000 stores in over 75 markets and has an online presence in 60 markets.¹²⁶⁸ Since its initial public offering on the Stockholm Stock Exchange in 1974,¹²⁶⁹ the H&M Group has developed into a multi-brand organization. Its portfolio includes the core brand H&M, which includes H&M HOME, and a collection of brands such as COS, Weekday, Monki, & Other Stories, ARKET and

¹²⁶⁶ See Stellantis, “EU Privacy Policy”, *supra* note 1249, s 4(f); Stellantis, “Canada Connected Services”, *supra* note 1250.

¹²⁶⁷ See Stellantis, “EU Privacy Policy”, *supra* note 1249, s 15; Stellantis, “Canada Connected Services”, *supra* note 1250.

¹²⁶⁸ See H&M Group, “About Us” (last visited 22 October 2024) online: <hmgroupprdapp.azurewebsites.net> [http://web.archive.org/web/20241003210330/https://hmgroupprdapp.azurewebsites.net/about-us/].

¹²⁶⁹ See H&M Group, “History” (last visited 22 October 2024) online: <hmgroupprdapp.azurewebsites.net> [http://web.archive.org/web/20241003205903/https://hmgroupprdapp.azurewebsites.net/about-us/history/].

Singular Society. The Group also manages New Growth & Ventures, which includes initiatives such as Creator Studio and the majority-owned resale platform Sellpy.¹²⁷⁰

According to the H&M Group Annual Report 2023, the corporation stays competitive by adapting quickly to an ever-changing world and acting with agility. One of the corporation's ongoing developments focusses on driving digitalization and the use of new technologies.¹²⁷¹ For example, in 2023 H&M focussed on achieving long-term profitable growth through digital and sustainability transformation, improving the customer offer, and integrating digital and physical channels. Key initiatives included optimizing the supply chain and introducing innovative business models.¹²⁷² As part of the digitalization efforts, some of the customer experience enhancements included a customer membership programme,¹²⁷³ visual search tools,¹²⁷⁴ and smart mirrors in fitting rooms¹²⁷⁵ to provide personalized recommendations and improve the shopping experience.

H&M has two relevant privacy policies. The first one applies to all customers of the H&M Group.¹²⁷⁶ The second policy applies to all past, present, and potential business partners, agents,

¹²⁷⁰ See H&M Group, "Organization and Management" (last visited 22 October 2024) online: <hmgroup-prd-app.azurewebsites.net> [<http://web.archive.org/web/20241003210147/https://hmgroup-prd-app.azurewebsites.net/about-us/corporate-governance/company-management/>].

¹²⁷¹ See H&M Group, *Annual and Sustainability Report 2023* (H&M Group, 2023) at 47.

¹²⁷² See H&M Group, *Annual Report H&M*, *supra* note 1271 at 46.

¹²⁷³ "Members receive personal fashion offers and services for an inspirational and more convenient shopping experience. Other benefits include rewards for bringing in clothes for H&M's garment collecting, attending exclusive events and receiving other offers." H&M Group, *Annual Report H&M*, *supra* note 1271 at 32.

¹²⁷⁴ These tools use image recognition to provide "recommendations and suggestions for styling and matching items based on pictures customers have taken and been inspired by." H&M Group, *Annual Report H&M*, *supra* note 1271.

¹²⁷⁵ These are mirrors "that recognise products brought inside the fitting room and offer personalised product and styling recommendations, or additional sizes and colours." H&M Group, *Annual Report H&M*, *supra* note 1271.

¹²⁷⁶ The text of this privacy policy will vary slightly depending on the country in which the consumer accesses the service. See e.g., H&M Group, "H&M Group Privacy Notice Canada" (September 2024) online: <hm.com> [http://web.archive.org/web/20230325072615/https://www2.hm.com/content/dam/Customer-Service/Legal/privacy-notice-pdf/en-CA_HM%20Group%20Customer%20Privacy%20Notice.pdf]; H&M Group, "H&M Group Privacy Notice EU" (October 2024) online: <hm.com> [http://web.archive.org/web/20240519040619/https://www2.hm.com/content/dam/Customer-Service/Legal/privacy-notice-pdf/IE_HM%20Group%20Customer%20Privacy%20Notice.pdf].

franchisees, suppliers, subcontractors, shareholders, on-site visitors (to its premises or websites) or other stakeholders with whom the H&M Group has a relationship.¹²⁷⁷ The majority of the following analysis is based on the information provided in the first privacy policy. In addition, some information from the “Brand and Consumer Perception Analysis” section of the second privacy policy will be considered. Where this is the case, reference will be made to the second policy.

	Information that the H&M Group Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
Revenue Breakdown	In its 2023 Annual Report, ¹²⁷⁸ the H&M Group reported the following revenue categories and amounts:	A. Revenue Breakdown Based on the information currently available in the H&M Group’s annual report and privacy policy, it is difficult to provide a precise breakdown of revenues related to data-driven activities. This may be due to the fact that data-driven activities are a new business area for the Group. However, the following example illustrates how the H&M Group might report under the proposed regulatory framework:
		1. Data-based Revenue:
	Group Net Sales:¹²⁷⁹ SEK 236,035 million	1.1. <u>Revenue from Targeted Ads</u> : the H&M Group uses browsing history and purchase data from online shoppers to deliver personalized ads via platforms such

¹²⁷⁷ See H&M Group, “H&M Group Privacy Notice: General” (June 2024) online: <hmgroup-prd-app.azurewebsites.net> [http://web.archive.org/web/20241003220534/https://hmgroup-prd-app.azurewebsites.net/legal-notice/].

¹²⁷⁸ H&M Group, *Annual Report H&M*, *supra* note 1271 at 94–113.

¹²⁷⁹ Net sales refer to both store and online and sales, and includes the “the sale of clothing, accessories, footwear, cosmetics, home textiles and homeware to consumers.” Additionally, “a smaller share of the total turnover also consists of the sale of services such as repair and rental, commission-based sales, second-hand online sales, a membership-based business model and B2B sales of print-on-demand.” H&M Group, *Annual Report H&M*, *supra* note 1271 at 111.

	Information that the H&M Group Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	Parent Company Net Sales:¹²⁸⁰ SEK 2,264 million	as Google or social media to encourage purchases.
		1.2 <u>Revenue from Personalized Shopping Experiences</u> : Data collected from online and in-store shopping behaviour (e.g., size preferences, style choices) is used to recommend products that can drive higher conversion rates in online sales.
		1. Non-Data-Based Revenue: SEK 236,035 million ¹²⁸¹
		2.1. <u>Sales</u> : 2.1.1. Clothing, accessories, footwear, cosmetics, home textiles and homeware 2.1.2. Second-hand online sales
		2.1 <u>Services</u> : 2.2.1. Clothes Repair 2.2.2. Rental Clothes
		2.3. <u>Membership-based business model</u> ¹²⁸²
		2.4 <u>B2B Sales of print-on-demand</u> ¹²⁸³
Data Processing	According to the H&M Group's privacy policies, the corporation collects and processes a wide range of behavioural data to support various aspects of its business,	B. Mapping of Data to Revenue Streams

¹²⁸⁰ The parent company's internal sales consist of royalties and other income from group companies. H&M Group, *Annual Report H&M*, *supra* note 1271 at 112.

¹²⁸¹ The proposed subcategories are currently reported under the net sales category. H&M Group, *Annual Report H&M*, *supra* note 1271 at 111.

¹²⁸² One example of this is their "Singular Society" brand. This is a membership-based brand that offers premium products at the cost of production. See H&M Group, *Annual Report H&M*, *supra* note 1271 at 29.

¹²⁸³ This is the case with Creator Studio. A B2B service offering on-demand printing services that enables external brands and content creators to use H&M Group's supply chain to produce their own merchandise for sale. See H&M Group, *Annual Report H&M*, *supra* note 1271 at 30, 45.

	Information that the H&M Group Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	including providing the products and services requested by customers, performing customer service functions, for security and fraud prevention, and for marketing and promotional purposes.	
	The data collected includes, but are not limited to: • Location data may be processed within mobile applications if the user enables location-based service, such as self-checkout in stores • IP address • Behavioural and contextual data collected through cookies or similar technology • MAC addresses • Other system generated data derived from the user's activities and engagement with the H&M Group. • Marketing email recipient engagement metrics, including email "read status," and timestamp • Transaction data, such as product information, order value, payment method and preferences • Interaction with social media images and videos¹²⁸⁴	E-commerce personalization and targeted advertising: the H&M Group would need to explain how data collected from user interactions with its website or app directly influences its advertising strategies and sales. For example, they could track how product recommendations based on previous purchases increase online sales.
		Inventory and supply chain optimization: the H&M Group would need to explain how it uses data on customer preferences to adjust inventory in real time to ensure that popular items are always available. This would show how data indirectly supports their sales by improving operational efficiency.

¹²⁸⁴ See H&M Group, "H&M Privacy Notice: General", *supra* note 1277.

	Information that the H&M Group Currently Discloses	Example of Reporting under the Proposed Regulatory Framework
	Interests based on social media activity¹²⁸⁵	

Table 6. H&M AB. reporting under the proposed regulatory framework

(d) Enforcement of the Duty

Given that the proposed duty will fall under corporate law, it should be monitored and enforced by the existing public authority responsible for ensuring compliance with corporate law.¹²⁸⁶ Assigning the new duty to the existing corporate law compliance authority offers several advantages, including leveraging established expertise, ensuring regulatory consistency, and streamlining compliance processes for corporations. The authority's existing resources and experience in overseeing corporate law could facilitate the effective implementation of the new duty, while its broader perspective could lead to comprehensive oversight.

A potential drawback, however, is that the authority may lack the specialized expertise needed to address the complex issues associated with data-driven business models. To address this, the regulatory framework could, as part of the reform, create a dedicated unit within the agency to oversee corporations that sell and use technologies to collect and process data about individuals and their behaviours. The benefit of creating this specialized unit would be a more

¹²⁸⁵ See H&M Group, *supra* note 1277.

¹²⁸⁶ In the case of Canada, for instance, this would be Corporations Canada. See Innovation, Science and Economic Development Canada, "Corporations Canada: About Us" (28 May 2024) online: <ised-isde.canada.ca> [http://web.archive.org/web/20240712120907/https://ised-isde.canada.ca/site/corporations-canada/en/about-us].

focussed and informed regulatory approach, enabling the agency to effectively monitor and address the unique challenges posed by data-driven business models.

Following the submission of a corporation's annual report, which would include the new reporting requirements outlined above, the public authority would review both the breakdown of revenues and the mapping of data to revenues. In particular, this will include an analysis of the "data-based revenues" and the explanation in the "mapping of data to revenue streams" sections to determine whether these revenues are mainly generated from behavioural surplus data, or from other types of data (e.g., non-behavioural data, or behavioural data). Given the pathological characteristics of corporations, including the tendency to manipulate information, and to ensure the accuracy of these reports, the regulator may require independent third-party audits to verify the corporation's data practices and their relationship to the revenue generation.

If the regulator finds that a corporation is not complying, or if the corporation fails to provide the required information (or provides incomplete information), the regulator would have the power to impose penalties,¹²⁸⁷ which would count towards the three strikes for non-compliance as described in the next section.

If a corporation fails to provide the required information, the regulator should request the missing information and allow 2–3 weeks for compliance. If the corporation still fails to comply, the authority could impose a fine and set a final deadline for compliance. Continued non-compliance after this period would result in additional fines and further enforcement action.

¹²⁸⁷ An example of a penalty could be the refusal of a certificate of compliance, as is currently the case in Canada, if a corporation fails to file its "Individuals with Significant Control" information. See Innovation, Science and Economic Development Canada, "Individuals with Significant Control" (26 February 2024) online: <ised-isde.canada.ca> [<http://web.archive.org/web/20240605184701/https://ised-isde.canada.ca/site/corporations-canada/en/individuals-significant-control-file-your-information>].

If a corporation submits complete information but is found to be non-compliant, the regulator could require the corporation to forfeit profits derived from prohibited data practices. This approach would directly target the financial incentives behind surveillance capitalism. In addition, the agency would order the corporation to change its business model within a specified period of time. During this time, the corporation would be required to report regularly to the agency on the steps it is taking to ensure compliance.

B. Consequences to Corporations' Own Existence: Mandatory Dissolution

A second aspect of the legal structure of the corporation that has contributed to its pathological personality is that, in the absence of real consequences for its own existence, compliance with the law for a corporation is simply a matter of costs and benefits.¹²⁸⁸ As a result, pathological traits such as irresponsible behaviour, refusal to accept responsibility or remorse, and asocial tendencies have been allowed to multiply.

Therefore, in order to limit the pathological personality of corporations, it is necessary that the proposed regulatory framework includes consequences for non-compliance that represent more than a simple economic cost-benefit decision for corporations. Specifically, this framework should provide for mandatory dissolution of the corporation as a measure for non-compliance with the proposed duty to limit revenue streams. This measure would be enforced by the same authority responsible for the enforcement of corporate law.

Given the significant harms and risks associated with corporate mass dataveillance systems, coupled with the substantial profits these systems generate and the lengths to which

¹²⁸⁸ See Bakan, *The Corporation*, *supra* note 1 at 79.

corporations will go to maintain and expand their dataveillance capabilities,¹²⁸⁹ the implementation of this strong remedy is both necessary and justified, as these systems constitute an ongoing and systematic interference with privacy.

Involuntary dissolution,¹²⁹⁰ or the revocation of a corporation's charter, is based on the premise that corporations are created by law, and given special privileges to enable them to function, such as limited liability. However, because some corporations abuse their privileges by repeatedly breaking the law and becoming a danger to society, the law also has the power to revoke a corporation's right to exist and do business.¹²⁹¹ This measure materializes the idea of democratic governance of corporations, and the idea that "corporations are our creations and that we—the people—still have the power to control them."¹²⁹²

Building on this concept, some academics and social organizations advocate for judicial dissolution as a tool to address corporate wrongdoing.¹²⁹³ They see it as a manifestation of the state's authority over corporations,¹²⁹⁴ and a means of promoting corporate responsibility to

¹²⁸⁹ See Chapter IV, *above*.

¹²⁹⁰ Involuntary dissolution occurs when a company is dissolved by an external authority or court order, rather than by the decision of its shareholders, which is the case in voluntary dissolution.

¹²⁹¹ See e.g., Bakan, *The Corporation*, *supra* note 1 at 156; Mary Kreiner Ramirez, "The Science Fiction of Corporate Criminal Liability: Containing the Machine Through the Corporate Death Penalty" (2005) 47 *Arizona Law Review* 933 at 197.

¹²⁹² Bakan, *The Corporation*, *supra* note 1 at 158. For as history of the charter revocation in the common law, and in the Canadian legal system see Gil Yaron, *Awakening Sleeping Beauty: Reviving Lost Memories and Discourses to Revoke Corporate Charters* (Master of Laws, University of British Columbia, 2000) [unpublished].

¹²⁹³ See e.g., Bri Holmes, "Our Model Corporate Charter Revocation Act" (14 March 2015) online: <freespeechforpeople.org> [<http://web.archive.org/web/20240622115614/https://freespeechforpeople.org/model-corporate-charter-revocation-act/>].

¹²⁹⁴ See Bakan, *The Corporation*, *supra* note 1 at 156–58.

See also Kyle Noonan, "The Case for a Federal Corporate Charter Revocation Penalty" (2012) 80:2 *George Washington Law Review* 602; Mitchell F Crusto, "Green Business: Should We Revoke Corporate Charters for Environmental Violations" (2003) 63 *Louisiana Law Review* 175.

society at large.¹²⁹⁵ Proponents argue that involuntary dissolution directly challenges a corporation's ability to break the law, thereby strengthening the integrity of legal systems by holding corporations accountable in a way that repeated fines may not achieve.¹²⁹⁶

A common feature of the proposals for judicial dissolution or charter revocation is that they are based on the violation of external regulations by corporations, such as corruption,¹²⁹⁷ environmental damage,¹²⁹⁸ and corporate crime.¹²⁹⁹ These proposals therefore seek to bridge the gap between the government's power to create corporations and its power to ensure that they comply with broader societal rules. While these approaches have merit, this thesis proposes an alternative solution that takes a different route.

Instead of relying on breaches of external law, this thesis advocates for a corporate-based solution by introducing a new duty within corporate law itself: the duty to limit revenue streams.¹³⁰⁰ This duty is consistent with the broader purpose of corporations proposed earlier,¹³⁰¹ and aims to address their pathological tendencies by transforming their institutional character from within.

Consequently, the proposed dissolution mechanism would be triggered by a breach of this newly established corporate duty. This approach directly links non-compliance with corporate governance principles to consequences for the corporation's existence, thereby reinforcing the

¹²⁹⁵ See e.g., Yaron, *Awakening Sleeping Beauty*, *supra* note 1292 at 155–56; Linzey, “Killing Goliath”, *supra* note 1077 at 63; Holmes, “Model Charter Revocation”, *supra* note 1293.

¹²⁹⁶ See e.g., Noonan, “Federal Corporate Charter Revocation”, *supra* note 1294 at 606.

¹²⁹⁷ See e.g., John F Hulpke, “If All Else Fails, A Corporate Death Penalty?” (2017) 26:4 *Journal of Management Inquiry* 433.

¹²⁹⁸ See e.g., Linzey, “Killing Goliath”, *supra* note 1077.

¹²⁹⁹ See e.g., Noonan, “Federal Corporate Charter Revocation”, *supra* note 1294 at 620; Ramirez, “Science Fiction of Corporate Criminal Liability”, *supra* note 1291.

¹³⁰⁰ See Section A-2, *above*.

¹³⁰¹ See Section A-1, *above*.

limits of its pathological behaviour. By integrating this mechanism into corporate law, it creates a more coherent framework for corporate accountability.

Current corporate law already provides for the dissolution of a corporation in certain cases, based mainly on the traditional view of corporate law as a set of rules for the protection of shareholders and the functioning of the corporation.¹³⁰² For instance, one ground for involuntary dissolution is that the corporation has failed to fulfill with some of its obligations under corporate law, such as notifying about relevant changes or completing annual reports.¹³⁰³ The proposed framework would add a new ground for the dissolution: failure to comply with the duty to limit revenue streams.

The remainder of this section sets out the details of the proposal, which builds on previous proposals to use mandatory dissolution as a measure for corporate wrongdoing.

1) Triggering the Dissolution of a Corporation

Since it is the state that grants corporations the right to exist, the power to take action to revoke this right also rests with the state. However, a significant limitation of the current charter revocation process, as highlighted in the literature, is the reluctance of the state to take such action, particularly against large corporations, due to political pressure.¹³⁰⁴ Linzey, for example, argues that the use of charter revocation has become almost obsolete in the US because of the reluctance of state officials to exercise their powers in the face of increasing economic dependence on large

¹³⁰² See Greenfield, “Proposition”, *supra* note 1139.

¹³⁰³ See e.g., *CBCA*, *supra* note 1191 at s 212; *Directive Regarding Company Law*, *supra* note 1222 at art 11.

¹³⁰⁴ See e.g., Charlie Cray, “Chartering a New Course: Revoking Corporations’ Right to Exist” (2002) *Multinational Monitor* 8.

corporations. This obsolescence is further exacerbated by the close links between corporations and political structures.¹³⁰⁵

This reluctance of the state to exercise its power to revoke the right of corporations to exist is particularly relevant in the case of corporations that facilitate or engage in mass dataveillance. As noted above, the data collected and processed by these corporations is also a goldmine for governments.¹³⁰⁶ This alignment of interests has led to a public-private surveillance partnership in which both corporations and governments have a vested interest in the continued collection of data about individuals, including behavioural data surpluses, by corporations.¹³⁰⁷ This partnership is likely to result in government inaction to trigger the dissolution of any of these corporations.

To address this lack of enforcement, one proposed solution is to clearly define the circumstances in which involuntary dissolution should be applied. For example, it could be stipulated that a corporation must be dissolved after it has committed three serious offences. This approach aims to create a clear obligation for states to address corporate abuse, rather than leaving it to the discretion of the state, as is currently the case. This model would establish a more structured and consistent method of holding corporations accountable for repeated violations.¹³⁰⁸

Another proposed solution is to allow individuals or groups, not just the state, to initiate the process of dissolving a corporation. Linzey, for example, argues that there is a need for a quasi-private cause of action that would allow citizen groups to challenge in court the inaction of the

¹³⁰⁵ See Linzey, “Killing Goliath”, *supra* note 1077 at 6.

¹³⁰⁶ See Chapter IV-III.C, *above*. See also Zuboff, *Age of Surveillance Capitalism*, *supra* note 170 c 4.

¹³⁰⁷ See e.g., Büchi et al, “The Chilling Effects of Algorithmic Profiling”, *supra* note 810; Bruce Schneier, “The Public-Private Surveillance Partnership”, *Bloomberg* (1 August 2013), online: <bloomberg.com> [http://web.archive.org/web/20201112024906/https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership].

¹³⁰⁸ See Noonan, “Federal Corporate Charter Revocation”, *supra* note 1294 at 623–25; Ramirez, “Science Fiction of Corporate Criminal Liability”, *supra* note 1291 at 41.

Attorney General in exercising his power to initiate charter revocation proceedings in cases where a corporation repeatedly acts illegally.¹³⁰⁹ Similarly, the organization Free Speech for People proposed that the law should authorize citizens to bring an action to revoke a corporation's charter. As a safeguard, they propose that such citizen suits must allege at least three separate offences committed by the corporation within a ten-year period.¹³¹⁰ Such proposals are intended to provide a means of direct citizen control over corporations.

The proposed framework will build on these proposals. First, it will clearly set out when non-compliance with the duty to limit revenue streams would lead to the dissolution of a corporation. As discussed in the previous section, corporations will be required to submit reports outlining their business models, which will allow authorities to verify compliance with the proposed duty.¹³¹¹ If a regulator determines that a corporation is not in compliance, or if the corporation fails to provide the required information (or provides incomplete information), the regulator would impose a penalty.¹³¹²

In cases of non-compliance or failure to provide complete information, the framework provides for a structured system of penalties. In particular, the framework would require the public authority to initiate the dissolution process after imposing three penalties on the corporation for non-compliance with the duty to limit revenue streams duty.¹³¹³ Setting a specific number of

¹³⁰⁹See Thomas Linzey, "Awakening a Sleeping Giant: Creating a Quasi-Private Cause of Action for Revoking Corporate Charters in Response to Environmental Violations" (1995) 13:1 Pace Environmental Law Review 219; Linzey, "Killing Goliath", *supra* note 1077.

¹³¹⁰ See Free Speech For People, "Model Corporate Charter Revocation Act" (13 March 2015) online (PDF): <freespeechforpeople.org> [<http://web.archive.org/web/20240128055455/https://freespeechforpeople.org/wp-content/uploads/2015/06/Free-Speech-For-Peoples-Model-Corporate-Charter-Revocation-Act.pdf>] at 1.

¹³¹¹ See Section A-2.b, above.

¹³¹² See Section A-2.d, above.

¹³¹³ In the context of charter revocation for corporate crimes, Ramirez and Noonan offer a similar approach based on the number of penalties or convictions previously imposed on the corporation. See Ramirez, "Science Fiction of Corporate Criminal Liability", *supra* note 1291; Noonan, "Federal Corporate Charter Revocation", *supra* note 1294.

penalties seeks to strike a balance between ensuring that the dissolution represents a real threat to the corporation, thereby deterring non-compliance, and recognizing that the transition to a business model that does not rely on the sale of technologies, products, or services that either facilitate, are based on, or are enhanced by the collection or processing of behavioural data surpluses may take time.

To increase transparency and accountability, any penalty imposed on a corporation would be recorded in a public register accessible on the public authority's website. This register would not only list all the penalties, but would also indicate whether dissolution proceedings have been initiated. Such transparency would allow the public to monitor a corporation's compliance record and hold the public authority accountable for its obligations under this new framework.

To address cases where public authorities may be reluctant to act, the framework should empower citizens or citizens' groups to initiate the dissolution process in cases where, according to the public register, a corporation has accumulated three or more sanctions without a dissolution proceeding having been initiated. If the case proceeds, this mechanism would help address situations where government officials may be reluctant to act due to political pressure or vested interests in the data collected by the corporation.

The dissolution process would follow the established rules for involuntary dissolution, including giving notice to the corporations and an opportunity for the corporation to appeal the public authority's decision to the court.¹³¹⁴ If the appeal is unsuccessful, the dissolution process would continue.

¹³¹⁴ See e.g., *CBCA*, *supra* note 1191 at s 246(g).

2) Dissolution Process and Alternatives.

The economic impact of dissolving a corporation, particularly a large one, can be significant. To mitigate these effects, the dissolution process must be carefully managed.¹³¹⁵ A committee composed of members of the enforcing public authority should be appointed to oversee the process, with final approval by a court. This committee should have some experience in the corporation's line of business and understand the corporation's upstream and downstream relationships.

This committee would have two options: either to proceed with the dissolution and ask the court to commence liquidation, or to determine that the dissolution would be detrimental to the public interest. Factors such as potential job losses, economic impact, or societal reliance on the corporation's technologies may justify preventing the dissolution. In such cases, the committee would need to find alternative solutions to allow the corporation to continue operating while still addressing the underlying issues that led to the original dissolution process.

Ramirez suggests that instead of dissolving the corporation, an alternative approach could be to "remove the directors and officers of the corporation."¹³¹⁶ Ramirez's proposal for a "corporate death penalty" is designed to deter managers from abusing their authority to engage in systematic criminal activity. The idea is that by removing these individuals from their roles, their control over corporate assets would be eliminated. This goal can be achieved either through the formal dissolution of the corporation or through the simple removal of the management, both of which achieve the intended remedial purpose.¹³¹⁷

¹³¹⁵ See e.g., Noonan, "Federal Corporate Charter Revocation", *supra* note 1294 at 628; Hulpke, "A Corporate Death Penalty?", *supra* note 1297 at 3.

¹³¹⁶ Ramirez, "Science Fiction of Corporate Criminal Liability", *supra* note 1291 at 975.

¹³¹⁷ See Ramirez, "Science Fiction of Corporate Criminal Liability", *supra* note 1291 at 975–76.

While Ramirez’s proposal aims to achieve accountability, it falls short of addressing the broader problem that the framework proposed in this thesis seeks to address. The purpose of corporate dissolution under the proposed framework is to pose a serious, existential threat to the corporation itself, thereby limiting its pathological tendencies. This would make compliance with the duty to limit revenue streams a priority for corporations, even if it temporarily reduces their profit margins. In cases where a corporation continues to ignore the duty to limit revenue streams, and continues to profit from the sale of technologies, products, or services that either facilitate, are based on, or are enhanced by the collection or processing of behavioural data surpluses, removing individual managers, as Ramirez suggests, may not be enough. The corporation would continue to operate and the systemic problems would remain. A more drastic measure, such as the dissolution, is needed to ensure that the corporation, not just its management, faces real consequences for continued non-compliance.

Instead, in cases where the Committee determines that the dissolution of the corporation would be detrimental to the public interest, it could propose that the corporation be converted to a different legal structure, such as a not-for-profit,¹³¹⁸ cooperative,¹³¹⁹ or hybrid model.¹³²⁰ This approach would effectively end the corporation in its current form, thereby fulfilling the intended purpose of the remedy while ensuring the continuation of its essential functions. Given the

¹³¹⁸ See e.g., C Callard, D Thompson & N Collishaw, “Transforming the Tobacco Market: Why the Supply of Cigarettes Should be Transferred from For-Profit Corporations to Non-Profit Enterprises with a Public Health Mandate” (2005) 14:4 Tobacco Control 278–283.

See also Charlie Cray & Lee Drutman, “Corporations and the Public Purpose: Restoring the Balance” (2005) 4:1 Seattle Journal for Social Justice 305 at 331–33.

¹³¹⁹ See e.g., Oier Imaz, Fred Freundlich & Aritz Kanpandegi, “The Governance of Multistakeholder Cooperatives in Mondragon: The Evolving Relationship among Purpose, Structure and Process” in Sonja Novković, Karen Miner & Cian McMahon, eds, *Humanistic Governance in Democratic Organizations: The Cooperative Difference* (Cham: Springer International Publishing, 2023) 285.

