PRIVATE LAW & PUBLIC SPACE: THE CANADIAN PRIVACY TORTS IN AN ERA OF PERSONAL REMOTE-SURVEILLANCE TECHNOLOGY

KRISTEN THOMASEN

Thesis submitted to the University of Ottawa in partial fulfillment of the requirements for a doctoral degree in Law

Faculty of Law

Common Law Section

University of Ottawa

Dedication

For Pake, who would have loved the chance to do this.

For Ian, who helped me realize I could do this.

For Lyne and Sterling, and all the possibilities.

Acknowledgements

I could not have written this thesis and completed this degree without the enormous and generous support of many people. As it turned out, this thesis was written during some personally and collectively very challenging times. It was also written during some peaceful morning hours. And with the vocal encouragement of two toddlers, born during the journey of this degree. It was finalized in the oncology wing of the BC Children's Hospital. This document marks a significant era of my life, and I'm forever grateful for the opportunity to have engaged with this process.

John, Lyne, and Sterling, (& Alabama) thank you forever for the unconditional support and the small and big sacrifices you made so that I could do this. My perseverance with this writing was only possible because of your encouragement, excitement, and promises of cake at the end of it all. Thank you to my parents and parents-in-law for offering so much support including with, among many other things, extensive child care especially during the pandemic so I could do some focused work. I'm grateful to my whole family, and especially my grandparents, for reminding me to keep at it and not take this opportunity for granted. I relatedly express my thanks for the financial support that I received for this dissertation from the Social Sciences and Humanities Research Council and the University of Ottawa. Thank you also the whole graduate department at the Faculty of Law for helping me through some challenging shifts throughout the course of this degree.

To my friends Alex Mogyoros, Shanthi Senthe, Sinzi Gutiu, and Katie Szilagyi thank you for being amazing writing buddies, for our many chats, co-writing sessions, reading each other's work, and overall support. So many people have talked me through parts or all of this thesis, and I am deeply grateful for their mentorship, insight, and support, including Sujith Xavier, Anne Uteck, Jon Khan, Suzie Dunn, Ryan Calo, Bita Amani, Amar Khoday, Daydra, and my incredibly supportive Windsor Law and Allard Law colleagues. I am also grateful to so many others who supported me along this journey in ways large and small, even if I have not named you here, you are in my heart and have my gratitude.

And to my amazing committee, thank you so much to Jennifer Chandler and Teresa Scassa, for all of your thoughtful comments and insights on this thesis which substantially improved my thinking and writing. But even bigger thanks to you for your immense support, both academic and personal, throughout this degree. I needed to ask for a lot of assistance and understanding in order to complete this dissertation, through which I sometimes convinced myself I was lesser-than. But your vocal encouragement and understanding of the circumstances helped me quiet that self-doubt and get through. You stepped into the role of being my co-supervisors without hesitation and it has been such an incredible experience and privilege to benefit from your mentorship and advice. I am also deeply grateful to my advisors, Jane Bailey and Carlisle Adams, for joining my committee and for your insightful feedback and comments, which all strengthened the thesis. I am also grateful to my external and internal examiners, Woodrow Hartzog and Amy Salyzyn, for participating in a wonderful dialogue about the final product of this degree, and for such thoughtful comments and feedback on the thesis.

I have been fortunate in many ways throughout this thesis, including by having *three* incredible supervisors and mentors. My final and effusive thanks goes to Ian Kerr. Ian offered an unconditional voice of IanKerragement that supported me in applying for this PhD. Ian supported me financially with RA-ships and co-teaching opportunities. And he supported me professionally with extensive advice, reference letters, and when I interviewed for my first job, he set up a mock interview with some of the smartest and kindest people at uOttawa to help me prepare. Ian treated me as an equal, and as a friend. I know we'd be celebrating this final draft over lunch and talking about what's next. Thank you, Ian.

Abstract

As increasingly sophisticated personal-use technologies like drones and home surveillance systems become more common, so too will interpersonal privacy conflicts. Given the nature of these new personal-use technologies, privacy conflicts will also continue to increasingly occur in public spaces. Tort law is one area of the Canadian legal system that can address interpersonal conflict and rights-infringements between people with no other legal relationship. However, building on a historical association between privacy and private property, the common and statutory law privacy torts in Canada fail to respond to such conflicts, I argue inappropriately. Privacy is an important dimension of public space, and the social interactions and relationships that arise in public spaces. Failing to recognize public space privacy in tort law leads to an overly narrow understanding of privacy, and can be considered contrary to binding precedent that says that the common law should evolve in line with (or at a minimum, not contrary to) *Charter* values. The *Charter* values of privacy, substantive equality, and expressive freedom support various reforms to the judicial understanding of the privacy torts in Canada.

Privacy, also understood as "private affairs" or "private facts" in tort, should not be predicated on property, and in fact, can sometimes take on *greater* value in public spaces. Privacy interests should be assessed through a normative lens, with a view to the long-term implications of a precedent for both privacy and substantive equality. Courts should assess privacy through a subjective-objective lens that allows for consideration of the lived experiences and expertise of the parties, their relative power, and their relationships. Adopting these principles into the statutory and common law torts would permit tort law to serve as a legal mechanism for addressing interpersonal, technology-mediated privacy conflicts arising in public spaces. This will be a socially valuable development as such conflicts become increasingly common and potentially litigated.

Table of Contents

"Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life…" (Warren and Brandeis, 1890)

"The privacy tort was the brainchild of nineteenth-century men of privilege, and it shows." (Allen and Mack, 1991)

Chapter 1 - Introduction

Technology and privacy have a long history of tension in North American society and legal scholarship. Privacy law is commonly perceived as falling behind advances in technology, and technologies of various types are often cited as the next threat to individual privacy. In this vein, this thesis examines new technologies that threaten privacy, where the law has yet to "catch up." But, the analysis in this thesis also frames the increasing popularity of personal-use surveillance technologies as an *opportunity* to push courts to rethink the judicial approach to personal privacy rights within the Canadian privacy torts, and perhaps tort law more broadly.

In this thesis, I argue that the growing prevalence of increasingly sophisticated personal-use surveillance technologies, which streamline interpersonal surveillance and interpersonal policing, adds urgency to the need for courts to recognize that personal privacy rights extend into public and shared spaces. In particular, I argue that courts must recognize *public space privacy harm* within the Canadian privacy torts, in order to bring the law in line with Canadian *Charter* values of privacy, substantive equality, and expressive freedom. This thesis blends private law with aspects of public law (specifically, some of the values embedded in the Canadian *Charter of Rights and Freedoms*) to argue for a more robust understanding of private-law privacy rights. Notably, the analysis in this thesis crosses the division between what is 'public' and 'private' in a range of ways – it mingles public with private law; privacy with public space; and examines conduct that is typically associated with public actors (surveillance, policing) but increasingly carried out by private actors. It is hoped that such an approach to considering the evolution of the private law in response to changing socio-technical

contexts could extend to other individual tort actions as well. Additionally, this thesis highlights some of the significant limits when considering individual rights-based approaches to address what are actually broader structural and architectural challenges.

Personal-use and remotely operated technologies, like drones and sophisticated home surveillance systems, are apt to cause interpersonal privacy conflicts. Drones, for instance, have been the source of a number of high-profile privacy conflicts in recent years. When a drone flew over a beach, discomforting sunbathers to the point of taking extreme measures, a woman confronted and assaulted the man operating the drone and was later criminally charged and convicted for the conflict. The drone operator faced no legal consequences.[1] When a similar drone flew over a residential backyard, discomforting the father of the children playing in the yard, the father used a rifle to shoot the drone down. He was later acquitted of any charges as he was protecting his property and privacy.[2] The drone operator unsuccessfully sued for compensation for his destroyed drone.[3]

In neither of these scenarios was it reportedly evident that the drone was actually collecting information; but in each, the presence of the drone and possibility of video collection raised concerns about privacy and unwanted entry into personal space. An important distinction in the legal treatment for both the subjects and objects of the drone encounters here was spatial – the first encounter occurred in a public space, and the second engaged private property. The different

---

[1] Coverage of the encounter went viral online. See for example, Yazhou Sun, "Connecticut Woman Arrested for Assaulting Teenager Flying Drone" (June 10, 2014) ABC News, online: <https://abcnews.go.com/US/conn-woman-arrested-assaulting-teenager-flying-drone/story?id=24076891> (accessed July 14, 2021).

[2] This encounter also went viral online. For an overview of the interaction and criminal case see e.g.: Cyrus Faviar, ""Drone Slayer" Cleared of Charges: "I wish this had never happened"" (October 27, 2015) Ars Technica, online: <https://arstechnica.com/tech-policy/2015/10/drone-slayer-cleared-of-charges-i-wish-this-had-never-happened/> (accessed July 14, 2021). The criminal court decision was never published.

[3] *Boggs v Meredith*, US District Court Western District of Kentucky at Louisville, Civil Action No. 3:16-CV-00006-TBR; Cyrus Faviar, "Judge Rules in Favor of "Drone Slayer," Dismisses Lawsuit Filed by Pilot" (March 24, 2017) Ars Technica, online: <https://arstechnica.com/tech-policy/2017/03/judge-rules-in-favor-of-drone-slayer-dismisses-lawsuit-filed-by-pilot/> (accessed July 14, 2021).

outcomes also evoke gendered and patriarchal dynamics of women permissibly surveilled on a beach, and children permissibly protected from the same experience by fathers through violence.[4] These dynamics are also historically connected to the spatial/property considerations alive in the different tort law treatment of a privacy conflict in public *vs.* private space.

In this thesis, I suggest that these sorts of interpersonal technology-mediated privacy conflicts are likely to become more common, particularly in public spaces where the legal treatment of such conflicts may be complicated or poorly developed. More specifically, I suggest that these technologies are apt to enable interpersonal surveillance and policing in ways not before possible or, at least, not possible with such ease. I examine whether one area of law that addresses interpersonal conflict – tort law, and the privacy torts specifically – can serve as a legal mechanism to address potential privacy harms arising in such technology-mediated encounters. Courts have, generally, interpreted the privacy torts as not applying to encounters occurring in public spaces, like the beach example cited above. The historical roots of the privacy torts have maintained a connection to private property and secrecy that limit their application with respect to privacy conflicts occurring in public spaces. Accordingly, the shift toward increased personal (i.e., individual, and not state or commercially-based) control and power over surveillance and information-collection that is currently taking place through the growing popularity of personal-use, remotely operated technologies is legally and socially significant. Private individuals are largely unregulated in terms of how, and how much, information they collect about others in public spaces, yet the capacity for private individuals to collect extensive information from public space is growing quickly.

[4] See e.g. Margot Kaminski, "Enough with the "Sunbathing Teenager" Gambit" (May 17, 2016) Slate, online: <https://slate.com/technology/2016/05/drone-privacy-is-about-much-more-than-sunbathing-teenage-daughters.html>; Kristen Thomasen, "Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation" 16(2) Canadian Journal of Law and Technology 307 [Thomasen, "Beyond Airspace Safety"].

I examine whether the trajectory of the torts could accordingly shift to account for public space privacy harms, and argue that such a shift would be justified through the application of a *Charter* values lens to the interpretation of these torts. I argue that application of such a lens is not only possible, but necessary in the context of the privacy tort jurisprudence; and that it could ground reforms that would render tort law, and the privacy torts specifically, a more viable mechanism for addressing some of the privacy conflicts likely to emerge in the context of increasingly automated personal-use technologies.

There are also some important limits to the scope of tort law in addressing the range of conduct considered here, particularly where shifts in interpersonal surveillance and policing reflect structural or architectural trends that are more difficult to address through a personal-rights framework like tort law. Perhaps tort reform could ground the beginnings of a broader socio-legal response to the ways in which surveillance norms may shift in the near future as personal-use surveillance technology becomes more prevalent.