¹³²⁰ See e.g., Carol Liao, “Disruptive Innovation and the Global Emergence of Hybrid Corporate Legal Structures” (2014) 11:2 European Company Law 67.

importance of the role of the corporation in society, it is crucial that this transition is completed as soon as possible. The framework should, therefore, provide for a specific timeframe, such as a maximum of two years, for the completion of the process.

The process would begin with the Committee preparing an initial transition plan and submitting it to the Court. This plan should be developed in consultation with the corporation's employees and shareholders. The plan should aim to preserve the majority of jobs and technologies that are essential to society, while transitioning the business model away from any reliance on the sale of technologies, products, or services that either facilitate, are based on, or are enhanced by the collection or processing of behavioural data surpluses for profit.

The first option should be to modify the technologies, services, or products so that they do not facilitate, are not based on, or are not informed or enhanced by the processing of behavioural data surpluses. If such modification is not feasible, the plan should include discontinuing certain products or services altogether. In addition, the plan must address the interests of shareholders by providing for either a phased compensation plan or, depending on the new legal structure, the conversion of their shares into membership rights in a cooperative or shares in the chosen hybrid model.

If the court approves this initial plan, it would order the transition to the alternative legal structure and appoint a person to oversee the process. This person should be experienced in the chosen structure and should work closely with representatives of the corporation's employees and shareholders to implement the transition plan. Any changes to the plan would require court approval.

C. Adoption of the Proposed Framework

Given the transnational activities of corporations that derive revenue from the sale of technologies, products or services that facilitate, are based on, or are enhanced by the collection or processing of behavioural data surpluses, it would be desirable for the proposed framework to be adopted by as many jurisdictions as possible. Widespread adoption will help to prevent “jurisdiction shopping,” where corporations choose to operate in regions with the most lenient regulations.¹³²¹

However, given the complexity of this regulatory reform—which will require changes to corporate law, particularly in the areas of corporate purpose, duties, financial reporting requirements, and liquidation and dissolution procedures—it may be prudent to begin implementation in a limited number of jurisdictions. This initial phase will provide an opportunity to assess the effectiveness of the framework, identify areas for improvement, and make any necessary adjustments. As a testing ground, this phased approach will provide valuable insights into its practical application and allow for the resolution of unforeseen challenges before the Framework, or a modified version of it, is recommended for wider international adoption.

It is important to emphasize that the proposed framework seeks to limit the ability of corporations to engage in mass dataveillance by regulating business models that rely on behavioural data surpluses. This framework should therefore be seen as complementary to existing data protection rules, which will continue to govern the processing of all other types of data (i.e., essential behavioural data and personal data).

Below is the model text of the proposed legal framework, which is intended as a basic template that can be adapted to the specificities of different legal systems.

¹³²¹ See Smith, “Response”, *supra* note 1144 at 1008.

A Corporate Law Reform to Limit Corporate Mass Dataveillance Capabilities.

Clause 1. The section on corporate purpose should be amended to include the following text:

The purpose of the corporations is to create sustainable value for the benefit of all stakeholders, including shareholders, employees, customers and communities. Corporations should seek to balance the pursuit of profit with their responsibilities to society by ensuring that their activities, including the development and use of technology, contribute positively to the well-being of all stakeholders.

Clause 2. The section on corporate duty should be amended to include the following text:

Duty to Limit Revenue Streams

(1) All corporations have a duty to ensure that their revenues are not derived from the sale of technologies, products, or services that either facilitate, are based on, or are informed or improved by the collection or processing of behavioural data surpluses.

(1.1) For the purposes of this duty, “behavioural data surpluses” should be understood as any data generated by an individual’s interactions with a technology that goes beyond what it is necessary to improve the technology, service, or product. This could include, but is not limited to:

- *Data from online activities, such as browsing history, clicks, social media interactions, and similar activities.*
- *Data from offline activities, such as location tracking through mobile devices, and other forms of physical tracking*
- *Data derived from the use of connected devices, such as the Internet of Things devices and similar technologies.*

Annual Financial Statement

(2) Corporations are required to include in their annual financial statements a detailed breakdown of all revenue streams. These streams shall be categorized as follows:

- *Revenue from data-driven activities*
- *Revenue from non-data-based activities,*

In addition, corporations must clearly link the use of data to specific revenue streams.

Offence

(3) *A corporation that, without reasonable cause, fails to comply with the duty under subsection (1) or the reporting requirements under subsection (2) shall be sanctioned by [the public authority].*

Requests for missing information

(4) *If a corporation fails to provide the information required under subsection (2), or provides incomplete information, [the public authority] shall issue a notice requesting the missing or corrected information. The corporation will be given a compliance period of 2–3 weeks from the date of the notice to provide the required information.*

Failure to comply after notice

(5) *If the corporation fails to comply within the initial compliance period, the regulator may:*

- *Impose a penalty*
- *Give the corporation a final compliance period to remedy the non-compliance.*

Continued non-compliance

(6) *If the corporation remains non-compliant after the final compliance period, this non-compliance will be considered a third strike and will trigger the dissolution of the corporation as outlined in section [Y].*

Penalties for failure to comply with the duty to limit the source of profits

(7) *If a corporation submits complete information but is found by [the public authority] to have failed to comply with the duty established in subsection (1), [the public authority] may require the corporation to forfeit any profits derived from prohibited data practices. Such non-compliance shall be considered as a first strike.*

(8) *In addition to penalties, [the public authority] shall require the corporation to adjust its business model to achieve compliance with subsection (1). The corporation would have a maximum of one year to make the necessary adjustments.*

Periodic reporting requirements

(9) *During the period of business model adjustment, the corporations shall report regularly to [the public authority] on the steps it is taking to ensure compliance. [The public authority] shall determine the frequency and content of these reports in order to monitor progress effectively.*

Strikes for non-compliance

(10) *Failure to provide the required periodic reporting or failure to adjust the business model within the specified timeframe will each count as one of the three strikes for non-compliance as outlined in Section [Y].*

Public register of compliance

(11) Each case of non-compliance with the duty to limit revenue streams shall be recorded by [the public authority] in a publicly accessible register on the authority's website. The register shall include information on any penalty imposed and whether dissolution proceedings have been initiated.

Clause 3. The section on the dissolution of corporations should be amended to include the following text:

(1) [the public authority] may dissolve a corporation after a third penalty for failure to comply with the duty to limit revenue streams established in Section [X].

(2) Any citizen or group of citizens may initiate dissolution proceedings before the competent court if, according to the public register established in section [X], the corporation has been sanctioned three or more times and [the public authority] has not initiated dissolution proceedings against that corporation.

Clause 4. The section on dissolutions should be amended to include the following subsection:

Dissolution Procedure in the event of non-compliance with the duty to limit revenue streams

Establishment of an Oversight Committee

(1) A committee composed of members of [the public authority] shall be appointed to oversee the dissolution process of a corporation. The members of the committee shall have expertise in the corporation's industry and a thorough understanding of the corporation's upstream and downstream relationships.

Committees' Decisions

(2) The Committee shall have the power to make one of two decisions:

(i) If the Committee determines that dissolution is appropriate, it shall recommend to the court that the corporation be dissolved and request the commencement of liquidation proceedings.

(ii) If the Committee determines that the dissolution of the Corporation would be detrimental to the public interest, it may recommend that dissolution proceedings be discontinued. In such a case, the Committee shall propose that the Corporation be converted to an alternative legal structure as set out in sections 7 to 14.

(3) In determining whether the dissolution would be detrimental to the public interest, the Committee shall take into account factors including, but not limited to, the following

- *Potential loss of jobs.*
- *The economic impact on the community or industry.*
- *The dependence of society on the technologies, services, or products of the corporation.*

Approval by the Court

(4) Any decision by the Committee, whether to proceed with the dissolution or to convert the Corporation to another legal structure, will require the final approval of a court. The Court shall review the Committee's recommendations to ensure that they are consistent with legal standards and the public interest.

(5) The Committee shall document its findings and recommendations in a detailed report to be submitted to the court for review. The report should include the reasons for the decision, the factors considered, and the proposed course of action.

(6) The Court shall have the power to accept, modify or reject the recommendations of the Committee on the basis of its assessment of the public interest and legal considerations. The decision of the Court shall be final and binding.

Procedure if the Corporation is not Dissolved

(7) If the Committee concludes that the dissolution of the Corporation would be contrary to the public interest, it may propose that the Corporation be converted to another legal structure. Possible alternatives include a not-for-profit organization, a cooperative model or a hybrid model.

(8) In such cases, the Committee shall develop a transition plan in consultation with representatives of the employees and shareholders of the corporation to ensure that the interests of all stakeholders are aligned.

(9) The transition plan shall seek to:

(i) Preserve the majority of jobs within the corporation;

(ii) Preserve and protect technologies essential to societal interests; and

(iii) Transition the Corporation's business model to eliminate any revenue dependence on the sale of technologies, products, or services that either facilitate, are based on, or are informed by or improve by the collection or processing of behavioural data surpluses for profit.

(10) Upon completion, the Committee shall submit the transition plan to the Court for review. This transition plan should include the rationale for the decision, the factors considered, and the proposed course of action.

(10.1) If the Court finds that the plan is consistent with the purposes of this Act, it shall approve the plan and issue an order to commence the transition to the alternative legal structure.

(10.2) Upon approval of the transition plan, the Court shall appoint an Overseer to supervise and facilitate the implementation of the transition plan.

(10.3) The overseer shall have proven experience in the designated legal structure and shall work with designated representatives of the corporation's employees and shareholders to implement the transition plan.

(11) The transition process shall be completed within a maximum of two (2) years from the date of the court's approval of the transition plan.

Reporting Requirements of the Overseer

(12) The Overseer shall submit a report to the Court on the progress of the transition plan one year after the start of the transition process. This report shall include a detailed timetable setting out what has been implemented and identifying any outstanding tasks.

(13) Any amendments to the initial transition plan shall require the prior approval of the Court.

(14) The Court shall have the power to accept, modify or reject any proposed amendments to the initial transition plan on the basis of public interest and compliance considerations. The decision of the Court shall be final and binding.

Clause 5. The provisions of this new framework shall take effect two years after its entry into force.¹³²²

¹³²² This is a similar period to that given between the entry into force of the GDPR and its application. *GDPR, supra* note 66 art 99(2).

III. Limits and Possible Critiques of the Proposed Framework

This final section explores some of the possible criticisms and limitations of the proposed framework, focussing on how the proposed regulation might affect different types of innovation, the logistical challenges it poses for regulators, and the broader systemic and political factors that may limit its effectiveness. Understanding these limitations provides a fuller picture of the potential impact of the framework, and highlights areas where further structural reforms may be needed to achieve meaningful corporate accountability.

The proposed duty for corporations to limit their revenue streams may have a significant impact on innovation, particularly in data-intensive sectors. By limiting the collection and processing of behavioural data surpluses as a potential revenue stream, the proposed regulatory framework can be seen as limiting innovation in these sectors. This critique will be consistent with broader debates about the relationship between innovation and regulation, where regulation is usually conceptualized as limiting innovation because it imposes additional costs on corporations, which in turn may reduce investment in their research and innovation departments.¹³²³

A critical issue in this debate is the definition of innovation, how it is measured, and what types of innovation might be affected by such regulations. In this regard, Tal Z. Zarsky explains that innovation can be divided into two groups: market-innovation and social-innovation. Market-innovations are developments that enable corporations to create new or improve products or services that are of interest to consumers. These innovations benefit the corporation, which can

¹³²³ See e.g., Bakan, *New Corporation*, *supra* note 5 at 105–06; Anu Bradford, “The False Choice Between Digital Regulation and Innovation” (2024) 119:2 *Northwestern University Law Review* 377; Marietje Schaake, “Lobbying for Unfettered Innovation is Bad for Democracy”, *Financial Times* (24 September 2024), online: <ft.com> [<http://web.archive.org/web/20240924040335/https://www.ft.com/content/ab2761bd-ace7-428b-aa3e-b7412ef69b48>].

capitalize on them through the sale or use of such products and services. However, these benefits often remain within the corporation and do not necessarily extend to society as a whole.¹³²⁴ In contrast, social-innovations refer to practices that create societal benefits that corporations may not be able to capitalize on directly, but which are instead distributed to users and customers through positive externalities, wealth redistribution, or alternative means.¹³²⁵

Taking these categories into account, the proposed framework will indeed limit certain types of market-innovation by reducing corporations' revenues from certain technologies, services or products. However, by limiting the ability of corporations to engage in mass dataveillance—and thereby mitigating some of the privacy and human rights concerns associated with these practices—the framework could actually encourage social-innovation. In addition, it could be argued that this regulation could encourage corporations to develop new technologies, services, and products that do not rely on behavioural data surpluses. Such a shift could, in the long run, stimulate alternative forms of market-driven innovation as corporations adapt to new revenue needs or pursue new business models.

Beyond the innovation-related criticisms, another limitation of the proposed framework is the fine line between essential behavioural data and behavioural data surplus. Behavioural data, or metadata, are the data generated by an individual's interactions with technology. Under the proposed framework, the use of behavioural data that are necessary for the functioning and improvement of the service or product remains permissible.¹³²⁶ However, the framework seeks to limit the collection and processing of behavioural data surpluses—additional metadata collected and processed beyond what is necessary for the functioning and improvement of the products or

¹³²⁴ See Tal Z Zarsky, "The Privacy-Innovation Conundrum" (2015) 19:1 Lewis & Clark Law Review 115 at 126.

¹³²⁵ See Zarsky, "Privacy-Innovation Conundrum", *supra* note 1324 at 126–27.

¹³²⁶ See Part I-B.3, *above*.

services.¹³²⁷ This distinction is likely to require case-by-case analysis, as different technologies, services, and products have different data needs.

For regulators, making such distinctions may require cooperation from the corporation selling the technology, service, or product being analyzed, including possible access to design details, data collection practices, or even the underlying code. Obtaining this level of cooperation may be challenging, as corporations may resist this level of transparency if it threatens their revenues. It will also require that the regulatory agency responsible for implementing the framework has the resources, i.e., the technical knowledge, the appropriate staff (in terms of skills and numbers), the necessary technology, and the financial capacity, to carry out such analysis.

Another limitation to the implementation and wider adoption of this framework is the willingness, or lack of it, of governments and legislators to limit the amount and type of data that corporations are allowed to collect and process. As noted above, governments have shown an interest in corporations' ability to collect rich data about individuals and their behaviour, as these data represents a valuable resource that governments can potentially access.¹³²⁸ This dynamic creates a tension: while the proposed framework seeks to limit corporate mass dataveillance, government interest in accessing corporate data may undermine the effectiveness of regulation.

A partial solution to these limitations is a broader reform of the economic systems and existing priorities, as well as the strengthening of democratic institutions and processes. For instance, strengthening grassroots movements and supporting representatives who are less susceptible to corporate influence could improve the effectiveness of regulations aimed at limiting

¹³²⁷ See Part I-B.3, and Part II-A.2.a, *above*.

¹³²⁸ See Part II-B.1, and Chapter IV-III.C, *above*.

corporate power.¹³²⁹ In addition, raising public awareness of the societal costs of data exploitation could mobilize public support for stronger data governance policies.

It is important to note that this proposed framework does not fundamentally change the profit-driven nature of corporations, which can often lead to exploitative practices. Rather, it is a targeted intervention aimed at addressing specific harms and risks associated with mass dataveillance systems. While broadening the purpose of corporations beyond profit maximization is a first step towards curbing the more harmful behaviours of corporations,¹³³⁰ further restrictions on profit-making models may still be needed. Therefore, future policy efforts could explore additional ways to limit revenue models that rely on behaviour that is detrimental to the communities in which corporations operate, to promote corporate accountability, and to prioritize societal well-being over profit maximization.

In summary, while the proposed framework represents an important step towards mitigating the risks associated with corporate mass dataveillance, it is not without its limitations. The framework's potential to restrict market-driven innovation in certain sectors is a legitimate concern, although it may also encourage alternative forms of social-innovation that prioritize the public good. Effective implementation of such provisions will require significant resources, corporate transparency and political will—factors that are difficult to achieve in the current economic and political landscape. For this framework to reach its full potential, it may need to be supported by broader economic reforms and strengthened democratic processes.

¹³²⁹ See Bakan, *New Corporation*, *supra* note 5 at ch 6; Waldman, *Industry Unbound*, *supra* note 15 at ch 6.

¹³³⁰ See Part II-A.1, *above*.

IV. Conclusions

This thesis has argued that current data protection frameworks are insufficient to effectively regulate corporate mass dataveillance systems and the risks they pose to privacy and other human rights. To address this, this chapter has argued that a new regulatory approach is needed. This approach should aim to constrain corporate mass dataveillance capabilities by limiting business models that rely on the collection and processing of behavioural data surpluses, as it is the profitability of these data that has incentivized the development and deployment of mass dataveillance systems.

Given the pathological personality of the corporation, this chapter has proposed a regulatory framework aimed at modifying certain aspects of the institutional nature of the corporation. More specifically, the framework targets two aspects of the corporation's legal structure of that have contributed to its pathological personality.

The first aspect can be described as the combination of three elements: a corporate purpose focussed solely on making a profit, a duty that compels directors to prioritize profit maximization, and an internal legal structure that imposes few, if any, restrictions on how this purpose is pursued. The second aspect is the lack of real consequences for the corporation's own existence. This has meant that for a corporation, compliance with the law is simply a question of costs and benefits.

The proposed framework has two key features. First, it sets clear limits on how corporations can generate revenue, by broadening the corporate purpose and introducing a duty to limit revenue streams derived from behavioural data surpluses. These two changes are designed to shift the focus of corporations away from profit maximization, and place clear limits on how corporations may generate revenue. Second, it creates a real threat to the existence of corporations by introducing the mandatory dissolution of the corporation in cases of non-compliance. This

embodies the idea that if and when corporations decide not to obey the law and become a danger to society, the government that granted them the right to do business has the power to revoke that right. Rather than of imposing penalties that corporations see as part of the cost of doing business, governments should use their power to revoke the right of corporations to exist and operate.

While the framework faces potential challenges in implementation and may limit certain forms of market-driven innovation, it represents an important step towards limiting corporate mass dataveillance capabilities and protecting privacy rights. Further research is needed on the practical implications and potential refinements as jurisdictions begin to adopt such measures.

It is important to emphasize that, as Bennet Mosses points out, the perspective adopted here is that of a legal scholar.¹³³¹ Effective regulation of corporations requires an interdisciplinary approach that incorporates the insights and expertise of professionals from fields such as economics, engineering, sociology, and the input of civil society. All of these perspectives are essential, for example, in identifying the best way to implement regulations without compromising social and economic stability due to the dominance of some of these corporations with a data-driven business model in the global economy and society.

It is also important to consider that practical challenges such as political will and corporate pressure must be addressed for any new regulation to significantly change the current system. In this sense, corporate mass dataveillance capabilities are only a small part of the larger problem of regulating of corporate power, which is exacerbated by the pathological nature of the corporation as a legal entity.

¹³³¹ See Bennett Moses, “How to Think about Law, Regulation and Tech”, *supra* note 18 at 20.

The following chapter, which is the concluding chapter, will summarize the argument of this thesis, highlighting its significance and contributions, and then explain the limitations of this thesis and set out questions for future research.

Chapter VII. Conclusions

To return to the Frankenstein analogy mentioned in the introductory chapter, if corporations are the government's Frankenstein creation, then the regulatory systems should be designed "to keep the Frankenstein monster on a chain and stop it from causing harm."¹³³² The nature of the regulation, the assumptions under which it is enacted, and its enforcement mechanisms are key to ensuring that it achieves its goal of protecting and promoting the public interest by stopping corporations from doing harm.¹³³³ In the case of corporations with a data-based business model, there have been several attempts to regulate them without much success.

This thesis has examined whether existing data protection frameworks, as the predominant choice for regulating corporate data practices, are sufficient to regulate and monitor corporate data practices in the current socio-technical landscape, and therefore adequate for states to fulfill their obligations under international human rights law, including the ICCPR, or whether a new framework is required instead. Using location mass dataveillance systems as a concrete example, this analysis identified significant limitations in current regulatory approaches and proposed a new framework to more effectively constrain corporate mass dataveillance.

This thesis builds on a significant body of existing literature that recognizes the inadequacies of data protection as the primary mechanism for curbing the mass dataveillance powers of corporations and for protecting the privacy of individuals and society.¹³³⁴ Scholars have long criticized data protection laws for their limited scope and effectiveness, often pointing out

¹³³² Bakan, *The Corporation*, *supra* note 1 at 166.

¹³³³ See Bakan, *The Corporation*, *supra* note 1; Waldman, *Industry Unbound*, *supra* note 15 at 237.

¹³³⁴ See Chapter II.I.B Specific Critiques of Data Protection Regulation, *above*.

that these regulations fail to address the root causes of privacy invasions and corporate overreach. They argue that data protection frameworks, while necessary, are insufficient in the face of rapidly advancing technologies and the pervasive data collection practices of corporations with data-based business models.¹³³⁵

This thesis differs from these scholars in its focus on corporate law reform to address these issues. By incorporating Bakan's concept of the corporation as having a psychopathic personality,¹³³⁶ this approach shifts the responsibility away from individuals, who are often burdened with managing their own privacy, to governments that have the authority and capacity to impose and enforce comprehensive regulatory measures on corporations.

Bakan's characterization suggests that corporations, by their very nature, prioritize profit over ethical and legal considerations, including human rights. This perspective provides insight into why corporations with data-driven business models persistently undermine data protection regulation in the pursuit of profit, and underscores the need for a regulatory framework that takes into account the pathological personality of the corporation in order to adequately regulate corporate mass dataveillance capabilities.

This concluding chapter is divided into two main parts. The first part summarizes the argument of this thesis and highlights its significance and contributions. The second part explains the limitations of this thesis and identifies areas for future research.

¹³³⁵ See Chapter II.I.B Specific Critiques of Data Protection Regulation, *above*.

¹³³⁶ See Chapter IV.I. Corporations as Psychopathic Institutions, *above*.

I. Summary and Contributions

According to the analytical lens proposed by Bennet Mosses and adopted as the methodology in this thesis, the “primary issue for regulators is not the need to ‘regulate technology’ but the need to ensure that laws and regulatory regimes are well adapted to the socio-technical landscape in which they operate, which change over time.”¹³³⁷ Within this framework, therefore, the first step was to define the current socio-technical landscape and determine whether it warranted a regulatory response.

The main features of the socio-technological landscape explored in this thesis can be summarized in two main aspects.¹³³⁸ First, the widespread adoption of digital technologies has facilitated the mass dataveillance of individuals by corporations. These technologies make it easy to generate, collect, and process vast amounts of data about individuals and their behaviour. For instance, they make it possible to automatically track the location and movements of individuals using data generated by the mobile devices that people use every day. The ability to quickly analyze these data has also made it possible to identify patterns in people’s movements and draw inferences about their lifestyles.¹³³⁹

Second, corporations not only have the capacity for mass dataveillance, but it has become extremely profitable for them to engage in such practices. As a result, corporations with data-based business models are constantly collecting and processing data about individuals and their behaviours. They monetize these data by directly selling them or by analyzing them to provide

¹³³⁷ Bennett Moses, “Regulating Sociotechnical Change”, *supra* note 152 at 577.

¹³³⁸ See Bennett Moses, “Why Have a Theory of Law & Tech Change?”, *supra* note 154 at 598; Bennett Moses, “Recurring Dilemmas”, *supra* note 156 at 245–46.

¹³³⁹ See Chapter III.I, B Location Technologies and Surveillance, *above*.

personalized inputs to individuals. These inputs are designed to change an individual's behaviour in ways that generate more data, perpetuating the cycle of mass dataveillance and profit.¹³⁴⁰

This socio-technical landscape warrants a regulatory response because it generates risks for individuals and democratic institutions. First, the vast pool of data about individuals and their behaviours is accessible not only to the corporation collecting the data but also to governments, paying customers, and hackers. Second, corporate systems of mass dataveillance serve as an important source of wealth for corporations, giving them considerable economic power to influence democratic institutions. Finally, corporations' direct access to individuals through the same devices and services they use to collect data, raises concerns about the manipulation of information, potentially affecting individuals' ability to form and develop independent opinions, access impartial information, and ultimately posing a threat to democratic processes.¹³⁴¹

Having assessed the current socio-technical environment and conclude that regulation is warranted, the next step in the methodology was to analyze the regulatory objectives and assumptions of the existing regulations. This analysis aimed to determine whether these regulations remain relevant and compatible with the current socio-technical landscape.¹³⁴²

The responsibility of states to implement appropriate regulatory framework may be rooted in international law. For instance, according to Article 2(2) of the ICCPR requires states to protect individuals from interference with their rights by both state and private actors, including

¹³⁴⁰ See Chapter IV.III.B. Corporate Dataveillance Systems and Surveillance Capitalism, *above*.

¹³⁴¹ See Chapter IV.III.B. Corporate Dataveillance Systems and Surveillance Capitalism, *above*.

¹³⁴² See Bennett Moses, "How to Think about Law, Regulation and Tech", *supra* note 18; Brownsword, "So What Does the World Need Now?", *supra* note 146 at 26–30; Brownsword, *Rights, Regulation, and the Technological Revolution*, *supra* note 151 at ch 6.

corporations. As part of this obligation, many states have enacted data protection regulations as the legal mechanism to oversee the data collection and processing activities of corporations.¹³⁴³

However, current data protection frameworks, such as GDPR and PIPEDA, are outdated as their regulatory objectives and assumptions do not adequately address the risks and harms posed by digital technologies in the evolving socio-technical landscape. These frameworks were created with the goal of fostering trust and promoting a data-based economy. To achieve this goal, they were enacted on the assumption that the collection and processing of data about individuals and their behaviours by corporations is a necessary and acceptable practice to promote a data-based economy.¹³⁴⁴

This underlying assumption poses a significant challenge to the regulation of corporate mass dataveillance capabilities, because by assuming that the collection and processing of data about individuals are a necessary and acceptable practice, these regulations lack the legal tools to assess whether the collection and processing of the data are desirable in the first place, leaving this decision entirely up to corporations. Moreover, these frameworks assume that corporations with a data-based business model will willingly change their behaviour to comply with regulations and protect the rights of their users, even at the expense of their profits. However, this assumption overlooks the pathological nature of corporations, their self-interested motivations, and their primary focus on profit maximization.¹³⁴⁵

Due to the disconnect between the goals and assumptions of current data protection regulation and the evolving socio-technical landscape, these regulations fail to effectively regulate

¹³⁴³ See Chapter V.I. States' Duty to Regulate Corporate Mass Dataveillance and Data Protection Regulations, *above*.

¹³⁴⁴ See Chapter V.I.A. Assumption 1: Data Must Be (Are) Collected and Processed by Corporations, *above*.

¹³⁴⁵ See Chapter V.I.B. Assumption 2: Corporations are Benevolent, *above*.

corporate mass dataveillance capabilities, and thus fall short of states' responsibilities under Article 2(2) of the ICCPR. Consequently, states have a duty to establish a new regulatory framework that specifically addresses corporate mass dataveillance and makes it specific and exceptional, rather than the *status quo*, as is currently the case.

To this end, this thesis proposed a regulatory framework to impose limits on the business model and pathological personality of corporations by modifying existing corporate law. The proposed framework seeks to address the issue of corporate mass dataveillance capabilities by targeting both the developers of the technologies that enable corporate mass dataveillance and the corporations that choose to rely on these practices.¹³⁴⁶

The proposed regulatory framework targets two key aspects of the institutional nature of corporations that have contributed to their pathological personality. The first aspect can be described as the combination of three elements: a corporate purpose focussed solely on making a profit, a duty that compels directors to prioritize profit maximization, and an internal legal structure that imposes few, if any, restrictions on how this purpose is pursued. The second aspect is the lack of real consequences for the corporation's own existence. This has meant that, for a corporation, compliance with the law is simply a question of costs and benefits.¹³⁴⁷

To address these two aspects, the proposed framework introduces a two-part approach. First, it places clear limits on the ways in which corporations can generate revenue by broadening the corporate purpose and introducing a duty to limit revenue streams derived from behavioural data surpluses. These two changes aim to shift the focus of corporations away from profit maximization and place clear limits on how corporations can generate revenue.¹³⁴⁸ Second, it

¹³⁴⁶ See Chapter VI.I.B. Regulatory Goal and Target *above*.