Why Personal-Use Remotely Operated Technologies?

The examples noted above both involved drone technology, a technology that works at a distance from its operator, and in both examples the technology was used for personal purposes. Within this thesis, I refer to 'personal-use' technologies as any technologies that can be used by individuals for personal (non-governmental, non-commercial) purposes. This can include a range of activities such as recreation/hobby, sport, creative expression, political expression, stalking, voyeurism, spying/control, personal/home security, *etc* - any personal function that does not engage commercial- and/or government-entity regulation.[5] I am interested in personal-use technologies and

[5] Though intrafamilial surveillance certainly comes within the scope of the inquiry in this thesis, I am focused here on the privacy-related issues in such a conflict and do not examine the additional legal considerations that might arise in a

the interactions between private individuals in part because much of privacy law, and privacy scholarship, focuses on individual privacy vis-à-vis the state, or vis-à-vis commercial entities; however interpersonal intrusions can cause significant harm, yet have received less attention. I hope to contribute to the privacy scholarship on interpersonal privacy dynamics through this thesis.

'Remotely-operated' refers to technology that can operate at a distance from the person controlling it, and/or that can operate automatically or autonomously such that a person does not need to constantly oversee its use. Such technology can be deployed and then left to carry out a task, including the collection of video, images, or other information. When a technology operates automatically without ongoing individual oversight, it becomes less time and labour intensive to use, which opens up the possibility for more widespread use, and/or use over longer periods of time, including perpetually. Through a privacy lens, for instance, this opens up the possibility of quantitatively more, perhaps even pervasive, information collection.

While one could certainly carry out a legal analysis more generally of the application of the privacy torts in public spaces, without reference to technological examples, I am particularly curious about whether the privacy torts can address the added nuances that arise when remotely-operated technology mediates the interaction. For instance, the use of remotely-operated technologies can complicate both the experience of privacy vis-à-vis another person by obscuring who that person is and why they are engaging the technology; and can complicate the legal analysis of whether a subject of privacy intrusion has a legal claim against another, as discussed in greater length in Chapters 2 and 3.[6] Accordingly, while the analysis in this thesis does seek to contribute more broadly to legal conversations about privacy in public spaces, it also specifically seeks to respond to what I suggest

family dispute involving, for instance, divorce or child custody. These are certainly not irrelevant, but difficult to appropriately integrate into this analysis in the abstract, and deserve further specific consideration.

[6] This may also complicate a tort analysis by begging the question of whether collection of information was done intentionally, or whether the automated nature of the technology mitigates intention, as discussed more in Chapter 3.

will be an increasingly challenging area of law and personal interaction in the coming years – interpersonal technology-mediated public space privacy conflicts.

In this thesis I focus on two types of increasingly popular remotely-operated technologies – drone systems, and what I will refer to as sophisticated home surveillance systems. Drones are the most prevalent robotic/semi-autonomous system in use in public spaces right now in Canada.[7] Transport Canada, the regulator of drones in Canada, has registered over 53,000 drones in Canada and more than 51,000 pilot certificates as of October, 2020.[8] Inferring from U.S. statistics, Transport Canada has estimated that a significant portion of drone use will be by private individuals for non-commercial purposes.[9] The popularity and prevalence of drone technology is expected to continue to grow.[10] A substantial academic literature, and popular debates, emphasize the privacy concerns associated with increasing drone use. Meanwhile, drone-specific regulations (which are outlined in Chapter 2) do not specifically address privacy or provide a mechanism for resolving privacy disputes. Accordingly, I explore the possibility for tort law to ground some resolution of privacy disputes involving drone technology.

---

[7] Various other technical terms can be used to refer to an aerial vehicle, including Unmanned Aircraft (UA), Remotely Operated Aircraft (ROA), Remotely Piloted Vehicle or Aircraft (RPV or RPA), and Unmanned Aerial Vehicle (UAV). Broader terms such as Unmanned Aerial/Aircraft System (UAS) (common in North America) and Remotely Piloted Aircraft Systems (RPAS) (used in the European Union and international aviation organizations) refer to both the physical device as well as the communication systems that permit the pilot to command the drone. See e.g.: Roger Clarke, "Understanding the Drone Epidemic" (2014) 30 Computer Law and Security Report 230 at 234. All of these terms generally refer to the same concept of an aerial device with no on-board human pilot. For both readability and a broad and inclusive denotation, I use the term "drone" to refer generally to the variety of remotely-piloted aerial vehicle systems that exist.

[8] Transport Canada, "Transport Canada's Drone Strategy to 2025" (2021), online: <https://tc.canada.ca/sites/default/files/2021-03/TC223-Drone-Strategy-ENG-ACC.pdf> at 9 [Transport Canada, "Drone Strategy"].

[9] Canada Gazette, Part I, Volume 151, Number 28: Regulations Amending the Canadian Aviation Regulations (Unmanned Aircraft Systems), Regulatory Impact Assessment, online: <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-07-15/html/reg2-eng.php>.

[10] See e.g. Scott Thompson and Alana Saulnier, "The "Rise" of Unmanned Aerial Vehicles (UAVs) in Canada: An Analysis of Special Flight Operation Certificates (SFOCs) from 2007 to 2012" (2015) 41 Canadian Public Policy 207 (offering an analysis of the increasing prevalence of commercial drones in Canada. The analysis includes only commercial drones because at time of publication there had been no mechanism through which Transport Canada could monitor the prevalence of recreational drones, as this use of drone technology had been largely unregulated). See also, Transport Canada, "Drone Strategy", *supra* note 8.

Drones raise a range of concerns that can complicate and nuance the privacy analysis, including that they operate predominantly (by regulation) in public airspace and often over public ground spaces (engaging multiple dimensions of public space); that the operator can be located at a distance leading to anonymity, or a disempowered sense for those encountering the drone who do not know who is flying it or for what purpose[11]; and that they can be operated for various expressive purposes, that may need to be balanced with the privacy interests of others when courts are asked to mediate drone-related privacy conflicts. I expand upon these considerations throughout the thesis.