¹³⁴⁷ See Chapter VI.II. Limiting Corporate Dataveillance: Essential Features, *above*.

¹³⁴⁸ See Chapter VI.II.A.2. Corporate Duties: Limiting How Corporations Can Generate Profit, *above*.

creates a real threat to the existence of corporations by introducing mandatory dissolution of the corporation in the event of non-compliance. This embodies the idea that if and when corporations decide not to obey the law and become a danger to society, the government that granted them the right to do business has the power to revoke that right.¹³⁴⁹

These recommendations should be seen as part of a wider reform of corporate law, which will require corresponding changes to the duties of corporations. However, because the profitability of corporate mass dataveillance capabilities is at the root of a number of other problems, this thesis calls for the urgent regulation of these systems. The proposed framework aims to regulate these capabilities by dismantling the business model of surveillance capitalism, thereby affecting the profits of corporations that rely on behavioural data surpluses.

This thesis made significant contributions to the field of corporate mass dataveillance and technology regulation. First, by applying Bakan's theory of the corporation to the field of technology regulation in general, and data protection regulation in particular, the analysis in this thesis offered a fresh perspective on the shortcomings of existing regulatory frameworks and provided valuable insights into why current approaches may be inadequate in addressing corporate data practices.

Building on this foundation, the thesis proposed a regulatory framework that goes beyond traditional approaches to regulate corporate data practices. This framework goes beyond data protection principles to address the underlying systemic drivers of corporate mass dataveillance. In doing so, it addresses part of the root cause: the pathological personality that drives corporations to maximize profit above all else, including human rights and social and democratic institutions.

¹³⁴⁹ See Chapter VI.II.B Consequences to Corporations' Own Existence: Mandatory Dissolution, *above*.

In addition, this thesis emphasized the need to consider the “psychopathic personality” of corporations when developing regulatory responses. This perspective is important when considering the regulation of technologies because corporations are key actors in their development, deployment, and implementation. Consequently, this approach suggests that in order to regulate technological change, regulatory strategies need to be tailored to take account of the unique characteristics and motivations of corporations.

By integrating these interrelated ideas, the thesis provided a comprehensive and nuanced approach to addressing the challenges posed by the regulation of corporate mass dataveillance. However, the approach proposed in this thesis could also be applied to other areas of technology regulation. This perspective offers policymakers and researchers a framework for developing regulatory solutions in a constantly evolving socio-technical landscape.

II. Limits and Further Research

The regulation of corporate mass dataveillance is only one critical aspect of the broader issue of corporate power over democratic institutions and societies. While comprehensive regulatory reform is needed to limit and regulate corporate power and its harmful tendencies, protecting the values and rights of democratic societies is a complex challenge. This situation resembles a chicken-and-egg dilemma, as the immense power wielded by corporations in general, and corporations with a data-based business model in particular, seems almost uncontrollable.

Several factors contribute to the difficulty of regulating corporations, including their transnational nature, which makes it difficult for a single national government to regulate them effectively, and their often “good neighbour” image projected onto governments and individuals,

which has led to a push for greater self-regulation.¹³⁵⁰ These challenges raise the question of whether there is a genuine desire to regulate them at all.

From a government's perspective, the problem goes beyond powerful corporate lobbying. Governments may lack the political will to regulate these corporations and their mass dataveillance systems because the data they collected and processed can be a valuable resource. It is often easier and cost-effective for governments to access these data than to collect and process them themselves.¹³⁵¹

As for individuals, mobilizing them to effectively push for government regulation of corporations with mass dataveillance capabilities presents its own set of challenges. Restricting these capabilities would affect the services that individuals rely on, many of which are often provided at no direct monetary cost to the user. This reliance on "free" services is a significant barrier to public support for increased corporate regulation.

The regulation of corporations requires a more structured and comprehensive reform, including a rethinking of the economic system.¹³⁵² In this context, the research carried out by scholars of human right-based economics could provide a good starting point.¹³⁵³ Furthermore, the structural nature of the corporation, which contributes to its pathological personality, is a legal creation and only one of the possible legal forms for promoting technological innovation.

¹³⁵⁰ See Chapter VI. Regulating Corporate Dataveillance in the Face of Socio-technical Change, *above*.

¹³⁵¹ See Chapter IV-III.C, *above*.

¹³⁵² See Bakan, *The Corporation*, *supra* note 1 at 161 ("...the corporations is an institutional reflection of the principles of laissez fair capitalism. Changing it must be understood as part of a larger project of economic change").

¹³⁵³ See e.g., Marianna Leite, "Beyond Buzzwords: Mandatory Human Rights Due Diligence and a Rights-Based Approach to Business Models" (2023) 8:2 Business and Human Rights Journal 197; Radhika Balakrishnan, James Heintz & Diane Elson, *Rethinking Economic Policy for Social Justice: The Radical Potential of Human Rights*, (London: Routledge, 2016); *Rights Based Economy: Putting People and Planet First*, by Kate Donald, (New York: Center for Economic and Social Rights, 2020) online: <<https://www.cesr.org/sites/default/files/Rights%20Based%20Economy%20briefing.pdf>> .

Therefore, future research should also explore alternative forms of legal entities that can promote technological innovation while addressing the current shortcomings of the corporation. As Sjøfjell et al. note in relation to the corporation,

Society has gradually accepted and even promoted the rise to dominance of this business form on the assumption that it contributes significantly to the overarching goal of society—that is, to increasing societal welfare, especially as measured in greater material wealth.¹³⁵⁴

However, this assumption may need to be re-evaluated in the light of the challenges posed by the pathological behaviour of the corporation, and its impact on society as a whole.

Further research is also needed to develop a robust framework for regulating corporations with mass dataveillance capabilities. This research should involve a diverse group of experts from different fields, including sociology, information studies, economics, engineering, and civil society. An interdisciplinary approach is crucial for effective regulation as it enables the integration of insights and expertise from different professional backgrounds, and points of view.

Equally important is the involvement of individuals in this reform process. As Bakan argues, to limiting and regulating corporate power requires public demand for greater government accountability and work to create more participatory democracies. Citizens need to challenge the government, stay informed, and protest when necessary.¹³⁵⁵ However, Bakan also notes that people everywhere are becoming disillusioned with the democratic process and feel that governments have failed them.¹³⁵⁶ To address this issue, it is essential to fund grassroots programs, support community leaders, and empower NGOs.

¹³⁵⁴ Sjøfjell et al, “Shareholder Primacy”, *supra* note 1166 at 79.

¹³⁵⁵ See Bakan, *The Corporation*, *supra* note 1 at 152.

¹³⁵⁶ See Bakan, *The Corporation*, *supra* note 1 at 171.

While this thesis was a small contribution to the larger issue, it argues that limiting the ability of corporations to engage in mass dataveillance is an essential step in any reform. However, the implementation of such a framework must be accompanied by measures that address the dependence of individuals and society on the technologies and services that these corporations provide. While more research is needed, it is equally important to begin implementing limits on these corporations to prevent their continued unchecked growth.

Finally, strengthening democratic institutions is essential for corporate control. This includes ensuring a balance of power and protecting essential institutions, such as a strong and independent public education system, and a free press capable of holding both governments and corporations accountable.

Bibliography

Legislation: Canada

An Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-391.

Canada Business Corporations Act, RSC 1985, c C-44 [CBCA].

Personal Information Protection Act, Alta Reg 366/2003.

Personal Information Protection Act, BC Reg 473/2003.

Personal Information Protection and Electronic Documents Act, SC 2000, c5 [PIPEDA].

Legislation: EU

EU, *Charter of Fundamental Rights of the European Union*, [2012] OJ, C316/26 [EU Charter].

———, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, [1995] OJ, L 281/31 [Directive 95/46/EC].

———, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*, [2002] OJ, L 201/37 [ePrivacy Directive].

———, *Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC Text with EEA relevance*, [2013] OJ, L182/19 [Directive on Corporate Financial Statements].

———, *Directive 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) (Text with EEA relevance)*, [2017] OJ, L169/46 [Directive Regarding Company Law].

———, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention Of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*, [2006] OJ, L105/54 [Data Retention Directive].

———, *Regulation of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC*, [2016] OJ, L 119/1 [GDPR].

Legislation: Other Countries

Code de commerce [C com France].

Companies Act 2006, (UK) [UK Companies Act].

Loi n° 2017-399 du 27 mars 2017, JO, 28 March 2017, no 0074 [*French Duty of Vigilance Law*].

The California Consumer Privacy Act of 2018, c 735, 2018 Cal SB 1121 [CCPA].

Legislation: Regional and International Human Rights Treaties

African Union, *African Charter on the Rights and Welfare of the Child*, July 1990 (entered into force on 29 November 1999).

American Convention on Human Rights, 22 November 1969, OEA Treaty Series No 36 B-12, 1144 UNTS 123 (entered into force: 18 July 1978).

League of Arab States, *Arab Charter on Human Rights*, OHCHR, UN doc [ST/HR/CHR/NONE/2004/40/Rev.1 (2004)].

Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 UNTS 221 (entered into force: 3 September 1953).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, 1496 UNTS 65 (entered into force: 1 October 1981).

Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 3 (entered into force: 2 September 1990).

International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, 18 December 1990, 2220 UNTS 3 (entered into force: 1 July 2003).

Organization of the Islamic Conference, *Cairo Declaration on Human Rights in Islam*, UN doc [ST/GENEVA/OIC/SEM/2002/2 (2002).

Universal Declaration of Human Rights, UNGA, 3rd Sess, UN doc A/810 (1948) GA Res 217A (III).

Jurisprudence: Regional Human Right Courts

InterAmerican Court of Justice

Case of Escher et al (Brazil) (2009), Inter-Am Ct HR (Ser C) No 200.

Case of Tristán Donoso (Panama) (2009), Inter-Am Ct HR (Ser C) 193.

Case of Artavia Murillo et al (“In Vitro Fertilization”) (Costa Rica) (2012), Inter-Am Ct HR (Ser C) No 257.

Case of Members of “José Alvear Restrepo” Lawyers Collective (Colombia) (2023), Inter-Am Ct HR (Ser C) No 506.

European Court of Human Rights

Bărbulescu v Romania [GC], No 61496/08 (5 September 2017).

Ben Faiza c France, No 31446/12 (8 February 2018).

Big Brother Watch and Others v the United Kingdom, No 58170/13 (13 September 2018).

Big Brother Watch and Others v the United Kingdom [GC], No 58170/13 (25 May 2021).

Centrum För Rättvisa v Sweden [GC], No 35252/08 (25 May 2021).

Huvig v France, No 11105/84 (24 April 1990).

Klass and Others v Germany, No 5029/71 (6 September 1978).

Liberty and Others v the United Kingdom, No 58243/00 (1 July 2008).

Malone v the United Kingdom, No 8691/79 (2 August 1984).

Niemietz v Germany, No 13710/88 (16 December 1992).

Peck v the United Kingdom, No 44647/98, [2003] I ECHR 123.

PG and JH v the United Kingdom, No 44787/98, [2001] IX ECHR 195.

Roman Zakharov v Russia [GC], No 47143/06, [2015] VIII ECHR 205.

S and Marper v The United Kingdom [GC], No 30562/04, [2008] V ECHR 167.

Szabó and Vissy v Hungary, No 37138/14 (12 January 2016).

Uzun v Germany, No 35623/05, [2010] VI ECHR 1.

Van Hannover v Germany (no2) [GC], No 40660/08 (7 February 2012).

Weber and Saravia v Germany, No 54934/00, [2006] XI ECHR 309.

Jurisprudence: CJEU

Digital Rights Ireland Ltd and Others [GC], C-293/12, [2014] ECLI:EU:C:2014:238.

Meta Platforms Inc and Others v Bundeskartellamt [GC], C-252/21, [2023] ECLI:EU:C:2023:537.

Tele2 Sverige AB and Others [GC], C-203/15, [2016] ECLI:EU:C:2016:970.

Jurisprudence: Canada

Englander v Telus Communications Inc, 2004 FCA 387.

R v Spencer, 2014 SCC 43.

Wansink v TELUS Communications Inc, 2007 FCA 21.

Jurisprudence: USA

Colopy v Uber Techs Inc, 2019 WL 6841218, (ND Cal 2019).

In re: Facebook Biometric Information Privacy Litigation, 522 F. Supp. 3d 617, (ND Cal 2021).

In re: Facebook, Inc Consumer Privacy User Profile Litigation, Settlement Agreement, 2023 U.S. Dist. LEXIS 182191, (ND Cal 2023).

Luis K Liggett Co et al v Lee, Comptroller et al, 288 U.S. 517, (1933).

Secondary Material: European Union Documents

Commission of the European Communities, *Community Policy on Data Processing*, SEC (73) 4300 final (21 November 1973) online: <<http://aei.pitt.edu/6337/1/6337.pdf>> .

Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No 108 (1981).

Council of the European Union, *Position (EU) No 6/2016 of the council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the*

protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Position, OJ, C 159/1 (2016).

European Commission, *Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*, COM(90) 314 final (13 September 1990) CELEX:51990DC0314.

———, *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century*, White Paper (Luxembourg: Official Publications of the European Communities, 1994).

———, *Report on Europe and the Global Information Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council*, by High Level Group on the Information Society, Bulletin of the European Union Supplement No. 2/94 (1994).

———, *Explanations Relating to the Charter of Fundamental Rights*, OJ, C 303/17 (2007).

———, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, proposal for a regulation, COM(2012) 11 final (2012).

———, *A European Strategy for Data*, COM(2020) 66 final (19 February 2020) CELEX:52020DC0066.

———, “Commission Proposes a Comprehensive Reform of the Data Protection Rules” (25 January 2012) online (Newsroom): ec.europa.eu [https://web.archive.org/web/20120129011210/http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm].

———, “Why Do We Need an EU Data Protection Reform?” (25 January 2012) online (PDF): ec.europa.eu [https://web.archive.org/web/20120227154845/http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf].

———, *Study on Directors’ Duties and Sustainable Corporate Governance: Final Report* (Luxembourg: Publications Office of the European Union, 2020).

- European Parliament, *Protection of Individuals with regard to the Processing of Personal Data*
***I European Parliament Legislative Resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Legislative resolution, OJ C 378, 9.11.2017 (2014).
- EDPB, *Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* (2019).
- , *Opinion 5/2019 on the Interplay Between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities* (2019).
- , *Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service* (5 December 2022).
- , *Binding Decision 4/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Instagram Service* (5 december 2022).
- Irish DPC, *Decision Concerning a Complaint Directed Against Meta Platforms Ireland Limited in Respect of the Facebook Service Made Pursuant to Section 113 of the Data Protection Act 2018*, DPC Inquiry Reference: IN 18-5-5 (31 December 2022).
- , *Decision Concerning a Complaint Directed Against Meta Platforms Ireland Limited in Respect of the Instagram Service Made Pursuant to Section 113 Of the Data Protection Act 2018*, DPC Inquiry Reference: IN 18-5-7 (12 January 2023).
- WP29, *Working Document of Biometrics*, 12168/02/EN WP 80 (2003).
- , *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices*, 811/11/EN WP 185 (2011).
- , *Opinion 15/2011 on the Definition of Consent*, 01197/11/EN WP187 (2011).
- , *Opinion 08/2012 Providing further Input on the Data Protection Reform Discussions*, 01574/12/EN WP199 (2012).
- , *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 844/14/EN WP 217 (2014).
- , *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 14/EN WP 223 (2014).

- , *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679*, WP 248 rev.01 (2017).
- , *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01 (2018).
- , *Guidelines on Consent under Regulation 2016/679*, WP259 rev.01 (2018).
- WP29 & WPPJ, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, 02356/09/EN WP 168 (2009).

Secondary Material: United Nations Documents

- B-Tech, *Addressing Business Model Related Human Rights Risks*, OHCHR (2020) B-Tech Foundational Paper online: [ohchr.org](https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf) [http://web.archive.org/web/20231218140015/https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf].
- , *Bridging Governance Gaps in the Age of Technology: Key Characteristics of the State Duty to Protect*, OHCHR (2021) B-Tech Foundational Paper online: [ohchr.org](https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf) [http://web.archive.org/web/20240722004358/https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf].
- OAS, Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression, *Standards for a Free, Open, and Inclusive Internet*, by Lanza Edison, OEA/Ser.L/V/II CIDH/RELE/INF.17/17 (2017).
- OHCHR, *General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)*, HRC, 32th Sess, UN Doc HRI/GEN/1/Rev.9 (Vol. I) (1988).
- , *The Right to Privacy in the Digital Age*, HRC, 27th Sess, UN Doc A/HRC/27/37 (2014).
- , *Report on Best Practices and Lessons Learned on How Protecting and Promoting Human Rights Contribute To Preventing and Countering Violent Extremism*, HRC, 33th Sess, UN Doc A/HRC/33/29 (2016).
- , *The Right to Privacy in the Digital Age*, HRC, 39th Sess, UN Doc A/HRC/39/29 (2018).
- , *The Right to Privacy in the Digital Age*, HRC, 48th Sess, UN Doc A/HRC/48/31 (2021).
- , *The Right to Privacy in the Digital Age*, HRC, 51st Sess, UN Doc A/HRC/51/17 (2022).

- , *The Practical Application of the Guiding Principles on Business and Human Rights to the Activities of Technology Companies*, HRC, 50th Sess, UN Doc A/HRC/50/56 (2022).
- SRSR, *Protect, Respect and Remedy: A Framework for Business and Human Rights*, by John Ruggie, HRC, 8th Sess, UN Doc A/HRC/8/5 (2008).
- , *Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework*, by John Ruggie, HRC, 17th Sess, UN Doc A/HRC/17/31 (2011).
- UN, *Report of the Special Rapporteur on the Right to Privacy*, by Joseph A. Cannataci, GA, 76th Sess, UN Doc A/76/220 (2021).
- , *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by David Kaye, HRC, 29th Sess, UN Doc A/HRC/29/32 (2015).
- , *Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by Irene Khan, HRC, 47th Sess, UN Doc A/HRC/47/25 (2021).
- , *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, by Frank La Rue, HRC, 23th Sess, UN Doc A/HRC/23/40 (2013).
- , *Hundred and Eighty-Third Plenary Meeting of the UN General Assembly*, GA, 3rd Sess, UN Doc A(01)/R3 (1948) 183th Mtg.
- , *Report of the Human Rights Committee*, GA, 46th Sess, UN Doc A/46/40 (1991) Supplement No 40.
- , *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, HRC, 18th Sess, UN Doc CCPR/C21/Rev.1/Add/13 (2004).
- , *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, by Martin Scheinin, HRC, 13th Sess, UN Doc A/HRC/13/37 (2009).
- , *The Right to Privacy in the Digital Age*, GA, 68th Sess, UN Doc A/RES/68/167 (2013) GA Res 68/167.
- , *Report of Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, GA, 69th Sess, UN Doc A/69/397 (2014).
- , *Report of the Special Rapporteur on the Right to Privacy*, HRC, 34th Sess, UN Doc A/HRC/34/60 (2017).

- , *The Right to Privacy in the Digital Age*, GA, 71th Sess, UN Doc A/RES/71/199 (2017) GA Res 71/199.
- , *The Right to Privacy in the Digital Age*, HRC, 34th Sess, UN Doc A/HRC/34/L.7/Rev.1 (2017) GA Res 34.
- , *The Right to Privacy in the Digital Age*, HRC, 34th Sess, UN Doc A/HRC/RES/34/7 (2017) GA Res 34/7.
- , *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, HRC, 41th Sess, UN Doc A/HRC/41/35 (2019).
- , *The Right to Privacy in the Digital Age*, GA, 73rd Sess, UN Doc A/RES/73/179 (2019) GA Res 73/179.
- , *The Right to Privacy in the Digital Age*, GA, 75th Sess, UN Doc A/RES/75/176 (2020) GA Res 75/176.
- , *Report of the Special Rapporteur on the Right to Privacy*, HRC, 43th Sess, UN Doc A/HRC/43/52 (2020).
- , *General Comment No. 25 on Children's Rights in Relation to the Digital Environment*, CRC, UN Doc CRC/C/GC/25 (2021).
- , *Rules of Procedure of the Human Rights Committee*, HRC, UN Doc CCPR/C/3/Rev.12 (2021).
- UNCHR, *Letter from the Chairman of the Commission on Human Rights to the President of the Economic and Social Council*, ECOSOC, UN Doc E/383 (1947).
- , Drafting Committee, *International Bill of Rights Documented Outline. Part I*, UN Doc E/CN.4/AC.1/3/Add.1 (1947).

Secondary Material: Canadian Government Documents

- House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*, (February 2018) (Chair: Bob Zimmer).
- , Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, (December 2018) (Chair: Bob Zimmer).
- , *Submissions on Bill C-27 The Digital Charter Implementation Act*, 44-1 (5 October 2023) (Brief submitted by Jane Bailey, Jacquelyn Burkell, and Brenda McPhail) online:

[ourcommons.ca](https://web.archive.org/web/20240214183340/https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605252/br-external/Jointly3-e.pdf)

[<https://web.archive.org/web/20240214183340/https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605252/br-external/Jointly3-e.pdf>].

Industry Canada and Justice Canada, *The Protection of Personal Information: Building Canada's Information Economy and Society*, by Task Force on Electronic Commerce, (Ottawa: IC, 1998) online: [e-com.ic.gc.ca](http://web.archive.org/web/20001012101540/http://www.e-com.ic.gc.ca/english/privacy/acroeng.pdf) [<http://web.archive.org/web/20001012101540/http://www.e-com.ic.gc.ca/english/privacy/acroeng.pdf>].

Information and Privacy Commissioner Ontario, *Privacy and Biometrics*, by Ann Cavoukian, (Toronto: IPC-ON, 1999).

———, *Privacy and Radical Pragmatism: Change the Paradigm*, by Ann Cavoukian, (white paper) (Toronto: IPC-ON, 2008).

———, *Redesigning IP Geolocation Privacy by Design and Online Targeted Advertising*, by Ann Cavoukian, (Toronto: IPC-ON, 2010).

———, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, by Ann Cavoukian & Marilyn Prosch, (Toronto: IPC-ON, 2010).

———, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers.*, by Ann Cavoukian, (Toronto: IPC-ON, 2014) online: [ipc.on.ca](http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf) [<http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>].

———, *Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design*, by Ann Cavoukian & Drummond Reed, (Toronto: IPC-ON, 2014) online: [ipc.on.ca](http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf) [<http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>].

———, *Privacy by Design: From Rhetoric to Reality* (Toronto: IPC-ON, 2014) online: [ipc.on.ca](http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf) [<http://web.archive.org/web/20220205025703/https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf>].

Innovation, Science and Economic Development Canada, “Bill C-27 Summary: Digital Charter Implementation Act, 2022” (18 August 2022) online: [ised-isde.canada.ca](https://web.archive.org/web/20231220102246/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020) [<https://web.archive.org/web/20231220102246/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020>].

- , “Canada’s Digital Charter” (13 March 2023) online: <ised-isde.canada.ca> [http://web.archive.org/web/20231220101549/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world].
- , “Consumer Privacy Protection Act” (13 March 2023) online: <ised-isde.canada.ca> [http://web.archive.org/web/20231220101915/https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act].
- , “Strengthening Privacy for the Digital Age” (21 May 2019) online: <ised-isde.canada.ca> [http://web.archive.org/web/20231220102053/https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/strengthening-privacy-digital-age].
- , “Individuals with Significant Control” (26 February 2024) online: <ised-isde.canada.ca> [http://web.archive.org/web/20240605184701/https://ised-isde.canada.ca/site/corporations-canada/en/individuals-significant-control-file-your-information].
- , “Corporations Canada: About Us” (28 May 2024) online: <ised-isde.canada.ca> [http://web.archive.org/web/20240712120907/https://ised-isde.canada.ca/site/corporations-canada/en/about-us].
- Office of the Privacy Commissioner of Canada, *Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices*, (consultation paper) (Ottawa: OPC, 2008).
- , *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act*, by Policy and Research Group, (Ottawa: OPC, 2016) online: <[priv.gc.ca](https://www.priv.gc.ca)> [http://web.archive.org/web/20231219165225/https://www.priv.gc.ca/media/1806/consent_201605_e.pdf].
- , *2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (Ottawa: OPC, 2017).
- , “Applying Paragraphs 7(3)(d1) and 7(3)(d2) of PIPEDA” (17 March 2017) online: <[priv.gc.ca](https://www.priv.gc.ca)> [http://web.archive.org/web/20231219173548/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/gd_d1-d2_201703/].
- , *2019-20 Departmental Plan* (Ottawa: OPC, 2019).

- , “PIPEDA Fair Information Principles” (May 2019) online: <[priv.gc.ca](http://web.archive.org/web/20231219174928/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/)> [http://web.archive.org/web/20231219174928/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/].
- , “Provincial Laws that May Apply instead of PIPEDA” (May 2020) online: <[priv.gc.ca](http://web.archive.org/web/20231219174406/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/)> [http://web.archive.org/web/20231219174406/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/].
- , *Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report*, by Ignacio Cofone, (2020) online: <[priv.gc.ca](http://web.archive.org/web/20231219145750/https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/)> [http://web.archive.org/web/20231219145750/https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011].
- , “PIPEDA Fair Information Principle 1: Accountability” (August 2020) online: <[priv.gc.ca](http://web.archive.org/web/20231219174547/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/)> [http://web.archive.org/web/20231219174547/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/].
- , “PIPEDA Fair Information Principle 3: Consent” (August 2020) online: <[priv.gc.ca](http://web.archive.org/web/20240717225530/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/)> [http://web.archive.org/web/20240717225530/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/].
- , “Guidelines for Obtaining Meaningful Consent” (13 August 2021) online: <[priv.gc.ca](http://web.archive.org/web/20231219174731/https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/)> [http://web.archive.org/web/20231219174731/https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/].
- , “Personal Information Retention and Disposal: Principles and Best Practices” (13 August 2021) online: <[priv.gc.ca](http://web.archive.org/web/20230517224750/https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/)> [http://web.archive.org/web/20230517224750/https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/].
- , “PIPEDA Reform: Submissions, Recommendations and Research” (last visited 23 November 2023) online: <[priv.gc.ca](http://web.archive.org/web/20231220101342/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/)> [http://web.archive.org/web/20231220101342/https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/].

Secondary Material: Books

- Bakan, Joel, *The Corporation: The Pathological Pursuit of Profit and Power*, ebook ed (Toronto: Penguin Group, 2009).
- , *The New Corporation: How “Good” Corporations are Bad for Democracy*, ebook ed (Canada: Allen Lane, 2020).
- Balakrishnan, Radhika, James Heintz & Diane Elson, *Rethinking Economic Policy for Social Justice: The Radical Potential of Human Rights*, (London: Routledge, 2016).
- Bank, Timothy M, *Guide to the Personal Information Protection and Electronic Documents Act: 2016 Edition*, (Toronto: LexisNexis Canada, 2015).
- Bennett, Colin J et al, eds, *Transparent Lives: Surveillance in Canada*, (Edmonton: AU Press, Athabasca University, 2014).
- Bennett, Colin J & Charles D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, (Cambridge, MA: MIT Press, 2006).
- Berman, Paul Schiff, ed, *Law and Society Approaches to Cyberspace*, (Hampshire, UK: Ashgate, 2007).
- Bijker, Wiebe E & John Law, eds, *Shaping Technology: Building Society: Studies in Sociotechnical Change*, (Cambridge, MA: MIT Press, 1992).
- Black, Edwin, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America’s most Powerful Corporation*, (New York: Three Rivers Press, 2002).
- Brownsword, Roger, *Rights, Regulation, and the Technological Revolution*, (New York: Oxford University Press, 2008).
- Chan, Eddie C L & George Baci, *Introduction to Wireless Localization*, (Singapore: John Wiley & Sons, 2012).
- Choudhury, Barnali & Martin Petrin, *Corporate Duties to the Public*, (Cambridge: Cambridge University Press, 2019).
- Clayton, Richard & Hugh Tomlinson, eds, *The Law of Human Rights*, 2nd ed (New York: Oxford University Press, 2009).
- Cohen, Julie E, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, (New York: Oxford University Press, 2019).
- , *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, (New Haven: Yale University Press, 2012).
- Coughlan, Stephen Gerard et al, *Law Beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization*, (Toronto: Irwin Law, 2014).