Meanwhile, home surveillance devices have existed for a long time. They have more recently become increasingly sophisticated and integrated both within the home architecture and with social networks beyond the home. Amazon's Ring is a striking example of such integration, though certainly not the only example.[12] The Ring system involves an extensive integrated network between various technologies, individuals, and institutions, including law enforcement agencies.[13] Ring is designed and patented specifically as a personal surveillance device,[14] in contrast with drone technology which can have social uses unrelated to surveillance. Amazon Ring is in widespread use in the US, and anecdotally appears to be growing in popularity in Canada.[15] It encourages seamless

---

[11] See e.g. Ciara Bracken-Roche, "Domestic Drones: The Politics of Verticality and the Surveillance Industrial Complex" (2016) 71 Geographica Helvetica 167 [Bracken-Roche, "Politics of Verticality"].

[12] A number of companies previously known for offering different home-related services have recently introduced their own iterations of home surveillance systems to the market. For instance, Google markets a smart home system that includes security and surveillance cameras, called Nest; other companies in Canada like Lorex offer a range of devices as well, more specifically tailored to home surveillance and security.

[13] The integration between law enforcement and companies raises important transparency concerns, which are now deepened by the added presence of a private individual carrying out the surveillance perhaps on behalf (explicitly or by implication) of the company and/or law enforcement agency. See Teresa Scassa, "Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges", (2017) 14(2) SCRIPTed 239 <https://script-ed.org/?p=3396> [Scassa, "Law Enforcement"].

[14] WIPO: WO2019133764A1, "Locating a person of interest using shared video footage from audio/video recording and communication devices" inventors: James Siminoff, Mark Troughton, Aviv Gilboa, Darell SOMERLATT, Alex Jacobson (2018), Google Patents, online, <https://patents.google.com/patent/WO2019133764A1/en>.

[15] Business assessments suggest Ring is the most popular of the home surveillance systems. See e.g., Business Wire, "Amazon's Ring Leads Google's Nest As 16% Of US Homes Adopt Video Doorbells: Strategy Analytics" (February 13, 2020), online: <https://www.businesswire.com/news/home/20200213005824/en/Amazon%E2%80%99s-Ring-Leads-Google%E2%80%99s-Nest-16-Homes>; over 400 police services in the US have also entered into partnerships with Amazon Ring – discussed at greater length below. See e.g., Drew Harwell, "Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns" (August 28, 2019) Washington Post, online:

sharing of information and video footage between neighbours, as well as with law enforcement agencies, engaging not only a privacy interest in information collection, but also in how that information is subsequently used, which may raise bodily integrity and autonomy concerns in relation to the citizen and state policing of various spaces that can be triggered through the Ring system. The system also promises to automate its recognition of 'suspicious' individuals in a neighbourhood, such that identification and notification could occur without a specific input from the owner of the device.[16] Ring, and other similar systems, sit on the boundary of the public/private divide (designed to sit on the home looking at the public and protecting the home from that public). Examining the Ring system in addition to drone technology facilitates a tort law analysis of the impact of technology-mediated information collection, use, and physical intrusion, on public space through various angles (literally – from above and from within architecture; and analytically – engaging some different aspects of interpersonal privacy). The growing popularity of these and similar technologies also points to the urgency for a consideration of how law, in particular the privacy torts, might deal with the interpersonal conflicts that will increasingly arise due to the use of personal, remotely-operated technologies.

Why Interpersonal Surveillance and Policing?

The interpersonal privacy conflicts I am especially focused on in this thesis are those that arise where technology has been used to surveil (e.g., intentionally monitor or gather information about another) or police (e.g., control, or enforce norms or regulation upon someone else) in public space. I am not specifically focusing, for instance, on cases where an individual might incidentally

<https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true>.

[16] See e.g., Sam Biddle, "Amazon's Ring Planned Neighbourhood "Watch Lists" Built on Facial Recognition" (November 26, 2019) The Intercept, online: <https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/>.

(not intentionally) capture an image of another person in the background of a photograph taken from a drone. While this latter scenario might also engage the considerations in this thesis depending on the circumstances, I am particularly interested in surveillance and policing of others because these actions raise an element of *intention*. In other words, the person using the technology at issue is doing so with the intent of collecting, using, or distributing information about another person (either someone who is pre-identified, or generally any people who enter within the scope of the technology's frame), or invading their personal space. I will refer to 'interpersonal privacy conflicts' as instances of interpersonal surveillance or policing in which the person under scrutiny (the plaintiff in a privacy tort action) resists or seeks vindication of the unwanted privacy impact of the defendant's technology-mediated conduct.

Interpersonal privacy conflicts are of course not confined to public spaces. Within Canadian tort law there are a number of cases that arose from a dispute between neighbours in which surveillance of opposing properties either initiated or became a symptom of the dispute. One such case specifically involves Amazon Ring, which I discuss at length below in Chapter 3.[17] Such conflicts contribute to and may shape the court's understanding of the private tort law as it relates to interpersonal surveillance in public space, and therefore are also considered in the analysis throughout this thesis. Though, because of the availability of other property-based legal protections in many of these cases (through which disputes are often resolved), these are not the primary focus of the thesis.

[17] *Zeliony v Dunn*, 2021 MBQB 136 (CanLII).

Why Tort Law, and Why the Privacy Torts?

Broadly speaking, Canadian tort law recognizes legal accountability for civil wrongs. Or, said somewhat differently, tort law remedies harms to a plaintiff caused by a defendant, with the goal of making the plaintiff 'whole again' to the extent this can be done through, typically, monetary compensation.[18] While tort claimants can seek other remedies, including injunctions to prevent harmful conduct from taking place or continuing,[19] tort actions are primarily focused on remedying harms to plaintiffs' recognized private rights and interests through a financial award from the defendant.

This thesis focuses on tort law's recognition and vindication of privacy interests for several reasons. Because I am interested in interpersonal privacy conflicts in this thesis, tort law, which deals with rights and interests between parties operating in a private (i.e., not state, or public) capacity, is a relevant site of inquiry. I am examining the rights and responsibilities between two or more people acting in their private capacities, and tort law specifically addresses rights and responsibilities in this context. Depending on the circumstances of the relationship, other areas of law such as employment, criminal, or family law might also be engaged. However, when addressing specifically the interpersonal privacy conflict under analysis in this thesis, tort law is the most consistently and directly relevant area of law in the Canadian legal system.

Tort law can also serve normative and educational functions, in the sense that a court's recognition of rights and responsibilities in different interpersonal encounters can be educational to others – who might now recognize their legal responsibilities to one another – and can be norm setting. When courts recognize a legal right, this can send a message that certain types of conduct are considered wrongful and could lead to legal or social consequences. In the context of what can

[18] See e.g., Chris Hunt, "From Right to Wrong: Grounding a "Right" to Privacy in the "Wrongs" of Tort" (2015) 52(3) Alberta Law Review 635 at 637 [Hunt, "Right to Wrong"].
[19] Which, of course, are only helpful if they are enforced.

sometimes be relatively minor violations in the sense that they may not garner a large damage award (not necessarily that they are unimportant to a plaintiff), the normative function of tort law might be more significant to individuals (knowing they have legal rights) than monetary compensation.

Notably though, the predominant academic and jurisprudential theory of tort law in Canada is corrective justice – i.e., that the function of tort is to primarily serve corrective justice rather than an educative or norm setting function. Corrective justice generally refers to the idea that the function of tort law is to correct, or reverse, an imbalance or injustice between two or more parties.[20] A corrective justice approach in tort law is concerned specifically with attaining justice between a wrongdoer and the victim of their conduct through the reversal of the wrong occurring between parties, usually through payment of monetary compensation. A key component of corrective justice is wrongfulness on the part of the defendant,[21] the defendant must do something more than simply cause the harm through their conduct (which, if actionable, would amount to strict liability). Formalistic views of corrective justice are narrowly concerned with the specific interaction between parties, such that considerations about who is in a better position to absorb the costs of harm (a distributional justice goal); what kind of message a court decision might send to the public (an educational function of tort law); or whether others should be deterred from engaging in similar behaviour (a deterrent function of tort law) may be seen as outside the scope of what tort law should aim to achieve or even consider.[22]

---

[20] According to Professor Ernst Weinrib, one of the leading proponents of this theory of tort, there is an intrinsic normative dimension to the relationship between plaintiff and defendant that tort recognizes - "each harm done and suffered is the core of a single transaction that relates this doer to this sufferer, and each such transaction is a discrete unit of normative significance." Ernst Weinrib, "The Special Morality of Tort Law" (1989) 34:3 McGill Law Journal 403 at 408 [Weinrib, "Morality"].

[21] E.g., *Fiala v Cechmanek*, 2001 ABCA 169 (CanLII) paras 31-32.

[22] For example, "If the harm constitutes an integrated relationship of doing and suffering, the respective parties cannot be considered independently of each other. Normative considerations that are unilaterally applicable either to the doer or to the sufferer are, therefore, out of place.": Weinrib, "Morality," *supra* note 20 at 408. Professor Elizabeth Adjin-Tettey has explained how inequitable a formalistic corrective justice view of damages can be. See for example: Elizabeth Adjin-Tettey, "Discriminatory Impact of Application of *Restitutio in Integrum* in Personal Injury Claims," Taking Remedies Seriously CIAJ 2009 Annual Conference, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2006550> [Adjin-Tettey, "Discriminatory Impact"]; see also, Elizabeth Adjin-Tettey, "Replicating and Perpetuating Inequalities in

However, tort law scholarship and jurisprudence in Canada have not generally taken this formalistic approach to corrective justice. For instance, theorists have proposed expanded conceptions of corrective justice, beyond formalistic constraints, to include other contextual considerations as well.[23] Public policy considerations are also common in tort reasoning, which invariably look beyond the relationship strictly between the plaintiff and the defendant.[24] Compensation for the plaintiff is often also raised as an important value in case law, and deterrence is occasionally cited as well.[25] Tort law has also been said to serve an ombudsperson function (as a system that permits weaker parties to hold more powerful parties to account, and perhaps even effect broader systemic change through, for example, large lawsuits), and a vindication function (creating an avenue through which to seek retribution).[26]

While courts predominantly focus their formal analysis on the dispute between the parties, there is often an implicit if not explicit consideration of policy, normative values, and sometimes other cited functions in tort decision-making, especially when the court is recognizing a new tort or reforming an existing doctrine.[27] As I will examine in greater depth in Chapter 6, tort doctrine is also meant to evolve in line with the values espoused by the *Canadian Charter of Rights and Freedoms*, which takes the judicial analysis beyond a formalistic corrective justice view to consider how important

---

Personal Injury Claims Through Female-Specific Contingencies" (2004) 49 McGill Law Journal [Adjin-Tettey, "Replicating Inequalities"].

[23] Professor Chris Hunt has assessed some of the primary theories of tort law, including different understandings of corrective justice, and argued that recognizing a tort for invasion of privacy fits within each theoretical framing – in other words, whichever function of tort law is applied, a court has the theoretical basis to recognize invasion of privacy as a wrong that must be remedied. See Hunt, "Right to Wrong," *supra* note 18. See also Peter Cane, *The Anatomy of Tort Law* (Portland, OR: Hart Publishing, 1997) at 15-18.

[24] E.g., there are legal tests within tort that specifically require the courts to consider policy and social impacts of their decisions (like the test for when courts should recognize a new duty of care, see e.g., *Cooper v Hobart*, [2001] 3 SCR 537 where the court discusses the role of policy in the court's analysis).