- Council of Europe et al, *Handbook on European Data Protection Law: 2018 Edition*, (Luxembourg: Publications Office of the European Union, 2018).
- Cresswell, Tim, *Place: An Introduction*, 2d ed (Malden, MA: John Wiley & Sons, 2015).
- Cukier, Kenneth & Viktor Mayer-Schönberger, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, (Boston: Houghton Mifflin Harcourt, 2013).
- Darian-Smith, Eve, *Laws and Societies in Global Contexts: Contemporary Approaches*, (New York: Cambridge University Press, 2013).
- DeCew, Judith Wagner, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, (Ithaca: Cornell University Press, 1997).
- Ebert, Isabel & Ana Beduschi, *Regulating Business Conduct in the Technology Sector: Gaps and Ways Forward in Applying the UNGPs*, Research Brief (Geneva Academy, 2022).
- Flaherty, David H, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and United States*, (Chapel Hill: The University of North Carolina Press, 1989).
- Gandy, Oscar H, *The Panoptic Sort: A Political Economy of Personal Information*, (Boulder, Colorado: Westview, 1993).
- Glasbeek, Harry, *Wealth By Stealth: Corporate Crime, Corporate Law, and the Perversion of Democracy*, (Toronto: Between The Lines, 2002).
- González Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, (Cham: Springer, 2014).
- Heyns, Christof, Frans Jacobus Viljoen & Rachel Murray, eds, *The Impact of the United Nations Human Rights Treaties on the Domestic Level: Twenty Years On*, 2nd rev ed (Leiden, The Netherlands: Brill, 2024).
- Hildebrandt, Mireille & Serge Gutwirth, eds, *Profiling the European Citizen: Cross-Disciplinary Perspectives*, (Dordrecht: Springer, 2008).
- Joseph, Sarah & Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, 3d ed (Oxford: Oxford University Press, 2013).
- Kitchin, Rob, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, (Los Angeles: SAGE, 2014).
- Kitchin, Rob & Martin Dodge, *Code/Space: Software and Everyday Life*, (Cambridge, MA: The MIT Press, 2011).
- LaMarca, Anthony & Eyal de Lara, *Location Systems: An Introduction to the Technology Behind Location Awareness*, (Morgan & Claypool, 2008).

- Lauren, Paul Gordon, *The Evolution of International Human Rights: Visions Seen*, 3rd ed (Philadelphia: University of Pennsylvania Press, 2011).
- Lessig, Lawrence, *Code: Version 2.0*, (New York: Basic Books, 2006).
- Lyon, David, *Surveillance Studies: An Overview*, (Cambridge, UK: Polity, 2007).
- , *The Electronic Eye: The Rise of Surveillance Society*, (Minneapolis: University of Minnesota Press, 1994).
- Marx, Gary T, *Undercover: Police Surveillance in America*, (Berkeley: University of California Press, 1988).
- , *Windows into the Soul: Surveillance and Society in an Age of High Technology*, (Chicago: University of Chicago Press, 2016).
- Michael, James, *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*, (Paris: UNESCO, 1994).
- Michael, Katina & MG Michael, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*, (Hershey, USA: IGI Global, 2009).
- Monmonier, Mark, *Spying with Maps: Surveillance Technologies and the Future of Privacy*, (Chicago: University of Chicago Press, 2002).
- Prosser, Tony, *The Regulatory Enterprise*, (New York: Oxford University Press, 2010).
- Regan, Priscilla M, *Legislating Privacy: Technology, Social Values, and Public Policy*, (Chapel Hill: University of North Carolina Press, 1995).
- Robertson, A H & J G Merrills, *Human Rights in the World: An Introduction to the Study of the International Protection of Human Rights*, 4th ed (Manchester: Manchester University Press, 1996).
- Rule, James B, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, (New York: Oxford University Press, 2007).
- , *The Politics of Privacy*, (Broadway: New American Library, 1980).
- Schoeman, Ferdinand David, *Privacy and Social Freedom*, (Cambridge, UK: Cambridge University Press, 1992).
- Solove, Daniel J, *Understanding Privacy*, (Cambridge, MA: Harvard University Press, 2008).
- Waldman, Ari Ezra, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*, (Cambridge, UK: Cambridge University Press, 2021).
- Westin, Alan F, *Privacy and Freedom*, (New York: Atheneum, 1967).
- White, Geoffrey, *Off the Grid: Pinpointing Location-Based Technologies and the Law*, (Ottawa: PIAC, 2015) online: piac.ca

[<http://web.archive.org/web/20231219145416/https://www.piac.ca/research-reports/do-the-watchers-need-more-watching-new-report-asks/>].

Wilken, Rowan, *Cultural Economies of Locative Media*, (New York: Oxford University Press, 2019).

Winner, Langdon, *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, (Chicago: The University of Chicago Press, 1989).

Yalden, Robert et al, *Business Organizations: Principles, Policies and Practice*, (Toronto: Emond Montgomery, 2008).

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, ebook ed (New York: Public Affairs, 2019).

Secondary Material: Books Chapters

Acquisti, Alessandro & Jens Grossklags, “What Can Behavioral Economics Teach Us About Privacy?” in Alessandro Acquisti et al, eds, *Digital Privacy: Theory, Technologies, and Practices* (New York: Auerbach Publications, 2007) 363.

Agnello, Alexander & Frédéric Mégret, “The Impact of the United Nations Human Rights Treaties on the Domestic Level in Canada” in Christof Heyns, Frans Jacobus Viljoen & Rachel Murray, eds, *The Impact of the United Nations Human Rights Treaties on the Domestic Level: Twenty Years On*, 2nd rev ed (Leiden, The Netherlands: Brill, 2024) 156.

Ando, Nisuke, “National Implementation and Interpretation” in Dinah Shelton, ed, *The Oxford Handbook of International Human Rights Law* (Oxford, UK: Oxford University Press, 2013) 698.

Andrejevic, Mark, “Becoming Drones: Smartphone Probes and Distributed Sensing” in Rowan Wilken & Gerard Goggin, eds, *Locative Media* (New York: Routledge, 2014) 193.

Andrienko, N et al, “Basic Concepts of Movement Data” in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 15.

Austin, Lisa M, “Enough About Me: Why Privacy is About Power, not Consent (or Harm)” in Austin Sarat, ed, *A World without Privacy: What Law Can and Should Do?* (Cambridge: Cambridge University Press, 2014) 131.

———, “Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State” in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (University of Ottawa Press, 2015) 103.

Barns, Sarah, “Joining the Dots: Platform Intermediation and the Recombinatory Governance of Uber’s Ecosystem” in Mike Hodson et al, eds, *Urban Platforms and the Future City*:

- Transformations in Infrastructure, Governance, Knowledge and Everyday Life* (London: Routledge, 2020) 87.
- Bijker, Wiebe E & John Law, “General Introduction” in Wiebe E Bijker & John Law, eds, *Shaping Technology/ Building Society: Studies in Sociotechnical Change* (Cambridge, Mass.: MIT Press, 1992) 1.
- Bloustein, Edward J, “Privacy as an Aspect of Human Dignity. An Answer to Dean Prosser” in Ferdinand D Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, UK: Cambridge University Press, 1984) 156.
- Bonchi, F et al, “Privacy in Spatiotemporal Data Mining” in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 297.
- Brownsword, Roger, “So What Does the World Need Now?: Reflections on Regulating Technologies.” in Roger Brownsword & Karen Yeung, eds, *Regulating Technologies : Legal Futures, Regulatory Frames and Technological Fixes* (London: Hart Publishing, 2008) 23.
- Brownsword, Roger, Eloise Scotford & Karen Yeung, “Law, Regulation, and Technology: The Field, Frame, and Focal Questions” in Roger Brownsword, Eloise Scotford & Karen Yeung, eds, *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2016).
- Bruner, Christopher M & Beate Sjøfjell, “Corporate Law, Corporate Governance and the Pursuit of Sustainability” in Beate Sjøfjell & Christopher M Bruner, eds, *The Cambridge Handbook of Corporate Law, Corporate Governance and Sustainability* (Cambridge: Cambridge University Press, 2019) 713.
- Cerda, Alberto, “The Myth of Global Online Surveillance Exempted From Compliance with Human Rights” in *Global Information Society Watch 2014: Communications Surveillance in the Digital Age* (APC and Hivos, 2014) 25.
- Chirwa, Danwood Mzikenge, “State Responsibility for Human Rights” in Mashood A Baderin & Manisuli Ssenyonjo, eds, *International Human Rights Law: Six Decades after the UDHR and Beyond* (Abingdon, Oxon: Routledge, 2016).
- Cohen, Julie E, “The Surveillance–Innovation Complex: The Irony of the Participatory Turn” in Darin Barney et al, eds, *The Participatory Condition in the Digital Age* (Minneapolis: University of Minnesota Press, 2016) 207.
- Conte, Alex, “Privacy, Honour and Reputation” in *Defining Civil and Political Rights*, 2d ed (Routledge, 2009) 201.
- Cuellar, Jorge R, “Location Information Privacy” in Behcet Sarikaya, ed, *Geographic Location in the Internet* (New York: Springer, 2002) 179.

- Damiani, Maria Luisa, “Privacy Enhancing Techniques for the Protection of Mobility Patterns in LBS: Research Issues and Trends” in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2012) 223.
- Davies, Simon G, “Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity” in Philip Agre & Marc Rotenberg, eds, *Technology and Privacy: The New Landscape* (Cambridge, Mass.: MIT Press, 1997) 143.
- De Hert, Paul & Gianclaudio Malgieri, “One European Legal Framework for Surveillance: The ECtHR’s Expanded Legality Testing Copied by the CJEU” in Valsamis Mitsilegas & Niovi Vavoula, eds, *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart Publishing, 2021) 255.
- Deva, Surya, “From Business or Human Rights to Business and Human Rights: What Next?” in *Research Handbook on Human Rights and Business* (Cheltenham: Edward Elgar Publishing, 2020) 1.
- Deva, Surya & Harpreet Kaur, “Business and Human Rights: From ‘Tokenism’ to ‘Centring’ Rights and Rights-Holders” in Marianna Leite & Matti Kohonen, eds, *Righting the Economy: Towards a People’s Recovery from Economic and Environmental Crisis* (Newcastle upon Tyne, UK: Agenda Publishing, 2024) 43.
- Dizon, Michael Anthony C, “From Regulating Technologies to Governing Society: Towards a Plural, Social and Interactive Conception of Law” in Heather M Morgan & Ruth Morris, eds, *Moving Forward: Tradition and Transformation* (Newcastle upon Tyne, UK: Cambridge Scholars Publishing, 2012) 115.
- Duckham, Matt & Lars Kulik, “Location Privacy and Location-Aware Computing” in Roland Billen, Elsa Joao & David Forrest, eds, *Dynamic and Mobile GIS: Investigating Changes in Space and Time* (Boca Raton: CRC Press, 2006).
- Flyverbom, Mikkel, “Corporate Advocacy in the Internet Domain: Shaping Policy Through Data Visualizations” in Christina Garsten & Adrienne Sörbom, eds, *Power, Policy and Profit: Corporate Engagement in Politics and Governance* (Cheltenham, UK: Edward Elgar Publishing, 2017) 115.
- Giannotti, Fosca & Dino Pedreschi, “Mobility, Data Mining and Privacy: A Vision of Convergence” in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 1.
- Guild, Elspeth, “Mapping Limitations on State Surveillance through the UN Human Rights Instruments” in Valsamis Mitsilegas & Niovi Vavoula, eds, *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart Publishing, 2021) 217.
- Gürses, Seda & Bettina Berendt, “PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm” in Serge Gutwirth,

- Yves Poullet & Paul De Hert, eds, *Data Protection in a Profiled World* (Dordrecht: Springer, 2010) 301.
- Hildebrandt, Mireille, “A Vision of Ambient Law” in Roger Brownsword & Karen Yeung, eds, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (London: Hart Publishing, 2008) 175.
- , “Privacy and Identity” in Erik Claes, Antony Duff & Serge Gutwirth, eds, *Privacy and the Criminal Law* (Antwerp: Intersentia, 2006) 61.
- Hughes, Kirsty, “The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 225.
- Hughes, Thomas P, “Technological Momentum” in Merritt Roe Smith & Leo Marx, eds, *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, Mass: MIT Press, 1994) 101.
- Hughes, Thomas Parke, “The Evolution of Large Technological Systems” in Wiebe E Bijker, Thomas P Hughes & Trevor Pinch, eds, *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, Mass.: MIT Press, 2012) 45.
- Iglesias Keller, Clara, “Don’t Shoot the Message: Regulating Disinformation Beyond Content” in Carlos Blanco de Moraes, Gilmar Ferreira Mendes & Thomas Vesting, eds, *The Rule of Law in Cyberspace* (Cham: Springer International Publishing, 2022) 309.
- Imaz, Oier, Fred Freundlich & Aritz Kanpandegi, “The Governance of Multistakeholder Cooperatives in Mondragon: The Evolving Relationship among Purpose, Structure and Process” in Sonja Novković, Karen Miner & Cian McMahon, eds, *Humanistic Governance in Democratic Organizations: The Cooperative Difference* (Cham: Springer International Publishing, 2023) 285.
- Jacobs, Bart, “Architecture is Politics: Security and Privacy Issues in Transport and Beyond” in Serge Gutwirth, Yves Poullet & Paul De Hert, eds, *Data Protection in a Profiled World* (Dordrecht: Springer, 2010) 289.
- Jones, Meg Leta, “The Internet of Other People’s Things: Conceptual and Regulatory Challenges” in Tjerk Timan, Bryce C Newell & Bert-Jaap Koops, eds, *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar Publishing, 2017) 242.
- Jørgensen, Rikke Frank, “Human Rights and Private Actors in the Online Domain” in Molly K Land & Jay D Aronson, eds, *New Technologies for Human Rights Law and Practice* (Cambridge, UK: Cambridge University Press, 2018) 243.

- Kälin, Walter & Jörg Künzli, “Protection of Private Life” in *The Law of International Human Rights Protection*, 2nd ed (Oxford: Oxford University Press, 2019) 376.
- Keller, Helen & Leena Grover, “General Comments of the Human Rights Committee and Their Legitimacy” in Helen Keller & Geir Ulfstein, eds, *UN Human Rights Treaty Bodies* (Cambridge, UK: Cambridge University Press, 2012) 116.
- Kellerbauer, Manuel et al, eds, “Article 7 CFR” in *The EU Treaties and Charter of Fundamental Rights: A Commentary* (Oxford, UK: Oxford University Press, 2024) 446.
- , eds, “Article 8 CFR” in *The EU Treaties and Charter of Fundamental Rights: A Commentary*, 2nd ed (Oxford, UK: Oxford University Press, 2024) 453.
- Kohli, Alice, “Data-Driven Human Rights Investigations” in Oliver Hahn & Florian Stalph, eds, *Digital Investigative Journalism: Data, Visual Analytics and Innovative Methodologies in International Reporting* (Cham: Springer International Publishing, 2018) 67.
- Koops, Bert-Jaap, “Criteria for Normative Technology: The Acceptability of ‘Code as Law’ in Light of Democratic and Constitutional Values” in Roger Brownsword & Karen Yeung, eds, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (London: Hart Publishing, 2008) 157.
- Leszczynski, Agnieszka, “Geoprivacy” in Rob Kitchin, Tracey P Lauriault & Matthew W Wilson, eds, *Understanding Spatial Media* (London: SAGE Publications, 2017) 235.
- Lucock, Carole & Katie Black, “Anonymity and the Law in Canada” in Ian Kerr, Valerie Steeves & Carole Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy & Identity in a Networked Society* (New York: Oxford University Press, 2009) 465.
- Lyon, David, “Introduction” in David Lyon, ed, *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination* (London: Routledge, 2005) 1.
- , “Surveillance as Social Sorting: Computer Codes and Mobile Bodies” in David Lyon, ed, *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (London: Routledge, 2005) 13.
- Makihara, Yasushi, Mark S Nixon & Yasushi Yagi, “Gait Recognition: Databases, Representations, and Applications” in Katsushi Ikeuchi, ed, *Computer Vision: A Reference Guide* (Cham: Springer, 2020) 1.
- Maras, Marie-Helen, “From Targeted to Mass Surveillance: Is The EU Data Retention Directive A Necessary Measure or An Unjustified Threat to Privacy?” in Benjamin J Goold & Daniel Neyland, eds, *New Directions in Surveillance and Privacy* (London: Willan Publishing, 2009) 74.
- Marx, Gary T, “Coming to Terms: The Kaleidoscope of Privacy and Surveillance” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 32.

- Mascetti, Sergio et al, “Anonymity: A Comparison Between the Legal and Computer Science Perspectives” in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2012) 85.
- Mather, Lynn, “Law and Society” in Robert E Goodin, ed, *The Oxford Handbook of Political Science* (Oxford: Oxford University Press, 2011) 289.
- Mattern, Friedemann & Christian Floerkemeier, “From the Internet of Computers to the Internet of Things” in Kai Sachs, Ilia Petrov & Pablo Guerrero, eds, *From Active Data Management to Event-Based Systems and More* (Berlin: Springer, 2010) 242.
- Mokrosinska, Dorota & Beate Roessler, “Introduction” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 1.
- Monmonier, Mark, “Geolocation and Locational Privacy: The ‘inside’ Story on Geospatial Tracking” in Katherine J Strandburg & Daniela Stan Raicu, eds, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (New York: Springer, 2005) 75.
- , “The Internet, Cartographic Surveillance, and Locational Privacy” in Michael Peterson, ed, *Maps and the Internet* (Pergamon, 2003) 97.
- Monreale, Anna et al, “Privacy-Preserving Distributed Movement Data Aggregation” in Danny Vandenbroucke, Bénédicte Bucher & Joep Crompvoets, eds, *Geographic Information Science at the Heart of Europe* (Cham: Springer, 2013) 225.
- Morris, John B, “The Elements of Location Tracking and Privacy Protection” in Behcet Sarikaya, ed, *Geographic Location in the Internet* (New York: Kluwer Academic Publishers, 2002) 163.
- Moses, Lyria Bennett & Monika Zalnieriute, “Law and Technology in the Dimension of Time” in Sofia Ranchordás & Yaniv Roznai, eds, *Time, Law and Change: An Interdisciplinary Study* (Oxford: Hart Publishing, 2020) 303.
- Paterson, Moira, “Surveillance in Public Places: The Regulatory Dilemma” in Normann Witzleb et al, eds, *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge, UK: Cambridge University Press, 2014) 201.
- Pedreschi, D et al, “Privacy Protection: Regulations and Technologies, Opportunities and Threats” in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 101.
- Pendry, Richard, “New Technology, War, and Human Rights Reporting” in Stephen J A Ward, ed, *Handbook of Global Media Ethics* (Cham: Springer, 2021) 1031.
- Phillips, David J, “Ubiquitous Computing, Spatiality, and the Construction of Identity: Directions for Policy Response” in Ian Kerr, Valerie M Steeves & Carole Lucock, eds, *Lessons from*

- the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* (New York: Oxford University Press, 2009) 303.
- Regan, Priscilla M, “Privacy and the Common Good: Revisited” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 50.
- Ropohl, Günter, “A Critic of Technological Determinism” in Paul T Durbin & Friedrich Rapp, eds, *Philosophy and Technology* (Dordrecht: Reidel, 1983) 83.
- Rouvroy, Antoinette & Yves Poullet, “The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy” in Serge Gutwirth et al, eds, *Reinventing Data Protection?* (Dordrecht: Springer, 2009) 45.
- Rule, James B, “Privacy: The Longue Durée” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 11.
- Scassa, Teresa, “A Human Rights-Based Approach to Data Protection in Canada” in Elizabeth Dubois & Florian Martin-Bariteau, eds, *Citizenship in a Connected Canada: A Policy and Research Agenda* (Ottawa: University of Ottawa Press, 2020) 173.
- Seck, Sara & Kirsten Stefanik, “Business and Human Rights: Challenges in Accessing Remedy and Justice Human Rights” in Gordon DiGiacomo, ed, *Human Rights: Current Issues and Controversies* (Toronto: University of Toronto Press, 2016) 381.
- Seibert-Fohr, Anja, “Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy” in Joseph E David et al, eds, *Strengthening Human Rights Protections in Geneva, Israel, the West Bank and Beyond* (Cambridge, UK: Cambridge University Press, 2021) 40.
- Sjåfjell, Beate, “Shareholder Primacy: The Main Barrier to Sustainable Companies” in Beate Sjåfjell & Benjamin J Richardson, eds, *Company Law and Sustainability: Legal Barriers and Opportunities* (Cambridge, UK: Cambridge University Press, 2015) 79.
- Solove, Daniel J, “A Brief History of Information Privacy Law” in Kristen J Mathews, ed, *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (New York: Practising Law Institute, 2006) 1.
- , “The Meaning and Value of Privacy” in Beate Roessler & Dorota Mokrosinska, eds, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge, UK: Cambridge University Press, 2015) 71.
- Steeves, Valerie, “Now You See Me: Privacy, Technology, and Autonomy in the Digital Age” in Gordon DiGiacomo, ed, *Human Rights: Current Issues and Controversies* (Toronto: University of Toronto Press, 2016) 461.

- Strandburg, Katherine J, “Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context” in Julia Lane, Victoria Stodden & Helen Nissenbaum, eds, *Big Data, and the Public Good: Frameworks for Engagement* (Cambridge, UK: Cambridge University Press, 2014) 5.
- Taylor, Paul M, ed, “Article 2: To ‘Respect and to Ensure’ Covenant Rights” in *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee’s Monitoring of ICCPR Rights* (Cambridge: Cambridge University Press, 2020) 58.
- , “Article 17: Privacy, Home, Correspondence; Honour and Reputation” in *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee’s Monitoring of ICCPR Rights* (Cambridge: Cambridge University Press, 2020) 458.
- Timan, Tjerk, “Conclusion: The Need for Privacy in Public Space.” in Tjerk Timan, Bryce C Newell & Bert-Jaap Koops, eds, *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar Publishing, 2017) 269.
- Torres-Solis, Jorge, Tiago H Falk & Tom Chau, “A Review of Indoor Localization Technologies: towards Navigational Assistance for Topographical Disorientation” in Felix Jesus Villanueva Molina, ed, *Ambient Intelligence* (InTech, 2010).
- Verykios, V S, M L Damiani & A Gkoulalas-Divanis, “Privacy and Security in Spatiotemporal Data and Trajectories” in Fosca Giannotti & Dino Pedreschi, eds, *Mobility, Data Mining and Privacy: Geographic Knowledge Discovery* (Berlin: Springer, 2008) 213.
- Vogiatzoglou, Plixavra & Peggy Valcke, “Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU law” in Eleni Kosta & Ronald Leenes, eds, *Research Handbook on EU Data Protection Law* (Cheltenham, UK: Edward Elgar Publishing, 2022) 11.
- Wasserstrom, Richard A, “Privacy: Some Arguments and Assumptions” in Ferdinand D Schoeman, ed, *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, UK: Cambridge University Press, 1984) 317.
- Wilken, Rowan, “The Necessity of Geomedia: Understanding the Significance of Location-Based Services and Data-Driven Platforms” in Karin Fast et al, eds, *Geomedia Studies: Spaces and Mobilities in Mediatized Worlds* (New York: Routledge, 2017) 21.
- Wood, David Murakami, “Spatial Profiling, Sorting and Prediction” in Rob Kitchin, Tracey P Lauriault & Matthew W Wilson, eds, *Understanding Spatial Media* (London: SAGE Publications, 2017) 225.
- Wright, David & Paul De Hert, “Introduction to Privacy Impact Assessment” in David Wright & Paul De Hert, eds, *Privacy Impact Assessment* (Dordrecht: Springer, 2012) 3.

- Wright, David & Emilio Mordini, “Privacy and Ethical Impact Assessment” in David Wright & Paul De Hert, eds, *Privacy Impact Assessment* (Dordrecht: Springer, 2012) 397.
- Zekavat, Seyed A Reza, Stuti Kansal & Allen H Levesque, “Wireless Positioning Systems: Operation, Application, and Comparison” in Seyed A Reza Zekavat & R Michael Buehrer, eds, *Handbook of Position Location* (Hoboken, NJ, USA: John Wiley & Sons, 2011) 3.
- Zuboff, Shoshana, ““We Make Them Dance”: Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights” in Rikke Frank Jørgensen, ed, *Human Rights in the Age of Platforms* (Cambridge, MA: The MIT Press, 2019) 3.

Secondary Material: Journal Articles

- Abbas, Roba et al, “Sketching and Validating the Location-Based Services (LBS) Regulatory Framework in Australia” (2013) 29 Computer Law & Security Review 576.
- Addo, Michael K, “The Reality of the United Nations Guiding Principles on Business and Human Rights” (2014) 14 Human Rights Law Review 133.
- Ahvar, Ehsan et al, “On Analyzing User Location Discovery Methods in Smart Homes: A Taxonomy and Survey” (2016) 76 Journal of Network and Computer Applications 75.
- Aiken, Emily et al, “Machine Learning and Phone Data Can Improve Targeting of Humanitarian Aid” (2022) 603:7903 Nature 864.
- Allen, Anita L, “Coercing Privacy” (1999) 40:3 William and Mary Law Review 723.
- Altman, Irwin, “Privacy: A Conceptual Analysis” (1976) 8:1 Environment and Behavior 7.
- , “Privacy Regulation: Culturally Universal or Culturally Specific?” (1977) 33:3 Journal of Social Issues 66–84.
- Ashbrook, Daniel & Thad Starner, “Using GPS to Learn Significant Locations and Predict Movement Across Multiple Users” (2003) 7 Personal and Ubiquitous Computing 275.
- Ataei, Mehrnaz, Auriol Degbelo & Christian Kray, “Privacy Theory in Practice: Designing a User Interface for Managing Location Privacy on Mobile Devices” (2018) 12:3–4 Journal of Location Based Services 141.
- Attaran, Mohsen, “The Impact of 5G on the Evolution of Intelligent Automation and Industry Digitization” (2023) 14:5 Journal of Ambient Intelligence and Humanized Computing 5977.
- Austin, Lisa M, “Surveillance and the Rule of Law” (2015) 13:2 Surveillance & Society 295.
- , “Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints” (2016) 17:2 Theoretical Inquiries in Law 451.