[25] See for example the case law on vicarious liability, which centers on concerns about compensation and deterrence (e.g., *Bazley v Curry*, [1999] 2 SCR 534); see also, e.g., *Clements v Clements*, [2012] 2 SCR 181 at para 41, a case involving negligence, where the court identifies the goals of negligence law as compensation, fairness, and deterrence, "in a manner consistent with corrective justice."

[26] E.g., Allen M. Linden, Lewis N. Klar and Bruce Feldthusen, *Canadian Tort Law, Cases, Notes & Materials*, 15th ed. (Toronto: Butterworths, 2018) at 1-42.

[27] E.g., *Jones v Tsige*, 2012 ONCA 32 at paras 39-46.

social values are reflected in the private law. All of this is to emphasize that while the theoretical view of tort law in Canada often refers to corrective justice, views of justice within tort law actually go well beyond the two parties involved in a dispute to also account for social context and policy concerns. This thesis argues that such an approach is helpful to developing a more nuanced and equitable approach to the privacy torts. My reason for investigating tort law in this thesis relies on the notion that tort can attain a range of policy functions, including but extending beyond corrective justice.

Theorists and scholars who focus on substantive equality in law view the potential goals and function of tort law as ripe for attaining equality goals. For instance, feminist legal scholars have cited tort law as a source of potential for working toward social equality and social justice. In part this stems from the underlying premise that tort law protects human dignity and promotes social cohesion.[28] For instance in her examination of tort as a potential tool for social justice, Professor Leslie Bender proposes the following:

> Tort law protects our interests in physical integrity, emotional health, individual and collective safety, and in personal human dignity through respect and social equality, because we recognize that those aspects of our human nature are as much prerequisites to our harmonious and cooperative social relationships as enforceable promises and possessory privileges are.[29]

She draws from the historical trajectory of tort law as a mechanism to secure compensation for injuries caused due to increasing industrialization in the early 20th century. Tort provides an avenue to hold larger or more powerful entities to account, and can empower individuals to "call the harm-causing defendants to court and to require them to justify themselves and defend their actions" because a defendant cannot ignore a legal action without consequences.[30] While tort law is

[28] Leslie Bender, "Tort Law's Role as a Tool for Social Justice" (1998) 37 Washburn Law Journal 249 at 253 [Bender, "Tort Law as a Tool for Social Justice"].
[29] Bender, "Tort Law as a Tool for Social Justice", *ibid* at 256.
[30] Bender, "Tort Law as a Tool for Social Justice", *ibid* at 259.

not a perfect mechanism for addressing harm, it can serve many equality-enhancing ends, over and above awards of monetary damages.[31]

Jennifer Wriggins has emphasized tort's important normative and narrative roles, in the ways that cases and actions can deal with personal experiences, changing behaviour, identifying injury, and redressing harm, which she identifies as feminist concerns.[32] Other scholars as well have emphasized the potential equality-enhancing and educational/norm setting nature of tort through its focus on interpersonal relations, while simultaneously critiquing formalist and economic approaches to adjudicating disputes.[33] Martha Chamallas notes in reference to recognition of injury and awards of damages that "a judgment also functions as a way of demonstrating the importance we place on human relationships and on legal rights" – sometimes for better or worse depending on the outcome.[34]

Additionally, while certain interpersonal privacy invasions are now addressed through criminal law in Canada,[35] I focus on tort because it can offer a number of practical advantages over criminal law approaches.[36] First, criminal law offences relating to interpersonal privacy intrusions are limited to specific types of highly intrusive conduct, such as criminal voyeurism. Criminal law does not address the spectrum of potential privacy harms in public space. Tort law offers a more general and

---

[31] E.g. Bender, "Tort Law as a Tool for Social Justice", *ibid*; see also, Jane Bailey, "Towards an Equality Enhancing Conception of Privacy" (2008) 31(2) Dalhousie Law Journal 267 (on enhancing the court's understanding of privacy as a producer of substantive equality, focusing on criminal law jurisprudence in this article).
[32] Jennifer B. Wriggins, "Toward a Feminist Revision of Torts" (2010) 12 Am U Journal of Gender, Social Policy & Law 139 at 140.
[33] E.g. Adjin-Tettey, "Discriminatory Impact," *supra* note 22; Adjin-Tetty, "Replicating and Perpetuating Inequalities," *supra* note 22; Jamie Cassels, "The Revival of Tort Theory in Canada" in *Review of Tort Theory*, edited by Ken Cooper-Stephenson and Elaine Gibson, (Toronto: Captus University Publications, 1993).
[34] Martha Chamallas, "The Architecture of Bias: Deep Structures in Tort Law" (1998) 146 University of Pennsylvania Law Review 463 at 507 [Chamallas, "Architecture of Bias"]. Chamallas also emphasizes a shift away from a strictly monetary way of understanding tort law: "interests may deserve legal recognition, even though they may lack precise market valuation": at 507.
[35] See for example the *Criminal Code*, RSC 1985, c C-46 provisions addressing voyeurism (s. 162); criminal harassment (s. 264).
[36] Notably, also, interpersonal privacy is specifically excluded from private sector data protection statutes. See e.g., *PIPEDA* s. 4(1).

more flexible framework for addressing privacy in public. Furthermore, the criminal law elements and burdens of proof are set at necessarily high thresholds, given the stakes for the accused's freedom. Tort law, operating on an evidentiary standard of a balance of probabilities, can be more attainable for a plaintiff in many cases. But more importantly, criminal law primarily provides a state-driven punitive and carceral solution to a social problem, one which further relies on policing and state management of any legal vindication (in the sense that the case is brought and handled by a Crown prosecutor on behalf of the state). Critiques of the carceral and policing system are long-standing and ever-growing.[37]

Tort law certainly has weaknesses and limitations. For instance, bringing forward a claim can place a substantial financial and emotional burden on a plaintiff, and on the defendant in responding. Often tort cases are resolved at the parties' agreement prior to a trial, however trial proceedings, when they occur, can threaten to re-traumatize parties. Tort is primarily responsive rather than proactive (responding to harm, rather than actively preventing it); though the system does enunciate rights, which can be norm setting or norm shifting, it only vindicates those rights after they have been violated. Tort predominantly remedies through money, which can mischaracterize the actual harm suffered (as a dollar value in place of, e.g., a loss of dignity). And tort has not always fulsomely recognized the scale of harm that can arise from psychological or dignitary injuries. Furthermore, tort operates as part of the colonially imposed legal system in Canada. Other ways of imagining justice in interpersonal conflicts are absolutely possible, and while beyond the scope of this thesis, will be necessary to a full examination of how society can and should respond to emerging automated surveillance technologies.