- Backer, Larry Cata, “Regulating Multinational Corporations: Trends, Challenges, and Opportunities Multinational Corporations” (2015) 22:1 *Brown Journal of World Affairs* 153.
- Bailey, Jane, “Systematic Government Access to Private-Sector Data in Canada” (2012) 2:4 *International Data Privacy Law* 207.
- Bakan, Joel, “The Invisible Hand of Law: Private Regulation and the Rule of Law” (2015) 48:2 *Cornell International Law Journal* 279.
- Banerjee, Syagnik, “Geosurveillance, Location Privacy, and Personalization” (2019) 38:4 *Journal of Public Policy & Marketing* 484.
- Banksto, Kevin S & Ashkan Soltani, “Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*” (2014) 123 *Forum*, online: <[yalelawjournal.org](http://web.archive.org/web/20231222141720/https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones)> [http://web.archive.org/web/20231222141720/https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones].
- Barreneche, Carlos & Rowan Wilken, “Platform Specificity and the Politics of Location Data Extraction” (2015) 18:4–5 *European Journal of Cultural Studies* 497.
- Bennett Moses, Lyria, “How to Think about Law, Regulation and Technology: Problems with ‘Technology’ as a Regulatory Target” (2013) 5:1 *Law, Innovation and Technology* 1.
- , “Recurring Dilemmas: The Law’s Race to Keep up with Technological Change” 2007:2 *University of Illinois Journal of Law, Technology & Policy* 239.
- , “Regulating in the Face of Sociotechnical Change” in Roger Brownsword, Eloise Scotford & Karen Yeung, eds, *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2016) 573.
- , “Why Have a Theory of Law and Technological Change?” (2007) 8:2 *Minnesota Journal of Law, Science & Technology* 589.
- , “Agents of Change: How the Law ‘Copes’ with Technological Change” (2011) 20:4 *Griffith Law Review* 763.
- Bennett, Colin J, “In Defence of Privacy: The Concept and the Regime” (2011) 8:4 *Surveillance & Society* 485.
- Beresford, Alastair R & Frank Stajano, “Location Privacy in Pervasive Computing” (2003) 2:1 *IEEE Pervasive Computing* 46.
- Bond, Robert M et al, “A 61-Million-Person Experiment in Social Influence and Political Mobilization” (2012) 489 *Nature* 295.
- Bradford, Anu, “The False Choice Between Digital Regulation and Innovation” (2024) 119:2 *Northwestern University Law Review* 377.

- Brena, Ramon F et al, “Evolution of Indoor Positioning Technologies: A Survey” (2017) *Journal of Sensors* 1.
- Büchi, Moritz et al, “The Chilling Effects of Algorithmic Profiling: Mapping the Issues” (2020) 36 *Computer Law & Security Review* 1.
- Burdon, Mark, “Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws” 2010:1 *Journal of Law, Technology and Policy* 1.
- Calacci, Dan et al, “The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good” (2019) arXiv, DOI: <10.48550/arXiv.1905.09350>.
- Callard, C, D Thompson & N Collishaw, “Transforming the Tobacco Market: Why the Supply of Cigarettes Should be Transferred from For-Profit Corporations to Non-Profit Enterprises with a Public Health Mandate” (2005) 14:4 *Tobacco Control* 278–283.
- Casado, Rubén & Muhammad Younas, “Emerging Trends and Technologies in Big Data Processing” (2015) 27:8 *Concurrency and Computation* 2078.
- Chapdelaine, Pascale, “Algorithmic Personalized Pricing” (2020) 17:1 *Journal of Law and Business* 1.
- , “Algorithmic Personalized Pricing: A Personal Data Protection and Consumers Law Perspective” (2024) 102:1 *The Canadian Bar Review* 1.
- Chen, Liang et al, “Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey” (2017) 5 *IEEE Access* 8956.
- Cheung, Anne SY, “Location Privacy: The Challenges of Mobile Service Devices” (2014) 30 *Computer Law & Security Review* 41.
- Choudhury, Barnali, “Corporate Law’s Threat to Human Rights: Why Human Rights Due Diligence Might Not Be Enough” (2023) 8:2 *Business and Human Rights Journal* 180.
- Christin, Delphine & Matthias Hollick, “Roadmap for Privacy Protection in Mobile Sensing Applications” in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer, 2012) 203.
- Clarke, Roger, “Person Location and Person Tracking: Technologies, Risks and Policy Implications” (2001) 14:2 *Information Technology & People* 206.
- , “The Digital Persona and Its Application to Data Surveillance” (1994) 10:2 *Information Society* 77.
- Clarke, Roger A, “Information Technology and Dataveillance” (1988) 31:5 *Communications of the ACM* 498.
- Clarke, Roger & Marcus Wigan, “You are Where You’ve Been: the Privacy Implications of Location and Tracking Technologies” (2011) 5:3–4 *Journal of Location Based Services* 138.

- Cohen, Julie E, “Privacy, Visibility, Transparency, and Exposure” (2008) 75 *The University of Chicago Law Review* 181.
- Cohen, Julie E, “What Privacy is For” (2013) 126 *Harvard Law Review* 1904.
- Cookfield, Arthur & Jason Pridmore, “A Synthetic Theory of Law and Technology” (2007) 8:2 *Minnesota Journal of Law, Science & Technology* 475.
- Cottrill, Caitlin D, “Location Privacy: Who Protects?” (2011) 23:2 *URISA* 49.
- Cottrill, Caitlin D & Piyushimita “Vonu” Thakuriah, “Location Privacy Preferences: A Survey-Based Analysis of Consumer Awareness, Trade-Off and Decision-Making” (2015) 56 *Transportation Research Part C* 132.
- Cray, Charlie, “Chartering a New Course: Revoking Corporations’ Right to Exist” (2002) *Multinational Monitor* 8.
- Cray, Charlie & Lee Drutman, “Corporations and the Public Purpose: Restoring the Balance” (2005) 4:1 *Seattle Journal for Social Justice* 305.
- Cresswell, Tim, “The Production of Mobilities” (2001) 43 *New Formations* 11. Crusto, Mitchell F, “Green Business: Should We Revoke Corporate Charters for Environmental Violations” (2003) 63 *Louisiana Law Review* 175.
- Cuijpers, Colette & Bert-Jaap Koops, “How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services” (2008) 33 *European Law Review* 880.
- Curry, Michael R, “Digital People, Digital Places: Rethinking Privacy in a World of Geographic Information” (1997) 7:3 *Ethics & Behavior* 253.
- Curry, Michael R, David J Phillips & Priscilla M Regan, “Emergency Response Systems and the Creeping Legibility of People and Places” (2004) 20:5 *Information Society* 357.
- Day, Gregory & Abbey Stemler, “Are Dark Patterns Anticompetitive?” (2020) 72:1 *Alabama Law Review* 1.
- Deva, Surya, “Business and Human Rights: Alternative Approaches to Transnational Regulation” (2021) 17 *Annual Review of Law and Social Science* 139.
- Diggelmann, Oliver & Maria Nicole Cleis, “How the Right to Privacy Became a Human Right” (2014) 14 *Human Rights Law Review* 441.
- Dijk, Niels van, Raphaël Gellert & Kjetil Rommetveit, “A Risk to a Right? Beyond Data Protection Risk Assessments” (2016) 32 *Computer Law & Security Review* 286.
- Dreyer, Jerome et al, “‘Informed’ Consent in Popular Location Based Services and Digital Sovereignty” (2022) 16:4 *Journal of Location Based Services* 312.

- Eagle, Nathan & Alex (Sandy) Pentland, "Reality Mining: Sensing Complex Social Systems" (2006) 10 *Personal and Ubiquitous Computing* 255.
- Elwood, Sarah & Agnieszka Leszczynski, "Privacy, Reconsidered: New Representations, Data Practices, and the Geoweb" (2011) 42 *Geoforum* 6.
- Flyverbom, Mikkel, Ronald Deibert & Dirk Matten, "The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business" (2019) 58:1 *Business & Society* 3.
- Fourcade, Marion & Kieran Healy, "Seeing Like a Market" (2017) 15:1 *Socio-Economic Review* 9.
- Fretty, Douglas A, "Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places" (2011) 16:03 *Virginia Journal of Law & Technology* 430.
- Fried, Charles, "Privacy" (1968) 77:3 *Yale Law Journal* 475.
- Fuchs, Doris & Markus ML Lederer, "The Power of Business" (2007) 9:3 *Business and Politics* 1.
- Furini, Marco, "Users Behavior in Location-Aware Services: Digital Natives versus Digital Immigrants" 2014 *Advances in Human-Computer Interaction* 1.
- Galič, Maša, Tjerk Timan & Bert-Jaap Koops, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation" (2017) 30 *Philosophy & Technology* 9.
- Gasson, Mark N et al, "Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones" (2011) 41:2 *IEEE Transactions on Systems, Man, and Cybernetics, Part C* 251.
- Gavison, Ruth, "Privacy and the Limits of Law" (1980) 89:3 *Yale Law Journal* 421.
- Geissler, Roger C, "Private Eyes Watching You: Google Street View and the Right to an Inviolable Personality" (2012) 63 *Hastings Law Journal* 897.
- Gellert, Raphaël & Serge Gutwirth, "The Legal Construction of Privacy and Data Protection" (2013) 29 *Computer Law & Security Review* 522.
- Goss, Jon, "'We Know Who You Are and We Know Where You Live': The Instrumental Rationality of Geodemographic Systems" (1995) 71:2 *Economic Geography* 171.
- Gratton, Eloïse, "M-commerce: The Notion of Consumer Consent in Receiving Location-Based Advertising" (2002) 1:3 *Canadian Journal of Law and Technology* 59.
- Greene, Daniel & Katie Shilton, "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development" (2018) 20:4 *New Media & Society* 1640.

- Greenfield, Kent, "Proposition: Saving the World with Corporate Law" (2008) 57:4 *Emory Law Journal* 947.
- Greenough, P Gregg & Erica L Nelson, "Beyond Mapping: A Case for Geospatial Analytics in Humanitarian Health" (2019) 13:1 *Conflict and Health* 50.
- Griffin, James, "The Human Right to Privacy" (2007) 44 *San Diego Law Review* 267.
- Haggerty, Kevin D & Richard V Ericson, "The Surveillant Assemblage" (2000) 51:4 *British Journal of Sociology* 605.
- Hall, Claire M, "An Army of Spies? The Gestapo Spy Network 1933—45" (2009) 44:2 *Journal of Contemporary History* 247.
- Hallinan, Dara & Nicholas Martin, "Fundamental Rights, the Normative Keystone of DPIA" (2020) 6:2 *European Data Protection Law Review* 178.
- Helmond, Anne, "The Platformization of the Web: Making Web Data Platform Ready" (2015) 1:2 *Social Media + Society* 1.
- Herbert, William A, "No Direction Home: Will The Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?" (2006) 2:2 *I/S: A Journal of Law and Policy for the Information Society* 409.
- Herrmann, Michael et al, "Privacy in Location-Based Services: An Interdisciplinary Approach" (2016) 13:2 *SCRIPTed* 144.
- Heyns, Christof & Frans Viljoen, "The Impact of the United Nations Human Rights Treaties on the Domestic Level" (2001) 23:3 *Human Rights Quarterly* 483.
- Hildebrandt, Mireille, "Profiling: From Data to Knowledge. The Challenges of a Crucial Technology" (2006) 30:9 *Datenschutz und Datensicherheit* 548.
- Hughes, Kirsty, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75:5 *The Modern Law Review* 806.
- Hulpke, John F, "If All Else Fails, A Corporate Death Penalty?" (2017) 26:4 *Journal of Management Inquiry* 433.
- Hutchins, Renée McDonald, "Tied Up in Knotts? GPS Technology and the Fourth Amendment" (2007) 55 *UCLA Law Review* 409.
- Jägers, Nicola, "UN Guiding Principles on Business and Human Rights: Making Headway towards Real Corporate Accountability?" (2011) 29:2 *Netherlands Quarterly of Human Rights* 159.
- Jain, AK, A Ross & S Prabhakar, "An Introduction to Biometric Recognition" (2004) 14:1 *IEEE Transactions on Circuits and Systems for Video Technology* 4.
- Kaminski, Margot E, "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability" (2019) 92 *Southern California Law Review* 1529.

- Keith, Mark J et al, "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior" (2013) 71:12 International Journal of Human-Computer Studies 1163.
- Kerr, Ian & Jessica Earle, "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy" (2013) 66 Stanford Law Review 65.
- Keyaerts, Katrien, "Ben Faiza v. France: Use of Cell Site Location Information by Police is Acceptable Interference with Right to Privacy" (2019) 5:1 European Data Protection Law Review 120.
- Khanna, Aran, "Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger" (2015) Technology Science, online: <techscience.org> [http://web.archive.org/web/20231222114452/https://techscience.org/a/2015081101/].
- Kim, Byoungjip et al, "Agatha: Predicting Daily Activities from Place Visit History for Activity-Aware Mobile Services in Smart Cities" (2015) 11:12 International Journal of Distributed Sensor Networks 1.
- Kosta, Eleni et al, "Legal Considerations on Privacy-Enhancing Location Based Services Using PRIME Technology" (2008) 24 Computer Law & Security Review 139.
- Kramer, Adam D I, Jamie E Guillory & Jeffrey T Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks" (2014) 111:24 PNAS 8788.
- Krumm, John, "A Survey of Computational Location Privacy" (2009) 13 Pers Ubiquit Comput 391.
- Laoudias, Christos et al, "A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation" (2018) 20:4 IEEE Communications Surveys Tutorials 3607.
- Lee, Chao, Yunchuan Guo & Lihua Yin, "A Framework of Evaluation Location Privacy in Mobile Network" (2013) 17 Procedia Computer Science 879.
- Leite, Marianna, "Beyond Buzzwords: Mandatory Human Rights Due Diligence and a Rights-Based Approach to Business Models" (2023) 8:2 Business and Human Rights Journal 197.
- Leszczynski, Agnieszka, "Spatial Big Data and Anxieties of Control" (2015) 33:6 Environ Plan D: Society and Space 965.
- Liang, Yunji et al, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective" (2020) 7:9 IEEE Internet of Things Journal 9128.
- Liao, Carol, "Disruptive Innovation and the Global Emergence of Hybrid Corporate Legal Structures" (2014) 11:2 European Company Law 67.
- Lindman, Juho, Jukka Makinen & Eero Kasanen, "Big Tech's Power, Political Corporate Social Responsibility and Regulation" (2023) 38:2 Journal of Information Technology 144.

- Linzey, Thomas, “Awakening a Sleeping Giant: Creating a Quasi-Private Cause of Action for Revoking Corporate Charters in Response to Environmental Violations” (1995) 13:1 *Pace Environmental Law Review* 219.
- , “Killing Goliath: Defending Our Sovereignty and Environmental Sustainability through Corporate Charter Revocation in Pennsylvania and Delaware” (1997) 6:1 *Penn State Environmental Law Review* 31.
- Liu, Bo et al, “Location Privacy and Its Applications: A Systematic Study” (2018) 6 *IEEE Access* 17606.
- Loenen, B van & J A Zevenbergen, “The Impact of the European Privacy Regime on Location Technology Development” (2007) 1:3 *Journal of Location Based Services* 165.
- Lyon, David, “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique” (2014) 1:2 *Big Data & Society* 1.
- Manousakas, Dionysis et al, “Quantifying Privacy Loss of Human Mobility Graph Topology” (2018) 3 *Proceedings on Privacy Enhancing Technologies* 5.
- Mantelero, Alessandro, “AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment” (2018) 34 *Computer Law & Security Review* 754.
- Martin, Kirsten & Katie Shilton, “Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices” (2016) 32:3 *Information Society* 200.
- McCorquodale, Robert & Stuart Neely, “Directors Duties and Human Rights Impacts: A Comparative Approach” (2022) 22:2 *Journal of Corporate Law Studies* 605.
- McDonald, Aleecia M & Lorrie Faith Cranor, “The Cost of Reading Privacy Policies” (2008) 4:3 *I/S: A Journal of Law and Policy for the Information Society* 540.
- Michael, Katina & Roger Clarke, “Location and Tracking of Mobile Devices: Überveillance Stalks the Streets” (2013) 29 *Computer Law & Security Review* 216.
- Milanovic, Marko, “Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age” (2015) 56:1 *Harvard International Law Journal* 81.
- Moerel, Lokke & Corien Prins, “Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things” (2016), online: [papers.ssrn.com](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123) [http://web.archive.org/web/20231222125842/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123].
- Monreale, Anna et al, “C-Safety: A Framework for the Anonymization of Semantic Trajectories” (2011) 4:2 *Transactions on Data Privacy* 73.

- Montjoye, Yves-Alexandre de et al, “Unique in the Crowd: The Privacy Bounds of Human Mobility” (2013) 3:1376 *Nature* 1.
- Myles, Ginger, Adrian Friday & Nigel Davies, “Preserving Privacy in Environments with Location-Based Applications” (2003) 2:1 *IEEE Pervasive Computing* 56.
- Narayanan, Arvind et al, “Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces” (2020) 18:2 *Queue* 67.
- Nissenbaum, Helen, “Privacy as Contextual Integrity” (2004) 79:1 *Washington Law Review* 119.
- , “Toward an Approach to Privacy in Public: Challenges of Information Technology” (1997) 7:3 *Ethics & Behavior* 207.
- Noonan, Kyle, “The Case for a Federal Corporate Charter Revocation Penalty” (2012) 80:2 *George Washington Law Review* 602.
- Otterberg, April A, “GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court’s Theory of the Public Space under the Fourth Amendment” (2005) 46:3 *Boston College Law Review* 661.
- Paton-Simpson, Elizabeth, “Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places” (2000) 50:3 *University of Toronto Law Journal* 305.
- Pentland, Alex “Sandy”, “Society’s Nervous System: Building Effective Government, Energy, and Public Health Systems” (2012) 45:1 *Computer* 31.
- Peppet, Scott R, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent” (2014) 93 *Texas Law Review* 85.
- Popiel, Pawel, “The Tech Lobby: Tracing the Contours of New Media Elite Lobbying Power: Communication, Culture & Critique” (2018) 11:4 *Communication, Culture & Critique* 566.
- Posner, Richard A, “The Economics of Privacy” (1981) 71:2 *American Economic Review* 405.
- Ramirez, Mary Kreiner, “The Science Fiction of Corporate Criminal Liability: Containing the Machine Through the Corporate Death Penalty” (2005) 47 *Arizona Law Review* 933.
- Ratner, Steven R, “Corporations and Human Rights: A Theory of Legal Responsibility” (2001) 111:3 *The Yale Law Journal* 443.
- Reiman, Jeffrey H, “Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future” (1995) 11 *Computer & High Technology Law Journal* 27.
- Richards, Neil & Woodrow Hartzog, “The Pathologies of Digital Consent” (2019) 96 *Washington University Law Review* 1461.

- Rock, Edward B, “For Whom Is the Corporation Managed in 2020? The Debate over Corporate Purpose Essays” (2020) 76:2 *Bus Law* 363.
- Rodríguez Casal, Carlos, “Location and Personal Information for Direct Marketing: Third Generation Killer Application” (2003) 5:2 *info* 45.
- Roessler, Beate, “X—Privacy as a Human Right” (2017) 117:2 *Proceedings of the Aristotelian Society* 187.
- Roessler, Beate & Dorota Mokrosinska, “Privacy and Social Interaction” (2013) 39:8 *Philosophy & Social Criticism* 771.
- Ronen, Yael, “Big Brother’s Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers” (2015) 31:80 *Utrecht Journal of International and European Law* 72.
- Rossi, Luca, James Walker & Mirco Musolesi, “Spatio-Temporal Techniques for User Identification by Means of GPS Mobility Data” (2015) 4 *EPJ Data Science* 11.
- Ruggie, John Gerard, Caroline Rees & Rachel Davis, “Ten Years After: From UN Guiding Principles to Multi-Fiduciary Obligations” (2021) 6:2 *Business and Human Rights Journal* 179.
- Rusinova, Vera, “Privacy and the Legalisation of Mass Surveillance: In Search of A Second Wind for International Human Rights Law” (2022) 26:4 *International Journal of Human Rights* 740.
- Sadilek, Adam & John Krumm, “Far Out: Predicting Long-Term Human Mobility” (2021) 26:1 *Proceedings of the AAAI Conference on Artificial Intelligence* 814.
- Sadowski, Jathan, “When Data is Capital: Datafication, Accumulation, and Extraction” (2019) 6:1 *Big Data & Society* 1.
- Samuel D Warren & Louis D Brandeis, “The Right to Privacy” (1890) 4:5 *Harvard Law Review* 193.
- Savourey, Elsa & Stéphane Brabant, “The French Law on the Duty of Vigilance: Theoretical and Practical Challenges Since its Adoption” (2021) 6:1 *Business and Human Rights Journal* 141.
- Scassa, Teresa, “Consumer Privacy and Radio Frequency Identification Technology” (2006) 37:2 *Ottawa Law Review* 215.
- , “Geographical Information as ‘Personal Information’” (2010) 10:2 *Oxford University Commonwealth Law Journal* 185.
- Scassa, Teresa & Anca Sattler, “Location-Based Services and Privacy” (2011) 9 *Canadian Journal of Law and Technology* 99.
- Schermer, Bart W, “The Limits of Privacy in Automated Profiling and Data Mining” (2011) 27 *Computer Law & Security Review* 45.

- Schwartz, Paul M, “European Data Protection Law and Restrictions on International Data Flows” (1994) 80:3 Iowa Law Review 471.
- , “Privacy and Democracy in Cyberspace” (1999) 52:6 Vanderbilt Law Review 1607.
- Sherman III, John, “Beyond CSR: The Story of the UN Guiding Principles on Business and Human Rights” (2020) Harvard Kennedy School, Working Paper No. 71.
- Shilton, Katie, “Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection” (2009) 52:11 Communications of the ACM 48.
- Shoja Ghiass, Reza et al, “Infrared Face Recognition: A Comprehensive Review of Methodologies and Databases” (2014) 47 Pattern Recognition 2807.
- Simitis, Spiros, “From the Market to the Polis: The EU Directive on the Protection of Personal Data” (1995) 80:3 Iowa Law Review 445.
- Simons, Penelope, “International Law’s Invisible Hand and the Future of Corporate Accountability for Violations of Human Rights” (2012) 3:1 Journal of Human Rights and the Environment 5.
- Siprut, Joseph, “Privacy Through Anonymity: An Economic Argument for Expanding the Right of Privacy in Public Places” (2006) 33 Pepperdine Law Review 311.
- Sjåfjell, Beate, “How Company Law Has Failed Human Rights-and What to Do About It” (2020) 5:2 Business and Human Rights Journal 179.
- Sjåfjell, Beate et al, “Securing the Future of European Business: SMART Reform Proposals” University of Oslo, Research Paper Series No. 2020-11.
- Smith, D Gordon, “Response: The Dystopian Potential of Corporate Law” (2008) 57:4 Emory Law Journal 985.
- Smith, Harrison, “Metrics, Locations, and Lift: Mobile Location Analytics and the Production of Second-Order Geodemographics” (2019) 22:8 Information, Communication & Society 1044.
- , “The Locative Imaginary: Classification, Context and Relevance in Location Analytics” (2020) 68:3 Sociological Review 641.
- Solove, Daniel J, “Introduction: Privacy Self-Management and the Consent Dilemma” (2013) 126 Harvard Law Review 1880.
- Song, Chaoming et al, “Limits of Predictability in Human Mobility” (2010) 327 Science 1018.
- Tene, Omer, “Privacy Law’s Midlife Crisis: A critical Assessment of the Second Wave of Global Privacy Laws” (2013) 74:6 Ohio State Law Journal 1217.
- Tom Gerety, “Redefining Privacy” (1977) 12:2 Harvard Civil Rights-Civil Liberties Law Review 233.

- Tranter, Kieran, “The Law and Technology Enterprise: Uncovering the Template to Legal Scholarship on Technology” (2011) 3:1 *Law, Innovation and Technology* 31.
- , “The Laws of Technology and the Technology of Law” (2011) 20:4 *Griffith Law Review* 753.
- Tufekci, Zeynep, “Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency” (2015) 13 *Colorado Technology Law Journal* 203.
- , “As the Pirates Become CEOs: The Closing of the Open Internet” (2016) 145:1 *Daedalus* 65.
- Turow, Joseph et al, “The Federal Trade Commission and Consumer Privacy in the Coming Decade” (2007) 3:3 *I/S: A Journal of Law and Policy for the Information Society* 723.
- Vardanyan, Lusine & Václav Stehlík, “Is the Case Law of ECtHR Ready to Prevent the Expansion of Mass Surveillance in the Post-Covid Europe?” (2020) 7 *European Studies* 253.
- Veale, Michael, Reuben Binns & Jef Ausloos, “When Data Protection by Design and Data Subject Rights Clash” (2018) 8:2 *International Data Privacy Law* 105.
- Vila, Tony, Rachel Greenstadt & David Molnar, “Why We Can’t Be Bothered to Read Privacy Policies” in Stephen Lewis & L Jean Camp, eds, *Economics of Information Security* (New York: Kluwer Academic Publishers, 2004) 143.
- Vo, Quoc Duy & Pradipta De, “A Survey of Fingerprint-Based Outdoor Localization” (2016) 18:1 *IEEE Communications Surveys Tutorials* 491.
- Wachter, Sandra, “Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR” (2018) 34 *Computer Law & Security Review* 436.
- Wachter, Sandra, Brent Mittelstadt & Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation” (2017) 7:2 *International Data Privacy Law* 76.
- Waldman, Ari Ezra, “Privacy Law’s False Promise” (2020) 97 *Washington University Law Review* 773.
- , “Privacy’s Law of Design” (2019) 9:5 *UC Irvine Law Review* 1239.
- Westin, Alan F, “Social and Political Dimensions of Privacy” (2003) 59:2 *Journal of Social Issues* 431.
- Wolfsteller, René & Yingru Li, “Business and Human Rights Regulation After the UN Guiding Principles: Accountability, Governance, Effectiveness” (2022) 23 *Hum Rights Review* 1.
- Yassin, Ali et al, “Recent Advances in Indoor Localization: A Survey on Theoretical Approaches and Applications” (2017) 19:2 *IEEE Communications Surveys Tutorials* 1327.

Zarsky, Tal Z, “The Privacy-Innovation Conundrum” (2015) 19:1 Lewis & Clark Law Review 115.

———, “Incompatible: The GDPR in the Age of Big Data” (2017) 47 Seton Hall Law Review 995.

Zuboff, Shoshana et al, “Surveillance Capitalism: An Interview with Shoshana Zuboff” (2019) 17:1/2 Surveillance & Society 257.

Secondary Material: Reports

32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* (Jerusalem: 2010).

Ackerman, Linda, James Kempf & Toshio Miki, *Wireless Location Privacy: Law and Policy in the US, EU and Japan*, Isoc Member Briefing #15 (Virginia: Internet Society, 2003) online: <[isoc.org](http://www.isoc.org/briefings/015/briefing15.pdf)> [https://web.archive.org/web/20050117191259/http://www.isoc.org/briefings/015/briefing15.pdf].

ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, (California: ACLU, 2010) online: <[aclunc.org](http://www.aclunc.org/sites/default/files/asset_upload_file183_9627.pdf)> [http://web.archive.org/web/20220126145214/https://www.aclunc.org/sites/default/files/asset_upload_file183_9627.pdf].

Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, (London: Amnesty International, 2019) online: <[amnesty.org](http://www.amnesty.org/en/documents/po130/1404/2019/en/)> [http://web.archive.org/web/20231218123100/https://www.amnesty.org/en/documents/po130/1404/2019/en/].

Bennett, Colin J. & Lori Crowe, Office of the Privacy Commissioner of Canada, *Locational-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risk in Canada*, Contributions Program 2004-05 (Ottawa: OPC, 2005).

Canetti, Ran et al, *Response to the RFI on Advancing Privacy-Enhancing Technologies*, Request for Information (RFI), Federal Register Notice 87 FR 35250 (2022).

Christl, Wolfie, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*, (Vienna: Cracked Labs, 2017) online: <crackedlabs.org> [http://web.archive.org/web/20231218113532/https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf].

Rights Based Economy: Putting People and Planet First, by Kate Donald, (New York: Center for Economic and Social Rights, 2020) online: <https://www.cesr.org/sites/default/files/Rights%20Based%20Economy%20briefing.pdf> > .

Expert Group 2, Smart Grid Task Force 2012-14, *Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems v.2* (2018) online: <ec.europa.eu> [https://web.archive.org/web/20190630074908/https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf].

Fédération Romande Des Consommateurs, *Allo, mon téléphone m'écoute!*, by Jean Busché & Sandra Imsand, (2023) online: <enquetes.frc.ch> [<https://web.archive.org/web/20231219172359/https://enquetes.frc.ch/data>].