[37] E.g., Angela Davis, *Are Prisons Obsolete?* (New York: Seven Stories Press, 2003); Michelle Alexander, *The New Jim Crow: Mass Incarceration in the Age of Colorblindness* (New York: The New Press, 2010); Mariame Kaba, *We Do This 'Til We Free Us: Abolitionist Organizing and Transforming Justice* (Chicago: Haymarket Books, 2021).

Nevertheless, the tort system offers a victim-driven approach to vindicating harm outside the criminal law system, which can be appealing to individuals for a variety of reasons. A tort claim will additionally often prompt settlement negotiations before full litigation of the matter, which can allow in some cases for a more flexible arrangement to be made between the parties, not limited to financial compensation, and can include vindicating measures like an apology. Finally, tort law provides a mechanism for groups of people who have been harmed by the same defendant to work collectively to vindicate their individual harms (notably, tort does not provide general mechanisms to vindicate *collective* as opposed to individual harm, though arguably such vindication could come from a negotiated settlement). Accordingly, it is a relevant if imperfect site of inquiry for considering the legal responses to interpersonal privacy conflicts arising in public spaces.

Why the Privacy Torts, Specifically?

Within tort law, a range of different actions could apply to privacy-engaging conduct. However, some of actions – like trespass and nuisance – do not apply in public space and are specifically designed to vindicate harm to private property interests. Other actions, like intentional infliction of mental suffering, could apply in certain circumstances but do not and are not meant to address specific *privacy* issues at stake in a claim. The Ontario Court of Appeal has recognized how challenging it is for parties and the courts to attempt to resolve a privacy issue through the application of other tort causes of action that were not designed to address privacy rights and harms.[38] Accordingly, I focus here on the various statutory and common law torts specifically designed to address privacy interests (which I refer to as the "privacy torts" for short). I want to know whether and how tort law can vindicate privacy rights specifically, especially in relation to emerging personal-use technologies in public space.

[38] *Jones v Tsige, supra* note 27 at para 15.

Also, within the scope of tort law, a negligence action might be available to a plaintiff to address interpersonal conflict and harm. Negligence vindicates harms that a defendant causes to a plaintiff due to the defendant's failure to exercise reasonable care – e.g., a failure to follow steps that a reasonable person would take to avoid the harmful outcome. Negligence actions may also be relevant to the sorts of interpersonal privacy conflicts that I examine in this thesis. However, this thesis focuses primarily on the privacy torts and not negligence for some important reasons. First, negligence, like the other torts above, is not meant to specifically address privacy in the same ways as the privacy torts. Second, negligence requires proof of damage – some form of physical or mental injury – as a result of the defendant's negligent behaviour. While the law around mental injury is still developing, it is clear that this must include a significant physiological or psychological impact on the plaintiff.[39] The privacy torts by contrast vindicate privacy harm *per se*, which means these torts recognize that the fact of having one's privacy invaded is a harm in and of itself, without need for proof of further damage. Both practically and in terms of principle, this can be significant to an analysis of interpersonal privacy conflicts in that it sets a lower threshold of proof for the plaintiff and recognizes their intrinsic right to privacy.

This latter distinction between negligence and the privacy torts stems from their different roles within the broader structure of tort law. The privacy torts are all *intentional* torts, which means a plaintiff must prove that the defendant acted intentionally in violating or invading their privacy (as opposed to simply unreasonably, in the case of negligence). Chapter 3 examines the intentionality analysis in greater depth. However, the requirement that a defendant acted intentionally may be complicated when information is collected or personal space is interfered with through the use of an automated technology.[40] This is a complication that may be of increasing relevance to plaintiffs in

[39] *Saadati v Moorhead*, [2017] 1 SCR 543 at paras 37-38; *Mustapha v Culligan of Canada Ltd.*, [2008] 2 SCR 114 at para 9.
[40] Someone acts intentionally when they act with "substantial certainty of the consequences of their actions" (*Garrat v Dailey*, 46 Wash 2d 197 (1955); see also, *Scott v. Shepherd*, 96 Eng Rep 525 (KB 1773)). It is not enough that the harm to a

intentional tort claims generally, given the growing use and prevalence of increasingly automated technologies in Canada.[41]

The ability to make a claim of intentionality can also be an important factor for a plaintiff in seeking accountability and vindication from someone who has caused them harm.[42] More specifically, where a plaintiff is successful in their claim, they will have established intentional wrongdoing on the part of the defendant which may, in addition to compensation, be an important vindicating dimension of their decision to litigate. Intention also serves an important role in constraining the scope of the tort. In some ways this internal limit also makes the privacy torts more relevant to interpersonal privacy conflicts in public space because it will only arise against individuals in instances where they are acting deliberately, and should not open a litigation floodgate in regards to accidental or incidental interpersonal information collection. Negligence and perhaps even vicarious liability might be relevant for addressing some of the peripheral issues not examined in this thesis. But my interest here is in whether the privacy torts, that are meant to vindicate privacy rights, can address the nuances of technology-mediated privacy conflicts in public space, including recognizing intention in the scope of surveillance or policing.

Why Privacy?