Fuster, Gloria González et al, *The Right to Lodge a Data Protection Complaint: OK, but Then What? An Empirical Study of Current Practices under the GDPR*, (Data Protection Law Scholars Network, 2022) online: <accessnow.org> [<https://web.archive.org/web/20231218161747/https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-Complaint-study.pdf>].

Future of Identity in the Information Society (No. 507512), *The Legal Framework for Location-Based Services in Europe* (2007) online: <fidis.net> [<https://web.archive.org/web/20231218160143/http://www.fidis.net/resources/fidis-deliverables/mobility-and-identity/d115-the-legal-framework-for-location-based-services-in-europe/doc/9/>].

Gambs, Sébastien, Office of the Privacy Commissioner of Canada, *Privacy and AI Ethics: Understanding The Convergences and Tensions for the Responsible Development of Machine Learning*, Contributions Program 2020-2021 (Ottawa: OPC, 2021) online: <priv.gc.ca> [https://web.archive.org/web/20231218154442/https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2020-2021/p_2020-21_09/].

Hightower, Jeffrey & Gaetano Borriello, *Location Sensing Techniques*, UW CSE 01-07-01 (University of Washington, Department of Computer Science and Engineering, 2001).

Hugger, Felix et al, *The Global Minimum Tax and the Taxation of MNE Profit*, OECD Taxation Working Papers, No 68 (Paris: OECD Publishing, 2024).

Lyon, David, Stephen Marmura & Pasha Peroff, Office of the Privacy Commissioner of Canada, *Location Technologies: Mobility, Surveillance and Privacy*, Contributions Program (Ottawa: OPC, 2005).

OECD, *Guidelines for Multinational Enterprises: 2011 Edition*, (OECD, 2011).

———, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (Paris: OECD, 2001).

Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment: A Concerning State of Play for the Right to Privacy in Europe*, (London: Privacy International, 2017) online: <[privacyinternational.org](http://web.archive.org/web/20231219153941/https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf)> [http://web.archive.org/web/20231219153941/https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf].

Shokri, Reza, Julien Freudiger & Jean-Pierre Hubaux, *A Unified Framework for Location Privacy*, EPFL Report 148708 (Switzerland: LCA, EPFL, 2010).

Wartell, Julie & J Thomas McEwen, Institute for Law and Justice, *Privacy in the Information Age: A Guide for Sharing Crime Maps and Spatial Data*, NCJ 188739 (Washington, DC: US Department of Justice, 2001) online: <[ojp.gov](http://web.archive.org/web/20231219151816/https://www.ojp.gov/pdffiles1/nij/188739.pdf)> [http://web.archive.org/web/20231219151816/https://www.ojp.gov/pdffiles1/nij/188739.pdf].

Secondary Material: Conference Papers

Asier, Aztiria, Juan Carlos Augusto & Izaguirre Alberto, “Spatial and Temporal Aspects for Pattern Representation and Discovery in Intelligent Environments” (Paper delivered at the Workshop on Spatial and Temporal Reasoning at 18th European Conference on Artificial Intelligence, Patras, Greece, July 2008) [unpublished] online: <<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7f0ed8fabe7cc6f7dd684e15568fcb773cc6f3ae>>.

Beresford, Alastair R & Frank Stajano, “Mix Zones: User Privacy in Location-Aware Services” (Paper delivered at the IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, FL, March 14-17, 2004) in Bob Werner, ed, *Proceedings PerCom 2004* (California: IEEE, 2004) 127, DOI:<[10.1109/PERCOMW.2004.1276918](https://doi.org/10.1109/PERCOMW.2004.1276918)>.

Briel, Frederik von & Per Davidsson, “Digital Platforms and Network Effects: Using Digital Nudges for Growth Hacking” (Paper delivered at the 40th International Conference on Information Systems, Munich, 2019) [unpublished] online: <https://aisel.aisnet.org/icis2019/innov_entre/innov_entre/8>.

- Clausen, Sünje et al, “From Dark Patterns to Digital Sludging: Mapping the Ethical Debate on Controversial Persuasive System Design” (Paper delivered at the 43th International Conference on Information Systems, Copenhagen, December 2022) [unpublished] online: <https://aisel.aisnet.org/icis2022/soc_impact_is/soc_impact_is/11>.
- Cvrcek, Dan et al, “The Value of Location Information: A European-Wide Study” (Paper delivered at the 14th International Workshop on Security Protocols, Cambridge, UK, March 27-29, 2006) in Bruce Christianson et al, eds, *Security Protocols* (Berlin: Springer, 2009) 112, DOI:<[10.1007/978-3-642-04904-0_15](https://doi.org/10.1007/978-3-642-04904-0_15)>.
- Decker, Michael, “Location Privacy-An Overview” (Paper delivered at the 7th International Conference on Mobile Business, Barcelona, July 7-8, 2008) in Silvia Ceballos, ed, *Proceedings ICMB 2008* (California: IEEE, 2008) 221, DOI:<[10.1109/ICMB.2008.14](https://doi.org/10.1109/ICMB.2008.14)>.
- Derawi, Mohammad Omar et al, “Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition”, (Paper delivered at the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany, 15-17 October 2010) in Isao Echizen et al, eds, *Proceedings IIHMSP 2010* (California: IEEE, 2010) 306, DOI:<[10.1109/IIHMSP.2010.83](https://doi.org/10.1109/IIHMSP.2010.83)>.
- Fabricius, Veronika, Tim Kollmer & Andreas Eckhardt, “Instances of Digital Dark Nudging: Findings of a Systematic Literature Analysis”, (Paper delivered at the AMCIS 2023, Panama City, August 10-12, 10 August 2023) [unpublished] online: <http://web.archive.org/web/20240906165031/https://aisel.aisnet.org/amcis2023/sig_adit/sig_adit/12/>.
- Feld, Michael, Tim Schwartz & Christian Müller, “This Is Me: Using Ambient Voice Patterns for In-Car Positioning” (Paper delivered at the First International Joint Conference Aml, Málaga, Spain, November 10-12, 2010) in Boris Ruyter et al, eds, *Ambient Intelligence* (Berlin: Springer, 2010) 290, DOI:<[10.1007/978-3-642-16917-5_33](https://doi.org/10.1007/978-3-642-16917-5_33)>.
- Gambs, Sébastien, Marc-Olivier Killijian & Miguel Núñez del Prado Cortez, “Show Me How You Move and I Will Tell You Who You Are” (Paper delivered at the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, San Jose, CA, November 2, 2010) in Maria Luisa Damiani & Yucel Saygin, eds, *Springl' 10* (New York: ACM, 2010) 34, DOI:<[10.1145/1868470.1868479](https://doi.org/10.1145/1868470.1868479)>.
- Golle, Philippe & Kurt Partridge, “On the Anonymity of Home/Work Location Pairs” (Paper delivered at the 7th International Conference on Pervasive Computing, Nara, Japan, May 11-14, 2009) in Hideyuki Tokuda et al, eds, *Pervasive Computing* (Verlag: Springer, 2009) 390, DOI:<[10.1007/978-3-642-01516-8_26](https://doi.org/10.1007/978-3-642-01516-8_26)>.
- Jacobs, Bart & Wiebren de Jonge, “Privacy-Friendly Electronic Traffic Pricing via Commits” (Paper delivered at the 5th International Workshop, Formal Aspects in Security and Trust, Malaga, Spain, October 9-10, 2008) in Pierpaolo Degano, Joshua Guttman & Fabio

- Martenelli, eds, *Formal Aspects in Security and Trust* (Berlin: Springer, 2009) 143, DOI:<[10.1007/978-3-642-01465-9_10](https://doi.org/10.1007/978-3-642-01465-9_10)>.
- Khuntia, Mitrabinda, Debabrata Singh & Sipra Sahoo, “Impact of Internet of Things (IoT) on 5G”, (Paper delivered at the 1st International Conference on Intelligent and Cloud Computing, Bhubaneswar, India, December 20, 2019) in Debahuti Mishra et al, eds, *ICICC 2019* (Singapore: Springer, 2021) 125, DOI:<[10.1007/978-981-15-6202-0_14](https://doi.org/10.1007/978-981-15-6202-0_14)>.
- Krumm, John, “Inference Attacks on Location Tracks”, (Paper delivered at the 5th International Conference on Pervasive Computing, Toronto, May 13-16) in Anthony LaMarca, Marc Langheinrich & Khai N. Truong, eds, *Pervasive Computing* (Berlin: Springer, 2007) 127, DOI:<[10.1007/978-3-540-72037-9_8](https://doi.org/10.1007/978-3-540-72037-9_8)>.
- Lampinen, Airi, Fred Stutzman & Markus Bylund, “Privacy for a Networked World: Bridging Theory and Design” (Paper delivered at the CHI Conference on Human Factors in Computing, Vancouver, BC, May 7-12, 2011) in Desney Tan, Bo Begole & Wendy A. Kellogg, eds, *CHI EA’ 11* (New York: ACM, 2011) 2441, DOI:<[10.1145/1979742.1979579](https://doi.org/10.1145/1979742.1979579)>.
- Ma, Chris YT et al, “Privacy Vulnerability of Published Anonymous Mobility Traces” (Paper delivered at the 16th Annual International Conference on Mobile Computing and Networking, Chicago, September 20-24, 2010) in Nitin Vaidya, Suman Banerjee & Dina Katabi, eds, *MobiCom’ 10* (New York: ACM, 2010) 185, DOI:<[10.1145/1859995.1860017](https://doi.org/10.1145/1859995.1860017)>.
- Minch, Robert, “Issues in the Development of Location Privacy Theory” (Paper delivered at the 44th Hawaii International Conference on System Sciences, Kauai, HI, January 4-7, 2011) in Ralph H. Sprague, ed, *Proceedings HICSS 2011* (California: IEEE, 2011), DOI:<[10.1109/HICSS.2011.262](https://doi.org/10.1109/HICSS.2011.262)>.
- Minch, Robert P, “Privacy Issues in Location-Aware Mobile Devices” (Paper delivered at the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, January 5-8, 2004) in Ralph H. Sprague, ed, *Proceedings HICSS 2004* (California: IEEE, 2004) 1, DOI:<[10.1109/HICSS.2004.1265320](https://doi.org/10.1109/HICSS.2004.1265320)>.
- Myllymaki, Jussi & Stefan Edlund, “Location Aggregation from Multiple Sources” (Paper delivered at the 3rd International Conference on Mobile Data Management MDM, Singapore, January 8-11, 2002) in A. Denise Williams, ed, *Proceedings MDM 2002* (California: IEEE, 2002) 131, DOI:<[10.1109/MDM.2002.994393](https://doi.org/10.1109/MDM.2002.994393)>.
- Palen, Leysia & Paul Dourish, “Unpacking ‘Privacy’ for a Networked World” (Paper delivered at the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, FL, April 5–10, 2003) in Gilbert Cockton & Panu Korhonen, eds, *CHI’ 03* (New York: ACM, 2003) 129, DOI:<[10.1145/642611.642635](https://doi.org/10.1145/642611.642635)>.

- Pedersen, Jens, “Privacy and Location Technologies” (Paper delivered at the Workshop on Location System Privacy and Control at Mobile HCI 2004, Glasgow, UK, September 2004) [unpublished] online: <http://web.archive.org/web/20131227142149/http://itu.dk/people/jensp/locationprivacy.pdf>.
- Shilton, Katie, “‘That’s Not An Architecture Problem!’: Techniques and Challenges for Practicing Anticipatory Technology Ethics” (Paper delivered at the iConference 2015, New Port Beach, California, 24 March 2015) [unpublished] online: <https://hdl.handle.net/2142/73672>.
- Shokri, Reza et al, “Quantifying Location Privacy” (Paper delivered at the 2011 IEEE Symposium on Security and Privacy, Oakland, CA, May 22-25, 2011) in Lisa O’Conner, ed, *Proceedings SP 2011* (California: IEEE, 2011) 247, DOI:<[10.1109/SP.2011.18](https://doi.org/10.1109/SP.2011.18)>.
- Snekkenes, Einar, “Concepts for Personal Location Privacy Policies” (Paper delivered at the 3rd ACM conference on Electronic Commerce, Tampa, FL, October 14-17, 2001) in Michael P. Wellman & Yoav Shoham, eds, *EC’ 01* (New York: ACM, 2001) 48, DOI:<[10.1145/501158.501164](https://doi.org/10.1145/501158.501164)>.
- Song, Yi, Daniel Dahlmeier & Stephane Bressan, “Not So Unique in the Crowd: A Simple and Effective Algorithm for Anonymizing Location Data” (Paper delivered at the PIR@SIGIR, Gold Coast, Australia, 11 July 2014) [unpublished] online: <https://dblp.org/rec/conf/sigir/SongDB14.html>.
- Tang, Karen P et al, “Putting People in Their Place: An anonymous and Privacy-Sensitive Approach to Collecting Sensed Data in Location-Based Applications” (Paper delivered at the SIGCHI conference on Human Factors in Computing Systems, Montreal, QC, April 22-27, 2006) in Rebecca Grinter, Thomas Rodden & Paul Aoki, eds, *CHI’ 06* (New York: ACM, 2006) 93, DOI:<[10.1145/1124772.1124788](https://doi.org/10.1145/1124772.1124788)>.
- Trestian, Ionut et al, “Measuring Serendipity: Connecting People, Locations and Interests in a Mobile 3G Network” (Paper delivered at the 9th ACM SIGCOMM Conference on Internet Measurement, Chicago, November 4-6, 2009) in Anja Feldmann & Laurent Mathy, eds, *IMC’ 09* (New York: ACM, 2009) 267, DOI:<[10.1145/1644893.1644926](https://doi.org/10.1145/1644893.1644926)>.
- Tsoukaneri, Galini et al, “On the Inference of User Paths from Anonymized Mobility Data” (Paper delivered at the 1st IEEE European Symposium on Security and Privacy, Saarbrücken, Germany, March 21-24, 2006) in Lisa O’Conner, ed, *Proceedings Euro S&P 2016* (California: IEEE, 2016) 199, DOI:<[10.1109/EuroSP.2016.25](https://doi.org/10.1109/EuroSP.2016.25)>.
- Zang, Hui & Jean Bolot, “Anonymization of Location Data Does Not Work: A Large-scale Measurement Study” (Paper delivered at the 17th Annual International Conference on Mobile Computing and Networking, Las Vegas, September 19-23, 2011) in Parameswaran

Ramanthan, Thyaga Nandagopal & Brian Neil Levine, eds, *MobiCom' 11* (New York: ACM, 2011) 145, DOI:<[10.1145/2030613.2030630](https://doi.org/10.1145/2030613.2030630)>.

Secondary Material: News Articles

“Facebook Buys Instagram For \$1 Billion, Turns Budding Rival into Its Standalone Photo App”, *TechCrunch* (9 April 2012), online: <techcrunch.com> [<https://web.archive.org/web/20190501061701/https://techcrunch.com/2012/04/09/facebook-to-acquire-instagram-for-1-billion/>].

“The Facebook Files”, *Wall Street Journal* (last visited 2 January 2024), online: <[wsj.com](https://www.wsj.com)> [<http://web.archive.org/web/20240102164327/http://web.archive.org/screenshot/https://www.wsj.com/articles/the-facebook-files-11631713039>].

“The Uber files”, *The Guardian* (last visited 2 January 2024), online: <[theguardian.com](https://www.theguardian.com)> [<https://web.archive.org/web/20240102163254/http://web.archive.org/screenshot/https://www.theguardian.com/news/series/uber-files>].

“The Way We Were in 1981: Technology”, *BBC News* (19 November 2010), online: <[bbc.com](https://www.bbc.com)> [<http://web.archive.org/web/20150703031841/https://www.bbc.com/news/uk-11789191>].

“Uber Files Archives”, *International Consortium of Investigative Journalists* (last visited 2 January 2024), online: <[icij.org](https://www.icij.org)> [<http://web.archive.org/screenshot/https://www.icij.org/tags/uber-files/>].

“‘We Will Not Make Excuses’: Uber Responds To Uber Files Leak”, *The Guardian* (10 July 2022), online: <[theguardian.com](https://www.theguardian.com)> [<http://web.archive.org/web/20240102173940/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/10/uber-response-uber-files-leak>].

Alecci, Scilla, “Uber Shifted Scrutiny to Drivers as it Dodged Tens of Millions in Taxes”, *International Consortium of Investigative Journalists* (11 July 2022), online: <[icij.org](https://www.icij.org)> [<http://web.archive.org/web/20240102172331/http://web.archive.org/screenshot/https://www.icij.org/investigations/uber-files/uber-tax-havens-dodge-drivers/>].

Bell, Karissa, “Mark Zuckerberg Promises to Rebuild Facebook as ‘Privacy-Focused’ Social Network”, *Mashable* (6 March 2019), online: <mashable.com> [<http://web.archive.org/web/20240102145430/http://web.archive.org/screenshot/https://mashable.com/article/mark-zuckerberg-privacy-focused-social-network>].

Bhuiyan, Johana & Dan Milmo, “‘Embrace The Chaos’: A History Of Uber’s Rapid Expansion And Fall From Favour”, (15 July 2022), online: <[theguardian.com](https://www.theguardian.com)> [<http://web.archive.org/web/20230730100557/https://www.theguardian.com/news/2022/jul/15/embrace-the-chaos-a-history-of-ubers-rapid-expansion-and-fall-from-favour>].

- Birnbaum, Emily, “Facebook Looking for Its Voice at a ‘Watershed Moment’”, *Politico* (25 October 2021), online: <[politico.com](http://web.archive.org/web/20211026071733/https://www.politico.com/news/2021/10/25/facebook-pr-war-517128)> [http://web.archive.org/web/20211026071733/https://www.politico.com/news/2021/10/25/facebook-pr-war-517128].
- Bourgery-Gonse, Théo, “Uber is Not What it Used to Be, CEO Tells French MPs”, *Euractiv* (26 May 2023), online: <[euractiv.com](http://web.archive.org/web/20240102171148/http://web.archive.org/screenshot/https://www.euractiv.com/section/gig-economy/news/uber-is-not-what-it-used-to-be-ceo-tells-french-mps/)> [http://web.archive.org/web/20240102171148/http://web.archive.org/screenshot/https://www.euractiv.com/section/gig-economy/news/uber-is-not-what-it-used-to-be-ceo-tells-french-mps/].
- Brody, Ben & Bill Allison, “Lobbying Group for Facebook and Google to Pitch Self-Regulation of Ads”, *Bloomberg* (24 October 2017), online: <[bloomberg.com](http://web.archive.org/web/20180509015759/https://www.bloomberg.com/news/articles/2017-10-24/lobby-group-for-facebook-google-to-pitch-self-regulation-of-ads)> [http://web.archive.org/web/20180509015759/https://www.bloomberg.com/news/articles/2017-10-24/lobby-group-for-facebook-google-to-pitch-self-regulation-of-ads].
- Browning, Kellen, “California Court Mostly Upholds Prop. 22 in Win for Uber and Other Gig Companies”, (13 March 2023), online: <[nytimes.com](http://web.archive.org/web/20230314040043/https://www.nytimes.com/2023/03/13/business/prop-22-upheld-california.html)> [http://web.archive.org/web/20230314040043/https://www.nytimes.com/2023/03/13/business/prop-22-upheld-california.html].
- Burgess, Matt, “The Quiet Way Advertisers Are Tracking Your Browsing”, *Wired* (26 February 2022), online: <[wired.com](http://web.archive.org/web/20220328060058/https://www.wired.com/story/browser-fingerprinting-tracking-explained/)> [http://web.archive.org/web/20220328060058/https://www.wired.com/story/browser-fingerprinting-tracking-explained/].
- Cadwalladr, Carole, “‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower”, *The Guardian* (18 March 2018), online: <[theguardian.com](http://web.archive.org/web/20240102144227/https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump)> [http://web.archive.org/web/20240102144227/https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump].
- Cadwalladr, Carole & Duncan Campbell, “Revealed: Facebook’s Global Lobbying Against Data Privacy Laws”, *The Observer* (2 March 2019), online: <[theguardian.com](http://web.archive.org/web/20240102154749/http://web.archive.org/screenshot/https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment)> [http://web.archive.org/web/20240102154749/http://web.archive.org/screenshot/https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment].
- Cadwalladr, Carole & Emma Graham-Harrison, “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach”, *The Guardian* (17 March 2018), online: <[theguardian.com](http://web.archive.org/web/20240102151856/http://web.archive.org/screenshot/https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election)> [http://web.archive.org/web/20240102151856/http://web.archive.org/screenshot/https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election].

- Chew, Jonathan, “7 Corporate Giants Accused of Evading Billions in Taxes”, *Fortune* (11 March 2016), online: <fortune.com> [http://web.archive.org/web/20240722162813/https://fortune.com/2016/03/11/apple-google-taxes-eu/].
- Chrisafis, Angelique, “France Hit by Day of Protest as Security Forces Fire Teargas at Taxi Strike”, *The Guardian* (26 January 2016), online: <theguardian.com> [http://web.archive.org/web/20240102132224/http://web.archive.org/screenshot/https://www.theguardian.com/world/2016/jan/26/french-taxi-drivers-block-paris-roads-in-uber-protest].
- Conger, Kate, Richard Fausset & Serge F Kovalski, “San Francisco Bans Facial Recognition Technology”, *The New York Times* (14 May 2019), online: <nytimes.com> [http://web.archive.org/web/20220709132351/https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html].
- Constine, Josh, “Facebook’s \$2 Billion Acquisition of Oculus Closes, Now Official”, *TechCrunch* (21 July 2014), online: <techcrunch.com> [https://web.archive.org/web/20240115092722/http://web.archive.org/screenshot/https://techcrunch.com/2014/07/21/facebooks-acquisition-of-oculus-closes-now-official/].
- Cook, Tim, “You Deserve Privacy Online. Here’s How You Could Actually Get It”, *Time* (2019), online: <time.com> [http://web.archive.org/web/20220618030148/https://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/].
- Cox, Joseph, “CBP Bought ‘Global’ Location Data from Weather and Game Apps”, (6 October 2020), online: <vice.com> [http://web.archive.org/web/20230329193633/https://www.vice.com/en/article/n7wakg/cbp-dhs-location-data-venntel-apps].
- Davies, Harry et al, “Uber Broke Laws, Duped Police and Secretly Lobbied Governments, Leak Reveals”, *The Guardian* (11 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102170300/https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign].
- Davies, Rob & Johana Bhuiyan, “Uber Used Greyball Fake App To Evade Police Across Europe, Leak Reveals”, *The Guardian* (12 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102172652/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/12/uber-used-greyball-fake-app-to-evade-police-across-europe-leak-reveals].
- Davies, Rob & Simon Goodley, “Uber Bosses Told Staff to Use ‘Kill Switch’ During Raids to Stop Police Seeing Data”, *The Guardian* (10 July 2022), online: <theguardian.com> [http://web.archive.org/web/20240102170046/http://web.archive.org/screenshot/https://w

www.theguardian.com/news/2022/jul/10/uber-bosses-told-staff-use-kill-switch-raids-stop-police-seeing-data].

Dezember, Ryan, “Your Smartphone’s Location Data Is Worth Big Money to Wall Street”, *Wall Street Journal* (2 November 2018), online: <[wsj.com](https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260)> [http://web.archive.org/web/20210624215349/https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260].

Eadicicco, Lisa, “Amazon Developing Advanced Voice-Recognition for Alexa”, *Time* (27 February 2017), online: <[time.com](https://time.com/4683981/amazon-echo-voice-id-feature-2017/)> [http://web.archive.org/web/20180308102426/https://time.com/4683981/amazon-echo-voice-id-feature-2017/].

Elliott, Vittoria, “Meta Lurches Toward Another Moderation Crisis”, *Wired* (23 January 2023), online: <[wired.com](https://www.wired.com/story/metasp-new-moderation-contractor-may-be-worse-than-its-last-one/)> [http://web.archive.org/web/20230821104014/https://www.wired.com/story/metasp-new-moderation-contractor-may-be-worse-than-its-last-one/].

Farber, Dan, “When iPhone met world, 7 years ago today”, *CNET* (9 January 2014), online: <[cnet.com](https://www.cnet.com/tech/tech-industry/when-iphone-met-world-7-years-ago-today/)> [http://web.archive.org/web/20220705220307/https://www.cnet.com/tech/tech-industry/when-iphone-met-world-7-years-ago-today/].

Fitzgerald, Maggie, “The CEOs of Nearly 200 Companies just Said Shareholder Value is No Longer Their Main Objective”, *CNBC* (19 August 2019), online: <[cnbc.com](https://www.cnbc.com/2019/08/19/the-ceos-of-nearly-two-hundred-companies-say-shareholder-value-is-no-longer-their-main-objective.html)> [http://web.archive.org/web/20240102162049/http://web.archive.org/screenshot/https://www.cnbc.com/2019/08/19/the-ceos-of-nearly-two-hundred-companies-say-shareholder-value-is-no-longer-their-main-objective.html].

Fowler, Geoffrey A, “At CES, Apple, Facebook and Amazon are Preaching Privacy. Don’t Believe the Hype”, (8 January 2020), online: <[washingtonpost.com](https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/)> [http://web.archive.org/web/20230608081904/https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/].

Freedberg, Sydney P et al, “How Uber Won Access to World Leaders, Deceived Investigators and Exploited Violence Against Its Drivers in Battle for Global Dominance”, *International Consortium of Investigative Journalists* (10 July 2022), online: <[icij.org](https://www.icij.org/investigations/uber-files/uber-global-rise-lobbying-violence-technology/)> [http://web.archive.org/web/20240102143849/https://www.icij.org/investigations/uber-files/uber-global-rise-lobbying-violence-technology/].

Hagey, Keach et al, “Facebook’s Pushback: Stem the Leaks, Spin the Politics, Don’t Say Sorry”, *Wall Street Journal* (29 December 2021), online: <[wsj.com](https://www.wsj.com/articles/facebook-whistleblower-pushback-political-spin-zuckerberg-11640786831)> [http://web.archive.org/web/20240102130635/http://web.archive.org/screenshot/https://www.wsj.com/articles/facebook-whistleblower-pushback-political-spin-zuckerberg-11640786831].

- Hagey, Keach & Jeff Horwitz, “Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead”, *Wall Street Journal* (15 September 2021), online: <[wsj.com](https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215)> [https://web.archive.org/web/20240102124309/http://web.archive.org/screenshot/https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215].
- Hern, Alex, “Facebook Owner To Settle Class-Action Suit Over Cambridge Analytica Scandal”, *The Guardian* (23 December 2022), online: <[theguardian.com](https://www.theguardian.com/business/2022/dec/23/facebook-owner-to-settle-class-action-suit-over-cambridge-analytica-scandal)> [https://web.archive.org/web/20240102122349/https://www.theguardian.com/business/2022/dec/23/facebook-owner-to-settle-class-action-suit-over-cambridge-analytica-scandal].
- Hopkins, Nick, “Why We Are Shining a Light on the World of Tax Havens Again”, *The Guardian* (5 November 2017), online: <[theguardian.com](http://www.theguardian.com/news/2017/nov/05/why-shining-light-world-tax-havens-again-paradise-papers)> [http://web.archive.org/web/20240415074926/https://www.theguardian.com/news/2017/nov/05/why-shining-light-world-tax-havens-again-paradise-papers].
- Isaac, Mike, “Uber Uses Tech to Deceive Authorities Worldwide”, *The New York Times* (4 March 2017), online: <[nytimes.com](http://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html?searchResultPosition=1)> [http://web.archive.org/web/20200210205756/https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html?searchResultPosition=1].
- Jee, Charlotte, “Google Has Promised to Make it Easier to Protect your Privacy”, *MIT Technology Review* (8 May 2019), online: <[technologyreview.com](http://www.technologyreview.com/2019/05/08/135461/google-has-promised-to-make-it-easier-to-protect-your-privacy/)> [http://web.archive.org/web/20240102133757/https://www.technologyreview.com/2019/05/08/135461/google-has-promised-to-make-it-easier-to-protect-your-privacy/].
- Keegan, Jon & Alfred Ng, “There’s a Multibillion-Dollar Market for Your Phone’s Location Data”, *The Markup* (30 September 2021), online: <[themarkup.org](http://themarkup.org/privacy/2021/09/30/heres-a-multibillion-dollar-market-for-your-phones-location-data)> [http://web.archive.org/web/20211001105321/https://themarkup.org/privacy/2021/09/30/heres-a-multibillion-dollar-market-for-your-phones-location-data].
- Korosec, Kirsten, “How Stellantis Plans to Make \$22.5B a Year from Software in its Cars, Trucks and SUVs”, *TechCrunch* (7 December 2021), online: <[techcrunch.com](https://techcrunch.com/2021/12/07/how-stellantis-plans-to-make-22-5b-a-year-from-software-in-its-cars-trucks-and-suvs/)> [http://web.archive.org/web/20220103175622/https://techcrunch.com/2021/12/07/how-stellantis-plans-to-make-22-5b-a-year-from-software-in-its-cars-trucks-and-suvs/].
- Lawrence, Felicity, “‘They Were Taking Us for a Ride’: How Uber Used Investor Cash to Seduce Drivers”, *The Guardian* (12 July 2022), online: <[theguardian.com](http://www.theguardian.com/news/2022/jul/12/they-were-taking-us-for-a-ride-how-uber-used-investor-cash-to-seduce-drivers)> [http://web.archive.org/web/20240102165430/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/12/they-were-taking-us-for-a-ride-how-uber-used-investor-cash-to-seduce-drivers].
- Lawrence, Felicity & Jon Henley, “‘Violence Guarantees Success’: How Uber Exploited Taxi Protests”, *The Guardian* (10 July 2022), online: <[theguardian.com](http://www.theguardian.com/news/2022/jul/10/violence-guarantees-success-how-uber-exploited-taxi-protests)> [http://web.archive.org/web/20240102173558/http://web.archive.org/screenshot/https://www.theguardian.com/news/2022/jul/10/violence-guarantees-success-how-uber-exploited-taxi-protests].

- Letzing, John, “Facebook Buys More Talent With Gowalla Deal”, *Wall Street Journal* (5 December 2011), online: <[wsj.com](https://www.wsj.com/articles/BL-DGB-23623)> [http://web.archive.org/web/20240102120405/https://www.wsj.com/articles/BL-DGB-23623].
- Levin, Sam, “Uber Lawsuits Timeline: Company Ordered to Pay Out \$161.9m since 2009”, *The Guardian* (13 April 2016), online: <[theguardian.com](https://www.theguardian.com/technology/2016/apr/13/uber-lawsuits-619-million-ride-hailing-app)> [http://web.archive.org/web/20240102171330/https://www.theguardian.com/technology/2016/apr/13/uber-lawsuits-619-million-ride-hailing-app].
- Lomas, Natasha, “Facebook Ignored Staff Warnings about ‘Sketchy’ Cambridge Analytica in September 2015”, *TechCrunch* (25 July 2019), online: <[techcrunch.com](https://techcrunch.com/2019/07/25/facebook-ignored-staff-warnings-about-sketchy-cambridge-analytica-in-september-2015/)> [http://web.archive.org/web/20190823164659/https://techcrunch.com/2019/07/25/facebook-ignored-staff-warnings-about-sketchy-cambridge-analytica-in-september-2015/].
- , “Report Reveals how Big Tech Lobbied to Weaken EU Rules”, *TechCrunch* (22 April 2022), online: <[techcrunch.com](https://techcrunch.com/2022/04/22/google-facebook-apple-eu-lobbying-report/)> [http://web.archive.org/web/20240102151532/http://web.archive.org/screenshot/https://techcrunch.com/2022/04/22/google-facebook-apple-eu-lobbying-report/].
- , “Uber Lobbies for ‘Prop 22’-Style Gig Work Standards in the EU”, *TechCrunch* (15 February 2021), online: <[techcrunch.com](https://techcrunch.com/2021/02/15/uber-lobbies-for-prop-22-style-gig-work-standards-in-the-eu/)> [http://web.archive.org/web/20240102171758/http://web.archive.org/screenshot/https://techcrunch.com/2021/02/15/uber-lobbies-for-prop-22-style-gig-work-standards-in-the-eu/].
- Medina, Brenda, “As Uber Expanded Globally, Many Drivers Felt Left Behind”, (19 July 2022), online: <[icij.org](https://www.icij.org/investigations/uber-files/as-uber-expanded-globally-many-drivers-felt-left-behind/)> [http://web.archive.org/web/20230531005548/https://www.icij.org/investigations/uber-files/as-uber-expanded-globally-many-drivers-felt-left-behind/].
- Medina, Brenda & Nicole Sadek, “‘We Co-Opted Democracy,’ Uber Files Whistleblower Tells European Parliament”, *International Consortium of Investigative Journalists* (25 October 2022), online: <[icij.org](https://www.icij.org/investigations/uber-files/we-co-opted-democracy-uber-files-whistleblower-tells-european-parliament/)> [http://web.archive.org/web/20240102173748/http://web.archive.org/screenshot/https://www.icij.org/investigations/uber-files/we-co-opted-democracy-uber-files-whistleblower-tells-european-parliament/].
- Newton, Casey, “The Trauma Floore: The Secret Lives of Facebook Moderators in America”, *The Verge* (25 February 2019), online: <[theverge.com](https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona)> [http://web.archive.org/web/20240102162750/https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona].
- O’Hare, Ryan, “Software Analyses Your Unique Gait from CCTV Footage”, *Daily Mail* (15 February 2016), online: <[dailymail.co.uk](https://www.dailymail.co.uk)>

- [<http://web.archive.org/web/20240102160415/http://web.archive.org/screenshot/https://www.dailymail.co.uk/sciencetech/article-3447957/Nowhere-run-Software-identify-way-WALK-using-grainy-CCTV-footage.html>].
- Panzarino, Matthew, “Facebook Buying WhatsApp For \$19B, Will Keep The Messaging Service Independent”, (19 February 2014), online: <[techcrunch.com](http://web.archive.org/web/20230306013400/https://techcrunch.com/2014/02/19/facebook-buying-whatsapp-for-16b-in-cash-and-stock-plus-3b-in-rsus/)> [<http://web.archive.org/web/20230306013400/https://techcrunch.com/2014/02/19/facebook-buying-whatsapp-for-16b-in-cash-and-stock-plus-3b-in-rsus/>].
- Paul, Kari & Julia Carrie Wong, “California Passes Prop 22 in a Major Victory for Uber and Lyft”, (4 November 2020), online: <[theguardian.com](http://web.archive.org/web/20230714162120/https://www.theguardian.com/us-news/2020/nov/04/california-election-voters-prop-22-uber-lyft)> [<http://web.archive.org/web/20230714162120/https://www.theguardian.com/us-news/2020/nov/04/california-election-voters-prop-22-uber-lyft>].
- Perrigo, Billy, “Inside Facebook’s African Sweatshop”, *Time* (14 February 2022), online: <[time.com](http://web.archive.org/web/20230802045128/https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/)> [<http://web.archive.org/web/20230802045128/https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/>].
- Pichai, Sundar, “Google’s Sundar Pichai: Privacy Should Not Be a Luxury Good”, *The New York Times* (8 May 2019), online: <[nytimes.com](http://web.archive.org/web/20190701181756/https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html)> [<http://web.archive.org/web/20190701181756/https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html>].
- Raymond, Nate, “Facebook Parent Meta to Settle Cambridge Analytica Scandal Case for \$725 Million”, *Reuters* (23 December 2022), online: <[reuters.com](http://web.archive.org/web/20231016162427/https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/)> [<http://web.archive.org/web/20231016162427/https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/>].
- Romer, Paul, “A Tax That Could Fix Big Tech”, *The New York Times* (6 May 2019), online: <[nytimes.com](http://web.archive.org/web/20241010054039/https://www.nytimes.com/2019/05/06/opinion/tax-facebook-google.html)> [<http://web.archive.org/web/20241010054039/https://www.nytimes.com/2019/05/06/opinion/tax-facebook-google.html>].
- Schaake, Marietje, “Lobbying for Unfettered Innovation is Bad for Democracy”, *Financial Times* (24 September 2024), online: <[ft.com](http://web.archive.org/web/20240924040335/https://www.ft.com/content/ab2761bd-ace7-428b-aa3e-b7412ef69b48)> [<http://web.archive.org/web/20240924040335/https://www.ft.com/content/ab2761bd-ace7-428b-aa3e-b7412ef69b48>].
- Scheck, Justin, Newley Purnell & Jeff Horwitz, “Facebook Employees Flag Drug Cartels and Human Traffickers. The Company’s Response Is Weak, Documents Show.”, *Wall Street Journal* (16 September 2021), online: <[wsj.com](http://web.archive.org/web/20240102120837/https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953)> [<http://web.archive.org/web/20240102120837/https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953>].

- Scheiber, Noam, “How Uber Uses Psychological Tricks to Push Its Drivers’ Buttons”, *The New York Times* (2 April 2017), online: <[nytimes.com](http://web.archive.org/web/20240102120103/https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?smid=pl-share)> [http://web.archive.org/web/20240102120103/https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?smid=pl-share].
- Shieber, Jonathan, “Facebook Suspends Cambridge Analytica, the Data Analysis Firm that Worked on the Trump Campaign”, *TechCrunch* (17 March 2018), online: <[techcrunch.com](https://web.archive.org/web/20240102123256/http://web.archive.org/screenshot/https://techcrunch.com/2018/03/16/facebook-suspends-cambridge-analytica-the-data-analysis-firm-that-worked-for-the-trump-campaign/)> [https://web.archive.org/web/20240102123256/http://web.archive.org/screenshot/https://techcrunch.com/2018/03/16/facebook-suspends-cambridge-analytica-the-data-analysis-firm-that-worked-for-the-trump-campaign/].
- Schneier, Bruce, “The Public-Private Surveillance Partnership”, *Bloomberg* (1 August 2013), online: <[bloomberg.com](http://web.archive.org/web/20201112024906/https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership)> [http://web.archive.org/web/20201112024906/https://www.bloomberg.com/opinion/articles/2013-07-31/the-public-private-surveillance-partnership].
- Solove, Daniel J, “Facebook’s Psych Experiment: Consent, Privacy, And Manipulation”, *The Huffington Post* (30 June 2014), online: <[huffingtonpost.com](http://web.archive.org/web/20240102125002/http://web.archive.org/screenshot/http://www.huffingtonpost.com/daniel-j-solove/facebook-psych-experiment_b_5545372.html)> [http://web.archive.org/web/20240102125002/http://web.archive.org/screenshot/http://www.huffingtonpost.com/daniel-j-solove/facebook-psych-experiment_b_5545372.html].
- Soltani, Ashkan & Barton Gellman, “New Documents Show How the NSA Infers Relationships based on Mobile Location Data”, *Washington Post* (10 December 2013), online: <[washingtonpost.com](http://web.archive.org/web/20180219012613/https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?utm_term=.fc24fe7d991b)> [http://web.archive.org/web/20180219012613/https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?utm_term=.fc24fe7d991b].
- Soper, Spencer, “Amazon Pitches Facial Recognition to Monitor Immigrants”, (23 October 2018), online: <[bloomberg.com](http://web.archive.org/web/20181106103109/https://www.bloomberg.com/news/articles/2018-10-23/amazon-pitches-facial-recognition-tools-to-monitor-immigrants)> [http://web.archive.org/web/20181106103109/https://www.bloomberg.com/news/articles/2018-10-23/amazon-pitches-facial-recognition-tools-to-monitor-immigrants].
- Temperton, James, “Apple Ordered to Pay €13bn in Back Taxes over ‘Illegal’ Deal in Ireland” *Wired* (30 August 2016), online: <[wired.com](http://web.archive.org/web/20240814024236/https://www.wired.com/story/apple-tax-european-commission-ireland-amount/)> [http://web.archive.org/web/20240814024236/https://www.wired.com/story/apple-tax-european-commission-ireland-amount/]. The New York Times, “How The Times Analyzed Location Tracking Companies”, *The New York Times* (10 December 2018), online: <[nytimes.com](http://web.archive.org/web/20190101020451/https://www.nytimes.com/2018/12/10/technology/location-tracking-apps-privacy.html)> [http://web.archive.org/web/20190101020451/https://www.nytimes.com/2018/12/10/technology/location-tracking-apps-privacy.html].
- Thompson, Stuart A & Charlie Warzel, “Smartphones Are Spies. Here’s Whom They Report To”, *The New York Times* (20 December 2019), online: <[nytimes.com](https://www.nytimes.com)>

- [<http://web.archive.org/web/20240102150117/http://web.archive.org/screenshot/https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html>].
- , “Twelve Million Phones, One Dataset, Zero Privacy”, *The New York Times* (19 December 2019), online: <[nytimes.com](https://www.nytimes.com)> [<http://web.archive.org/web/20240102151033/https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>].
- Tsotsis, Alexia, “Facebook Buys Location-Based Discovery App Glancee”, *TechCrunch* (5 May 2012), online: <techcrunch.com> [<http://web.archive.org/web/20140525172610/http://techcrunch.com/2012/05/04/facebook-k-buys-location-based-discovery-app-glancee/>].
- Tsukayama, Hayley, “Why It Matters that Google Home Can Now Identify You by Voice”, *The Washington Post* (20 April 2017), online: <[washingtonpost.com](https://www.washingtonpost.com)> [http://web.archive.org/web/20170421012451/https://www.washingtonpost.com/web/20170421012451/https://www.washingtonpost.com/news/the-switch/wp/2017/04/20/why-it-matters-that-google-home-can-now-identify-you-by-voice/?utm_term=.8e5e3b86e2aa].
- Valentino-DeVries, Jennifer et al, “Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret”, *New York Times* (10 December 2018), online: <[nytimes.com](https://www.nytimes.com)> [<http://web.archive.org/web/20240102115358/https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?smid=nytcore-ios-share#>].
- Walle, Thomas, “Untangling the Location Data Ecosystem”, *Street Fight* (29 October 2018), online: <streetfightmag.com> [<http://web.archive.org/web/20200621205557/https://streetfightmag.com/2018/10/29/untangling-the-location-data-ecosystem/>].
- Warzel, Charlie & Stuart A Thompson, “They Stormed the Capitol. Their Apps Tracked Them.”, *The New York Times* (5 February 2021), online: <[nytimes.com](https://www.nytimes.com)> [<http://web.archive.org/web/20240102150552/https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html>].
- Welch, Chris, “Amazon’s Alexa Can Now Recognize Different Voices and Give Personalized Responses”, (11 October 2017), online: <theverge.com> [<http://web.archive.org/web/20181023112538/https://www.theverge.com/circuitbreaker/2017/10/11/16460120/amazon-echo-multi-user-voice-new-feature>].
- Wong, Julia Carrie, “Greyball: How Uber Used Secret Software to Dodge the Law”, *The Guardian* (4 March 2017), online: <theguardian.com> [<http://web.archive.org/web/20170313181501/https://www.theguardian.com/technology/2017/mar/03/uber-secret-program-greyball-resignation-ed-baker>].

Secondary Material: Blogposts

“Capitalism’t: Why We Should Tax Digital Advertising” (11 March 2021) online (podcast):
<chicagobooth.edu>

[<http://web.archive.org/web/20240805064608/https://www.chicagobooth.edu/review/capitalism-why-we-should-tax-digital-advertising>].

Blank, Steve, “What’s A Startup? First Principles” (25 January 2010) online (blog):
<steveblank.com>

[<http://web.archive.org/web/20231221115305/https://steveblank.com/2010/01/25/whats-a-startup-first-principles/>].

Bryant, Jennifer, “Uber’s CPO on Embracing the Challenge of Privacy” (19 October 2020) online (blog):
<iapp.org>

[<http://web.archive.org/web/20230325204334/https://iapp.org/news/a/uber-cpo-the-turn-around-queen-embraces-the-challenge-of-privacy/>].

Burke, Melissa, “The Nuts and Bolts of Location Intelligence” (8 March 2018) online (blog):
<skyhook.com>

[<http://web.archive.org/web/20231221120252/https://www.skyhook.com/blog/nuts-and-bolts-of-location-intelligence/>].

Cino, Jessica Gabel, “Facial Recognition is Increasingly Common, but How Does It Work?” (4 April 2017) online (blog): <theconversation.com>

[<http://web.archive.org/web/20231221152836/https://theconversation.com/facial-recognition-is-increasingly-common-but-how-does-it-work-61354>].

ICRC, “The 1864 Geneva Convention” (18 August 2013) online (blog): <icrc.org>

[<http://web.archive.org/web/20231221120504/https://www.icrc.org/en/doc/resources/documents/treaty/geneva-convention-1864.htm>].

Kitchin, Rob, “Continuous Geosurveillance in the ‘Smart City’” (last visited 2 May 2018) online (blog): <dismagazine.com>

[<http://web.archive.org/web/20231221151522/http://dismagazine.com/dystopia/73066/rob-kitchin-spatial-big-data-and-geosurveillance/>].

Lively, Taylor Kay, “The Way the Third-Party Cookie Crumble: Part 2 Shifting Industry Practices and Alternatives to Third-Party Cookies” (9 December 2021) online (blog): <iapp.org>

[<http://web.archive.org/web/20231218064654/https://iapp.org/news/a/the-way-the-third-party-cookie-crumbles-part-2-shifting-industry-practices-and-alternatives-to-third-party-cookies/>].

———, “The Way the Third-Party Cookie Crumbles: Part 1 EU and UK Developments” (7 December 2021) online (blog): <iapp.org>

[<http://web.archive.org/web/20230922104837/https://iapp.org/news/a/the-way-the-third-party-cookie-crumbles-part-1-eu-and-uk-developments/>].

Milanovic, Marko, “The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa” (26 May 2021) online (blog): <[ejiltalk.org](http://web.archive.org/web/20230603080359/https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/)> [<http://web.archive.org/web/20230603080359/https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/>].

Mitnick, Drew, “UN Special Rapporteur Report on Mass Surveillance: Much to Like, Some to Debate” (17 October 2014) online (blog): <[www.accessnow.org](http://web.archive.org/web/20230927124030/https://www.accessnow.org/un-special-rapporteur-report-on-mass-surveillance-much-to-like-some-to-deba/)> [<http://web.archive.org/web/20230927124030/https://www.accessnow.org/un-special-rapporteur-report-on-mass-surveillance-much-to-like-some-to-deba/>].

Moerel, Lokke, “GDPR Conundrums: Processing Special Categories of Data” (12 September 2016) online (blog): <[iapp.org](http://web.archive.org/web/20231221153045/https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/)> [<http://web.archive.org/web/20231221153045/https://iapp.org/news/a/gdpr-conundrums-processing-special-categories-of-data/>].

Schneier, Bruce, “Metadata Equals Surveillance” (23 September 2013) online (blog): <[schneier.com](http://web.archive.org/web/20230925103941/https://www.schneier.com/blog/archives/2013/09/metadata_equals.html/)> [http://web.archive.org/web/20230925103941/https://www.schneier.com/blog/archives/2013/09/metadata_equals.html/].

Siminoff, Jaimie, “Introducing Ring Always Home Cam: An Innovative New Approach to Always Being Home” (24 September 2020) online (blog): <[blog.ring.com](http://web.archive.org/web/20231221142722/https://blog.ring.com/2020/09/24/introducing-ring-always-home-cam-an-innovative-new-approach-to-always-being-home/)> [<http://web.archive.org/web/20231221142722/https://blog.ring.com/2020/09/24/introducing-ring-always-home-cam-an-innovative-new-approach-to-always-being-home/>].

Wolford, Ben, “Privacy Washing: Google’s Attempts to Redefine What Privacy Means” (7 August 2023) online (blog): <proton.me/blog>.

Zalnieriute, Monika, “A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence” (4 June 2021) online (blog): <[ejiltalk.org](http://web.archive.org/web/20231221143013/https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/)> [<http://web.archive.org/web/20231221143013/https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/>].

Secondary Material: Corporations Documents

Meta Platforms Inc

SEC Documents

Facebook Inc, *Registration Statement (Form S-1)*, Registration No.333-179287 (United States Securities and Exchange Commission, 2012).

Meta Platforms Inc, *Annual Report 2021 (Form 10-K)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2022).

———, *Annual Report 2022 (Form 10-K)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2023).

———, *Quarterly Report Q3 (Form 10-Q)*, Commission File Number: 001-35551 (United States Securities and Exchange Commission, 2023).

———, *Annual Report 2023 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2023).

Newsroom

Clark, Mike, “Privacy Matters: Meta’s Generative AI Features” (27 September 2023) online (Newsroom): [<about.fb.com/news>](https://about.fb.com/news/2023/09/privacy-matters-metas-generative-ai-features/)
[<http://web.archive.org/web/20231010061401/https://about.fb.com/news/2023/09/privacy-matters-metas-generative-ai-features/>].

Egan, Erin, “Marking Data Privacy Day 2019” (28 January 2019) online (Newsroom): [<about.fb.com/news>](https://about.fb.com/news/2019/01/data-privacy-day/)
[<http://web.archive.org/web/20230923021031/https://about.fb.com/news/2019/01/data-privacy-day/>].

Protti, Michel, “Building and Innovating With Privacy in Mind” (23 January 2023) online (Newsroom): [<about.fb.com/news>](https://about.fb.com/news/2023/01/building-and-innovating-with-privacy-in-mind/)
[<http://web.archive.org/web/20231221150511/https://about.fb.com/news/2023/01/building-and-innovating-with-privacy-in-mind/>].

Meta, “Facebook and Instagram to Offer Subscription for No Ads in Europe” (30 October 2023) online (Newsroom): [<about.fb.com/news>](https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/)
[<http://web.archive.org/web/20231221152119/https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>].

- , “Facebook Here Together (UK)” (25 April 2018) online (video): <[youtube.com](https://www.youtube.com/watch?v=Q4zd7X98eOs)> [http://web.archive.org/web/20231220131821/https://www.youtube.com/watch?v=Q4zd7X98eOs].
- , “Facebook to Acquire Oculus” (25 March 2014) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221152403/https://about.fb.com/news/2014/03/facebook-to-acquire-oculus/].
- , “How Meta Uses Legal Bases for Processing Ads in the EU” (last visited 21 December 2023) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221153329/https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/].
- , “Introducing Portal From Facebook: New Video Calling Devices to Connect You With Friends and Family” (8 October 2018) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221153652/https://about.fb.com/news/2018/10/introducing-portal/].
- , “Introducing Ray-Ban Stories: First-Generation Smart Glasses” (last visited 15 March 2023) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20231221153854/https://about.fb.com/news/2021/09/introducing-ray-ban-stories-smart-glasses/].
- , “Meet the New Portal Family: Smart Video Calling on Your TV and Anywhere in Your Home” (18 September 2019) online (Newsroom): <about.fb.com/news> [http://web.archive.org/web/20230921195319/https://about.fb.com/news/2019/09/meet-the-new-portal-family/].
- , “Meta Platforms Technologies Products Definition” (last visited 20 September 2023) online: <https://www.meta.com/gb/legal/meta-platforms-technologies-products/?utm_source=www.facebook.com&utm_medium=dollyredirect>.
- Meta, “Privacy Policy” (last visited 28 August 2024) online (Privacy Center): <<https://www.facebook.com/privacy/policy>>.
- , “Privacy Policy: How We Use Location-Related Information” (last visited 1 December 2022) online (Privacy Center): <<https://www.facebook.com/privacy/policy/?subpage=2.subpage.6-HowWeUseLocation>>.

- , “Privacy Policy: Personalizing Ads for You and Others” (last visited 5 January 2023) online (Privacy Center): [https://www.facebook.com/privacy/policy/?annotations\[0\]=2.story.3-PersonalizingAdsForYou&subpage=2.subpage.6-HowWeUseLocation](https://www.facebook.com/privacy/policy/?annotations[0]=2.story.3-PersonalizingAdsForYou&subpage=2.subpage.6-HowWeUseLocation).
- , “Privacy Policy: What Products Does This Policy Cover?” (last visited 5 January 2023) online (Privacy Center): [https://www.facebook.com/privacy/policy/?annotations\[0\]=0.ex.0-WhatProductsDoesThis](https://www.facebook.com/privacy/policy/?annotations[0]=0.ex.0-WhatProductsDoesThis).
- , “Ray-Ban Meta Smart Glasses” (last visited 20 December 2023) online: <https://www.meta.com/gb/smart-glasses/>.
- , “Recapping Our Privacy Controls on Data Privacy Day” (28 January 2021) online (Newsroom): [about.fb.com/news](https://about.fb.com/news/2021/01/recapping-our-privacy-controls-on-data-privacy-day/) [http://web.archive.org/web/20230520175443/https://about.fb.com/news/2021/01/recapping-our-privacy-controls-on-data-privacy-day/].
- , “Recapping Our Privacy Efforts on Data Privacy Day” (28 January 2022) online (Newsroom): [about.fb.com/news](https://about.fb.com/news/2022/01/recapping-our-privacy-efforts-on-data-privacy-day/) [http://web.archive.org/web/20230913013408/https://about.fb.com/news/2022/01/recapping-our-privacy-efforts-on-data-privacy-day/].
- , “Suspending Cambridge Analytica and SCL Group From Facebook” (17 March 2018) online (Newsroom): [about.fb.com/news](https://about.fb.com/news/2018/03/suspending-cambridge-analytica/) [http://web.archive.org/web/20230427101118/https://about.fb.com/news/2018/03/suspending-cambridge-analytica/].
- , “WhatsApp” (last visited 20 September 2023) online: <https://about.meta.com/uk/technologies/whatsapp/>.
- Meta Inc, “Meta Human Rights Report: Insights and Actions 2020-2021” (July 2022) online (PDF): https://about.fb.com/wp-content/uploads/2022/07/Meta_Human-Rights-Report-July-2022.pdf.
- Zuckerberg, Mark, “Our Commitment to the Facebook Community” (29 November 2011) online: blog.facebook.com [https://web.archive.org/web/20111130104852/http://blog.facebook.com/blog.php?post=10150378701937131].
- , “A Privacy-Focused Vision for Social Networking” (26 September 2018) online: facebook.com/notes/mark-zuckerberg

[https://webcache.googleusercontent.com/search?q=cache:Ts_epQrWoysJ:https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/&cd=1&hl=en&ct=clnk&gl=ch].

———, “A Privacy-Focused Vision for Social Networking” (6 March 2019) online (Newsroom): about.fb.com/news [<http://web.archive.org/web/20231221143617/https://about.fb.com/news/2019/03/vision-for-social-networking/>].

———, “Founder’s Letter, 2021” (28 October 2021) online (Newsroom): about.fb.com/news [<http://web.archive.org/web/20231221152944/https://about.fb.com/news/2021/10/founders-letter/>].

Uber Technologies Inc

SEC Documents

Uber Technologies Inc, *Registration Statement (Form S-1)*, Registration No. 333-230812 (United States Securities and Exchange Commission, 2019).

———, *Annual Report 2021 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2022).

———, *Annual Report 2022 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2023).

———, *Annual Report 2023 (Form 10-K)*, Commission File Number: 001-38902 (United States Securities and Exchange Commission, 2023).

Blogposts

Mansukhani, Ha, “Rideshare in California is at Risk” (18 August 2020) online (blog): uber.com/blog [<http://web.archive.org/web/20231005010747/https://www.uber.com/blog/rideshare-in-california-is-at-risk/>].

Voytek, “Rides of Glory” (26 March 2012) online (blog): blog.uber.com [<https://web.archive.org/web/20141118192805/https://blog.uber.com/ridesofglory>].

Yang, Jessie, “5 Tips to Protect Your Data Privacy with Uber” (26 January 2023) online (blog): medium.com/uber-security-privacy/

[<http://web.archive.org/web/20231221142446/https://medium.com/uber-security-privacy/5-tips-to-protect-your-data-privacy-with-uber-d6e2edf792f9>].

Zefo, Ruby, “Celebrating Data Privacy Every Day” (25 January 2021) online (blog): [<medium.com/uber-security-privacy/>](https://medium.com/uber-security-privacy/)
[<http://web.archive.org/web/20231221150901/https://medium.com/uber-security-privacy/celebrating-data-privacy-every-day-5809e9aa367c>].

Newsroom

Danker, Daniel, “Arriving Now: The New Uber Eats” (7 October 2020) online (Newsroom): uber.com [<http://web.archive.org/save/https://www.uber.com/newsroom/arriving-now-the-new-uber-eats/>].

Hazelbaker, Jill, “Statement on the ICIJ Investigation” (10 July 2022) online (Newsroom): uber.com
[<http://web.archive.org/web/20231221121214/https://www.uber.com/newsroom/icij-statement/>].

Spaeth, Molly, “Class Action Settlement” (11 February 2016) online (Newsroom): uber.com
[<http://web.archive.org/web/20231221151337/https://www.uber.com/newsroom/class-action-settlement/>].

Uber, “Cheers! Uber Completes Acquisition of Drizly” (13 October 2021) online (Press Release): investor.uber.com
[<http://web.archive.org/web/20231220122715/https://investor.uber.com/news-events/news/press-release-details/2021/Cheers-Uber-Completes-Acquisition-of-Drizly/default.aspx>].

———, “Privacy Overview” (last visited 20 December 2023) online: <https://www.uber.com/global/en/privacy/overview/>.

———, “Uber Apps, Products, and Offerings” (last visited 20 September 2023) online: <https://www.uber.com/us/en/about/uber-offerings/>.

———, “Uber Connect” (last visited 2 November 2023) online: uber.com
[<http://web.archive.org/web/20231111214123/https://www.uber.com/us/en/item-delivery/>].

———, “Uber Privacy Notice (6/13/2022)” (13 June 2022) online: <https://www.uber.com/legal/en/document/>.

———, “Uber Privacy Notice (12/1/2023)” (12 January 2023) online: <<https://www.uber.com/legal/en/document/>>.

———, “Uber’s Lime Scooter Partnership” (last visited 2 November 2023) online (Help): <<https://help.uber.com/riders/article/ubers-lime-scooter-partnership?nodeId=80c4aa93-02b6-4a56-af22-d20ff487b8ac>>.

———, “Uber Privacy Notice (7/17/2024)” (last visited 28 August 2024) online: <<https://www.uber.com/legal/en/document/>>.

Uber Freight, “About us” (last visited 2 November 2023) online: <[uberfreight.com](http://web.archive.org/web/20231219172124/https://www.uberfreight.com/about-us/)> [http://web.archive.org/web/20231219172124/https://www.uberfreight.com/about-us/].

Uber Inc, “ESG Report 2022” (last visited 28 April 2023) online (PDF): <<https://uber.app.box.com/s/7otjaxo7978mio4x59kqovh47dopp4w>>.

H & M Hennes & Mauritz AB (H&M Group)

H&M Group, *Annual and Sustainability Report 2023* (H&M Group, 2023).

H&M Group, “About us” (last visited 22 October 2024) online: <[hmgroupprd-app.azurewebsites.net](http://web.archive.org/web/20241003210330/https://hmgroupprd-app.azurewebsites.net/about-us/)> [http://web.archive.org/web/20241003210330/https://hmgroupprd-app.azurewebsites.net/about-us/].

———, “History” (last visited 22 October 2024) online: <[hmgroupprd-app.azurewebsites.net](http://web.archive.org/web/20241003205903/https://hmgroupprd-app.azurewebsites.net/about-us/history/)> [http://web.archive.org/web/20241003205903/https://hmgroupprd-app.azurewebsites.net/about-us/history/].

———, “H&M Group Privacy Notice Canada” (September 2024) online: <[hm.com](http://web.archive.org/web/20230325072615/https://www2.hm.com/content/dam/Customer-Service/Legal/privacy-notice-pdf/en-CA_HM%20Group%20Customer%20Privacy%20Notice.pdf)> [http://web.archive.org/web/20230325072615/https://www2.hm.com/content/dam/Customer-Service/Legal/privacy-notice-pdf/en-CA_HM%20Group%20Customer%20Privacy%20Notice.pdf].

———, “H&M Group Privacy Notice EU” (October 2024) online: <[hm.com](http://web.archive.org/web/20240519040619/https://www2.hm.com/content/dam/Customer-Service/Legal/privacy-notice-pdf/IE_HM%20Group%20Customer%20Privacy%20Notice.pdf)> [http://web.archive.org/web/20240519040619/https://www2.hm.com/content/dam/Customer-Service/Legal/privacy-notice-pdf/IE_HM%20Group%20Customer%20Privacy%20Notice.pdf].

———, “H&M Group Privacy Notice: General” (June 2024) online: <[hmgroupprd-app.azurewebsites.net](http://web.archive.org/web/20241003220534/https://hmgroupprd-app.azurewebsites.net/legal-notice/)> [http://web.archive.org/web/20241003220534/https://hmgroupprd-app.azurewebsites.net/legal-notice/].

———, “Organization and Management” (last visited 22 October 2024) online: <[hmgroupprd-app.azurewebsites.net](http://web.archive.org/web/20241003220534/https://hmgroupprd-app.azurewebsites.net/legal-notice/)>.

app.azurewebsites.net> [http://web.archive.org/web/20241003210147/https://hmggroup-prd-app.azurewebsites.net/about-us/corporate-governance/company-management/].

Stallantis N.V.

Stellantis N.V., *Annual Report for the Year Ended December 31, 2023* (Stellantis N.V., 2023).

Stellantis, “Appendix II : European Connected Vehicles Privacy Policy” (last visited 16 October 2024) online (PDF): <[services-store.peugeot.co.uk](https://services-store.peugeot.co.uk/sites/peugeot/files/2024-02/Privacy%20Policy%20UK%2010-23.pdf)> [http://web.archive.org/web/20241108155700/https://services-store.peugeot.co.uk/sites/peugeot/files/2024-02/Privacy%20Policy%20UK%2010-23.pdf].

———, “Brand Connect Powered by SiriusXM Privacy Policy” (22 August 2023) online: <[driveuconnect.ca](https://www.driveuconnect.ca/connected-services/privacypolicy.html)> [http://web.archive.org/web/20240519200318/https://www.driveuconnect.ca/connected-services/privacypolicy.html].

———, “Dare Forward 2030: Financials” (last visited 22 October 2024) online: <[stellantis.com](https://www.stellantis.com/en/company/dare-forward-2030/financials)> [http://web.archive.org/web/20241009105942/https://www.stellantis.com/en/company/dare-forward-2030/financials].

———, “Europe’s General Privacy Policy” (30 June 2023) online: <[jeep.co.uk](https://www.jeep.co.uk/privacy)> [http://web.archive.org/web/20241015015305/https://www.jeep.co.uk/privacy].

———, “FCA Canada Inc Privacy Policy” (15 August 2019) online: <[fcacanada.ca](https://www.fcacanada.ca/privacy/)> [http://web.archive.org/web/20240926114254/https://www.fcacanada.ca/privacy/].

———, “Mobilisights” (last visited 10 October 2024) online: <[mobilisights.com](https://www.mobilisights.com/)> [http://web.archive.org/web/20241010000049/https://www.mobilisights.com/].

———, “New ‘Mobilisights’ Business Unit Advances Stellantis’ Growing Data and Connected Services Offer” (5 January 2023) online (Press Release): <[stellantis.com](https://www.stellantis.com/en/news/press-releases/2023/january/new-mobilisights-business-unit-advances-stellantis-growing-data-and-connected-services-offer)> [http://web.archive.org/web/20240430153841/https://www.stellantis.com/en/news/press-releases/2023/january/new-mobilisights-business-unit-advances-stellantis-growing-data-and-connected-services-offer].

Secondary Material: Others

Amazon.com, Inc., *Annual Report 2023 (Form 10-K)*, Commission File No. 000-22513 (United States Securities and Exchange Commission, 2023).

Bakan, Joel & Jennifer Abbott, “The New Corporation: The Unfortunately Necessary Sequel” (2022) online (Documentary): <thenewcorporation.movie> [http://web.archive.org/web/20230701111918/https://thenewcorporation.movie/about-the-film/].

Bakan, Joel, Mark Achbar & Jennifer Abbott, “The Corporation” (2003) online (Documentary): <thecorporation.com> [http://web.archive.org/web/20230926133755/https://thecorporation.com/film/].

Department of Trade and Industry, “Explanatory Notes to Companies Act 2006” (last visited 18 August 2024) online: <[legislation.gov.uk](https://www.legislation.gov.uk)> [http://web.archive.org/web/20240422131159/https://www.legislation.gov.uk/ukpga/2006/46/notes/division/6/2].

Gaughan, Melissa, *Privacy in the Smart City: Implications of Sensor Network Design, Law, and Policy for Locational Privacy* (Master of Urban Planning, University of Washington, 2016) [unpublished].

Palantir Technologies Inc., *Annual Report 2023 (Form 10-K)*, Commission File Number: 001-39540 (United States Securities and Exchange Commission, 2023).

———, “James et al v Uber Technologies Inc” (last visited 10 October 2023) online: <[jamesvuber.com](https://www.jamesvuber.com)> [http://web.archive.org/web/20231220141023/https://www.jamesvuber.com/].

Yaron, Gil, *Awakening Sleeping Beauty: Reviving Lost Memories and Discourses to Revoke Corporate Charters* (Master of Laws, University of British Columbia, 2000) [unpublished].

Secondary Material: Websites

Amazon, “Amazon One” (last visited 19 December 2023) online: <one.amazon.com> [http://web.archive.org/web/20231219172713/https://one.amazon.com/how-it-works].

Apple, Apple, “iBeacon” (last visited 21 October 2019) online: <developer.apple.com> [http://web.archive.org/web/20231221122652/https://developer.apple.com/ibeacon/].

———, “Privacy on iPhone: The Waiting Room” (24 May 2023) online (video): <[youtube.com](https://www.youtube.com/watch?v=4-7jSoINyq4)>
[<http://web.archive.org/web/20231221121550/https://www.youtube.com/watch?v=4-7jSoINyq4>].

Brandwatch, “Retail” (last visited 8 October 2024) online: <[brandwatch.com](https://www.brandwatch.com/industries/retail/)>
[<http://web.archive.org/web/20240927141356/https://www.brandwatch.com/industries/retail/>]. Holmes, Bri, “Our Model Corporate Charter Revocation Act” (14 March 2015) online: <[freespeechforpeople.org](https://www.freespeechforpeople.org/)>
[<http://web.archive.org/web/20240622115614/https://freespeechforpeople.org/model-corporate-charter-revocation-act/>].

Business Roundtable, “Business Roundtable Redefines the Purpose of a Corporation to Promote ‘An Economy That Serves All Americans’” (19 August 2019) online: <[businessroundtable.org](https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans)>
[<http://web.archive.org/web/20231220143611/https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans>].

Business & Human Rights Resource Centre, “France’s Duty of Vigilance Law” (last visited 19 August 2024) online: <[business-humanrights.org](https://www.business-humanrights.org/en/big-issues/corporate-legal-accountability/frances-duty-of-vigilance-law)>
[<http://web.archive.org/web/20240921145006/https://www.business-humanrights.org/en/big-issues/corporate-legal-accountability/frances-duty-of-vigilance-law/>].

Caltrider, Jen, Misha Rykov & Zoë MacDonald, “*Privacy Not Included: A Buyer’s Guide for Connected Products” (6 September 2023) online: <[foundation.mozilla.org](https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy)>
[<http://web.archive.org/web/20240605142413/https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy>].

CDT, “The Project on Systematic Government Access to Data Held by the Private Sector” (2013) online: <[govaccess.cdt](https://govaccess.cdt.info/about.php)>
[<http://web.archive.org/web/20231220133800/https://govaccess.cdt.info/about.php>].

Computer History Museum, “Timeline of Computer History” (last visited 22 November 2023) online: <[computerhistory.org](https://www.computerhistory.org/timeline/1981/)>
[<http://web.archive.org/web/20231220140300/https://www.computerhistory.org/timeline/1981/>].

Corporate Europe Observatory, “Lobbying Power of Amazon, Google and Co Continues to Grow” (8 September 2023) online: <corporateeurope.org>

[<http://web.archive.org/web/20231221122155/https://corporateeurope.org/en/2023/09/lobbying-power-amazon-google-and-co-continues-grow>].

Council of Europe, “28 January: Data protection day” (last visited 12 October 2023) online: <[coe.int](http://web.archive.org/web/20231219170934/https://www.coe.int/en/web/portal/28-january-data-protection-day)>

[<http://web.archive.org/web/20231219170934/https://www.coe.int/en/web/portal/28-january-data-protection-day>].

CPDP Conferences, “CPDP 2023 Sponsors” (last visited 2 August 2023) online: <[cpdpconferences.org](http://web.archive.org/web/20231221114859/https://www.cdpconferences.org/sponsors-and-partners/platinum-sponsors)>

[<http://web.archive.org/web/20231221114859/https://www.cdpconferences.org/sponsors-and-partners/platinum-sponsors>].

EDPB, “Facebook and Instagram Decisions: ‘Important Impact on Use of Personal Data for Behavioural Advertising’” (12 January 2023) online (Press Release): <[edpb.europa.eu](http://web.archive.org/web/20231220115357/https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural_en)>
[http://web.archive.org/web/20231220115357/https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural_en].

———, “Legacy: Art 29 Working Party” (last visited 14 November 2023) online: <[edpb.europa.eu](http://web.archive.org/web/20231220132132/https://edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en)>

[http://web.archive.org/web/20231220132132/https://edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en].

Electronic Frontier Foundation, “Cell Site Location Information” (4 April 2018) online (PDF): <[eff.org](http://web.archive.org/web/20201024220927/https://www.eff.org/files/2019/03/28/csli_one-pager.pdf)>

[http://web.archive.org/web/20201024220927/https://www.eff.org/files/2019/03/28/csli_one-pager.pdf].

EUR-Lex, “Procedure 1990/0287/COD COM (1990) 314 - 2: Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data” (last visited 22 November 2023) online: <[eur-lex.europa.eu](http://web.archive.org/web/20231220134505/https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex%3A31995L0046)>
[<http://web.archive.org/web/20231220134505/https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex%3A31995L0046>].

Facebook, “What are the Meta Products?” (last visited 20 September 2023) online (Help Center): <<https://www.facebook.com/help/1561485474074139>>.

Free Speech For People, “Model Corporate Charter Revocation Act” (13 March 2015) online (PDF): <[freespeechforpeople.org](http://web.archive.org/web/20240128055455/https://freespeechforpeople.org/wp-)>
[<http://web.archive.org/web/20240128055455/https://freespeechforpeople.org/wp->

content/uploads/2015/06/Free-Speech-For-Peoples-Model-Corporate-Charter-Revocation-Act.pdf].

FIDIS, “Mobility and Identity: Future of IDentity in the Information Society” (2006) online: <[fidis.net](http://www.fidis.net)>
[<http://web.archive.org/web/20231221121811/http://www.fidis.net/resources/fidis-deliverables/mobility-and-identity/>].

Global Network Initiative, “Company Assessments” (last visited 10 January 2023) online (Global Network Initiative): <globalnetworkinitiative.org>
[<http://web.archive.org/web/20231220144913/https://globalnetworkinitiative.org/company-assessments/>].

———, “Our Members, Fellows, & Observers” (last visited 2 December 2023) online: <<https://globalnetworkinitiative.org/>>.

———, “The GNI Principles” (last visited 2 December 2022) online: <globalnetworkinitiative.org>
[<http://web.archive.org/web/20231220132905/https://globalnetworkinitiative.org/gni-principles/>].

———, “Uber Joins GNI as a Company Observer” (27 June 2021) online: <globalnetworkinitiative.org>
[<https://web.archive.org/web/20240116105143/http://web.archive.org/screenshot/https://globalnetworkinitiative.org/uber-joins-gni-as-a-company-observer/>].

Google,Google, “Google Privacy & Security” (last visited 1 August 2023) online (video): <[youtube.com](https://www.youtube.com)>
[http://web.archive.org/web/20231221124225/https://www.youtube.com/playlist?list=PL590L5WQmH8cDdey4_8Fy9qJnkHWFxcDg].

———, “Voice Match and Media on Google Nest and Google Home speakers and displays” (last visited 31 August 2020) online (Help Center): <support.google.com>
[<http://web.archive.org/web/20231221115839/https://support.google.com/googlenest/answer/7342711>].

Hickins, Michael, “How Data Analytics Informs the Fashion Industry” (24 February 2023) online: <[oracle.com](https://www.oracle.com)>
[<http://web.archive.org/web/20240817234418/https://www.oracle.com/retail/fashion/fashion-analytics/>].

History, “The Invention of the Internet” (28 October 2019) online: <[history.com](https://www.history.com/topics/inventions/invention-of-the-internet)>
[<http://web.archive.org/web/20231220140502/https://www.history.com/topics/inventions/invention-of-the-internet>].

IAPP, “IAPP Europe Data Protection Congress 2023” (last visited 2 August 2023) online: <[iapp.org](https://iapp.org/conference/iapp-europe-data-protection-congress/)>
[<http://web.archive.org/web/20230810214727/https://iapp.org/conference/iapp-europe-data-protection-congress/>].

Irish DPC, “Data Protection Impact Assessments” (last visited 24 November 2023) online (Data Protection Commission): <[dataprotection.ie](https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments)>
[<http://web.archive.org/web/20231220115011/https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments>].

Leiner, Barry M et al, “Brief History of the Internet: Internet Timeline” (last visited 19 July 2016) online: <[internetsociety.org](https://www.internetsociety.org/internet/history-internet/brief-history-internet/)>
[<http://web.archive.org/web/20231220135850/https://www.internetsociety.org/internet/history-internet/brief-history-internet/>].

Lyytinen, Kalle, “Understanding the Real Innovation Behind the iPhone” (27 June 2017) online: <[theconversation.com](https://theconversation.com/understanding-the-real-innovation-behind-the-iphone-79556)>
[<http://web.archive.org/web/20231221120051/https://theconversation.com/understanding-the-real-innovation-behind-the-iphone-79556>].

McKinsey & Company, “What is 5G technology?” (7 October 2022) online: <[mckinsey.com](https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-5g)>
[<http://web.archive.org/web/20231112053416/https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-5g>].

MightySignal, “Beacon SDK Category Apps and Analytics” (last visited 8 February 2021) online: <[mightysignal.com](https://mightysignal.com/sdk-category/46/beacon)>
[<http://web.archive.org/web/20230130105723/https://mightysignal.com/sdk-category/46/beacon>].

———, “Location SDK Category Apps and Analytics” (last visited 8 February 2021) online: <[mightysignal.com](https://mightysignal.com/sdk-category/12/location)>
[<http://web.archive.org/web/20230130123541/https://mightysignal.com/sdk-category/12/location>].

Mozilla Location Service, “Statistics” (last visited 21 October 2020) online: <[location.services.mozilla](https://location.services.mozilla.com/stats)>
[<http://web.archive.org/web/20231221121039/https://location.services.mozilla.com/stats>].

Noyb, “Noyb Files GDPR Complaint Against Meta over ‘Pay or Okay’” (28 November 2023) online (News): <noyb.eu>
[<http://web.archive.org/web/20231220140812/https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay>].

Office of the New York State Attorney General, “AG Schneiderman Announces Settlement with Uber to Enhance Rider Privacy” (6 January 2016) online (News release): <ag.ny.gov>
[<http://web.archive.org/web/20231221150249/https://ag.ny.gov/press-release/2016/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy>].

OHCHR, “B-Tech Project” (last visited 22 December 2023) online: <<https://www.ohchr.org/en/business-and-human-rights/b-tech-project>>.

———, “Using Social Media to Promote Human Rights” (10 August 2011) online: <[ohchr.org](https://www.ohchr.org)>
[<http://web.archive.org/web/20240127170700/https://www.ohchr.org/en/stories/2011/08/using-social-media-promote-human-rights>].

OpenDataCity, “Data Retention in Switzerland: The Monitored Life of National Councilor Balthasar Glättli” (last visited 15 August 2018) online: <digitale-gesellschaft.ch>
[http://web.archive.org/web/20231220144611/https://www.digitale-gesellschaft.ch/vds-suisse/index_en.html].

Oracle, “Oracle Retail Data Store Cloud Service” (2024) online (PDF): <[oracle.com](https://www.oracle.com)>
[<http://web.archive.org/web/20230314055028/https://www.oracle.com/a/ocom/docs/industries/retail/retail-data-store-ds.pdf>].

Pialat, Romain, “GeoTrouveTous: Projet de Réidentification par Géolocalisation” (14 July 2023) online: <linc.cnil.fr>
[<http://web.archive.org/web/20231221124813/https://linc.cnil.fr/geotrouvetous-projet-de-reidentification-par-geolocalisation>].

Reform Government Surveillance, “Purpose and Members” (last visited 24 August 2023) online: <reformgovernmentsurveillance.com>
[<http://web.archive.org/web/20231220133513/https://www.reformgovernmentsurveillance.com/about>].

RightsCon, “Welcome to all RightsCon Sponsors” (last visited 2 August 2023) online: <rightscon.org>
[<http://web.archive.org/web/20231220142454/https://www.rightscon.org/sponsors/>].

Rodriguez, Katitza, Cindy Cohn & Karen Gullo, “European Court on Human Rights Bought Spy Agencies’ Spin on Mass Surveillance” (26 May 2021) online: <[eff.org](http://web.archive.org/web/20231221151759/https://www.eff.org/deeplinks/2021/05/european-court-human-rights-bought-spy-agencies-spin-mass-surveillance)> [http://web.archive.org/web/20231221151759/https://www.eff.org/deeplinks/2021/05/european-court-human-rights-bought-spy-agencies-spin-mass-surveillance].

Signal, “Signal Messenger: Speak Freely” (last visited 16 November 2023) online: <<https://signal.org/>>.

Sissons, Miranda, “Our Commitment to Human Rights” (16 March 2021) online (Newsroom): <[about.fb.com/news](http://web.archive.org/web/20221220121005/https://about.fb.com/news/2021/03/our-commitment-to-human-rights/)> [http://web.archive.org/web/20221220121005/https://about.fb.com/news/2021/03/our-commitment-to-human-rights/].

Skyhook Wireless Inc, “Locate and Position Devices Worldwide” (last visited 23 October 2020) online: <[skyhook.com](http://web.archive.org/web/20210612141916/https://www.skyhook.com/precision-location)> [http://web.archive.org/web/20210612141916/https://www.skyhook.com/precision-location].

Sullivan, Mark, “A Brief History of GPS” (9 August 2012) online: <[pcworld.com](http://web.archive.org/web/20231219171822/https://www.pcworld.com/article/461346/a-brief-history-of-gps.html)> [http://web.archive.org/web/20231219171822/https://www.pcworld.com/article/461346/a-brief-history-of-gps.html].

Supreme Court of California, “Summary of Cases Accepted and Related Actions During Week of June 20, 2022” (30 June 2023) online (News Release): <[supreme.courts.ca.gov](http://web.archive.org/web/20231221120848/https://supreme.courts.ca.gov/sites/default/files/supremecourt/default/documents/ws062623.pdf)> [http://web.archive.org/web/20231221120848/https://supreme.courts.ca.gov/sites/default/files/supremecourt/default/documents/ws062623.pdf].

Teare, Gené, “What Are The Odds Of Success For A US Seed Funded Startup?” (1 December 2021) online: <[news.crunchbase.com](http://web.archive.org/web/20231221115535/https://news.crunchbase.com/liquidity/seed-funding-series-a-success/)> [http://web.archive.org/web/20231221115535/https://news.crunchbase.com/liquidity/seed-funding-series-a-success/].

The Bridge, “Legal Theory: Law and Society” (last visited 24 February 2017) online: <[cyber.harvard.edu](http://web.archive.org/web/20231221122349/https://cyber.harvard.edu/bridge/LawSociety/essay1.htm)> [http://web.archive.org/web/20231221122349/https://cyber.harvard.edu/bridge/LawSociety/essay1.htm].

UN, “History of the Declaration” (last visited 29 September 2021) online: <[un.org](http://web.archive.org/web/20231220111458/https://www.un.org/en/about-us/udhr/history-of-the-declaration)> [http://web.archive.org/web/20231220111458/https://www.un.org/en/about-us/udhr/history-of-the-declaration].

———, “The Foundation of International Human Rights Law” (last visited 29 September 2021) online: [un.org](https://www.un.org/en/about-us/udhr/foundation-of-international-human-rights-law) [\[http://web.archive.org/web/20231220114207/https://www.un.org/en/about-us/udhr/foundation-of-international-human-rights-law\]](http://web.archive.org/web/20231220114207/https://www.un.org/en/about-us/udhr/foundation-of-international-human-rights-law).

———, “Drafting of the Universal Declaration of Human Rights: Drafting Committee Members” (last visited 22 January 2024) online: [research.un.org](https://research.un.org/en/undhr/draftingcommittee) [\[http://web.archive.org/web/20240120024735/https://research.un.org/en/undhr/draftingcommittee\]](http://web.archive.org/web/20240120024735/https://research.un.org/en/undhr/draftingcommittee).

UN Special Rapporteur on Freedom of Opinion and Expression et al, “Joint Declaration on Freedom of Expression and Responses to Conflict Situations” (4 May 2015) online: [oas.org](https://www.oas.org/en/iachr/expression/showarticle.asp?artID=987&lID=1) [\[https://web.archive.org/web/20231220114722/https://www.oas.org/en/iachr/expression/showarticle.asp?artID=987&lID=1\]](https://web.archive.org/web/20231220114722/https://www.oas.org/en/iachr/expression/showarticle.asp?artID=987&lID=1).

UNCTAD, “Data Protection and Privacy Legislation Worldwide” (last visited 11 October 2021) online: [unctad.org](https://unctad.org/page/data-protection-and-privacy-legislation-worldwide) [\[http://web.archive.org/web/20231220111334/https://unctad.org/page/data-protection-and-privacy-legislation-worldwide\]](http://web.archive.org/web/20231220111334/https://unctad.org/page/data-protection-and-privacy-legislation-worldwide).

US Securities and Exchange Commission, “SEC v Facebook, Inc Case No 3:19-cv-04241-JD (ND Cal)” (last visited 28 April 2023) online: [sec.gov](https://www.sec.gov/enforcement/information-for-harmed-investors/facebook) [\[https://web.archive.org/web/20231218145706/https://www.sec.gov/enforcement/information-for-harmed-investors/facebook\]](https://web.archive.org/web/20231218145706/https://www.sec.gov/enforcement/information-for-harmed-investors/facebook).

———, “Annual Report” (last visited 22 May 2024) online: [investor.gov](https://www.investor.gov/introduction-investing/investing-basics/glossary/annual-report) [\[http://web.archive.org/web/20240425153855/https://www.investor.gov/introduction-investing/investing-basics/glossary/annual-report\]](http://web.archive.org/web/20240425153855/https://www.investor.gov/introduction-investing/investing-basics/glossary/annual-report).

Zefo, Ruby, “Living Up to Our Privacy Principles: Introducing Uber’s Privacy Center” (18 January 2022) online (Newsroom): [uber.com/newsroom](https://www.uber.com/newsroom/privacycenter) [\[http://web.archive.org/web/20230306225003/https://www.uber.com/newsroom/privacycenter\]](http://web.archive.org/web/20230306225003/https://www.uber.com/newsroom/privacycenter).

“An Excerpted Document From Britain’s Government Communications Headquarters From May 2010” (May 2010) online (PDF): <http://web.archive.org/web/20231219173411/https://www.documentcloud.org/documents/1009661-gchq.html>.

“An Excerpted Document From the NSA From May 2010” (May 2010) online (PDF):
<<http://web.archive.org/web/20231219172950/https://www.documentcloud.org/documents/1009660-nsa.html>>.