Privacy is a notoriously difficult concept to define. There is no universally accepted definition of "privacy," and there has been considerable judicial and academic recognition that the concept is both difficult to delineate and likely encompasses various considerations or expectations.

---

plaintiff be foreseeable, it must be a substantially certain consequence of the defendant's conduct (*Bettel v Yim* (1978), 20 OR (2d) 617). As discussed at greater length in Chapter 3 below, the privacy torts have been interpreted to require more than just intentional conduct. The defendant must *intend to violate/invade privacy* through their conduct.

[41] Kristen Thomasen, "AI and Tort Law" in Florian Martin-Bariteau & Teresa Scassa, eds., *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021).

[42] Jennifer B. Wriggins, "Toward a Feminist Revision of Torts", *supra* note 32 from 153 onward; Leslie Bender, "Teaching Torts as if Gender Matters: Intentional Torts" (1994) 2 Virginia Journal of Social Policy and Law 115 at 118-21.

Professors Daniel Solove and Ari Ezra Waldman, for example, respectively provide detailed analyses of many of the different understandings of privacy, as well as the shortcomings of some theories, especially more traditional theories of privacy that rely on ideas of secrecy and seclusion in the home or a private or controlled space.[43] Solove emphasizes that the privacy discourse that engages in a debate over what should or should not be considered privacy or private is ineffective, and proposes an approach that instead considers privacy to be a cluster of different but related considerations or concerns. In particular, he focuses on "privacy" as relating to the collection, processing, and dissemination of personal information, as well as physical invasions of privacy/intrusions.[44] For the purposes of this thesis I adopt this categorization of privacy, which has also already been generally reflected in the structure of the Canadian privacy torts.[45]

Notably, there is still much to debate about how to *assess* whether and in what circumstances someone could expect privacy - i.e., when one can expect to have a legal interest vis-à-vis the collection, use, sharing of one's personal information or an intrusion into one's personal space. This assessment is usually carried out through an analysis of one's 'reasonable expectation of privacy,' (or a similar concept worded differently), asking whether the reasonable person would expect privacy in the plaintiff's circumstances. There are a range of theoretical approaches that can help to assess 'reasonable expectations,' which I will discuss at greater length later in the thesis, particularly in Chapters 5 and 6.

---

[43] For example, the theory that privacy is synonymous for secrecy (that what is private is that which you keep secret or concealed), or that privacy is synonymous with control (a right to privacy is a right to control information about oneself or access to oneself), are often too vague (e.g., it is unclear what the right or expectation really *is*), too broad (e.g., capturing more than could be legally recognized) or too narrow (e.g., missing significant privacy concerns), or somehow all three at once. See, Daniel J. Solove, *Understanding Privacy* (Cambridge MA: Harvard University Press, 2008); Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge UK: Cambridge University Press, 2018) [Waldman, *Privacy as Trust*].

[44] Solove, *Understanding Privacy, ibid* at 10.

[45] For instance, the common law torts in Ontario generally deal with collection and invasion (intrusion upon seclusion), and dissemination of information (disclosure of a private fact; false light); in the provinces with statutory torts, the statutory language is sufficiently general to address all four of these aspects of privacy violation. These common law and statutory torts are discussed at length in Chapter 3. See also, Hunt, "Right to Wrong," *supra* note 18.

This thesis considers the *privacy* impact of personal-use technology in public space, which reflects just one dimension of interpersonal relationships that might be engaged in public space and mediated through technology. I am focusing on interpersonal privacy in public because it is, as I will show in Chapter 3, a judicially under-theorized area of privacy law in Canada – in other words, courts have not extensively developed this area of privacy in tort law. Yet, drawing on examples of popular and available public facing technologies that are either specifically designed to, or provide seamless affordances to, collect, use, share information and/or physically interfere in one's space, I suggest interpersonal *privacy* intrusions (collection, use, sharing of information and physical intrusion) will become an increasingly significant legal issue in the coming years. Thus, as I examine in Chapter 3, there is a gap in the law in addressing this particular dimension of interpersonal relations in public space. My thesis seeks to contribute to the discussion around how this gap may be addressed.

Notably, also, interpersonal privacy has always been important, even if not as prevalent of a social or political concern. Interpersonal privacy can engage significant power dynamics between those involved, depending on the circumstances. These conflicts can also engage state power – for instance where an individual collects information about another and then shares that with public law enforcement. This is an important realm of interpersonal dynamics which new technologies are bringing to the fore for courts and communities alike. While state and commercial collection of information or physical intrusion is often considered high-stakes in the sense that serious life-altering decisions can be made about people by such powerful institutions, there are many ways in which interpersonal privacy invasions can also be high-stakes for those experiencing intrusions. Stalking, harassment, domestic surveillance, vigilantism, and 'citizen policing' that are facilitated through the informational and physical affordances of remote surveillance technologies can also

threaten the victim's freedom, security, and potentially their life.[46] Interpersonal privacy invasions can be just as harmful to some plaintiffs as state or commercial invasions. Accordingly, it is worth considering how tort law, particularly the privacy torts, might respond to the range of technology-mediated interpersonal privacy conflicts that could occur in public space.[47]

Why Public Space?

For the purpose of this thesis, when I refer to public space, I mean spaces over which private entities and individuals do not have a legal right of exclusion – e.g., not private property (like a home), or quasi-private property where a communal space is operated by a private entity (like a shopping center). Quasi-public private spaces — like private malls, grocery stores, or promenades — might raise some of the same concerns discussed throughout the thesis, but are often subject to different sets of rules and values based on their private-ownership, and so these are excluded. While government control and "ownership" of public spaces is also a contentious issue,[48] I am interested in focusing on the application of the privacy torts in public space because this is where many

[46] See e.g., Jordan Pearson, "Meet the 'Drone Vigilante' who Spies on Sex Workers" (April 4, 2016) Vice News, online: <https://www.vice.com/en/article/kb7zga/drone-vigilante-brian-bates-johntv-oklahoma-spies-on-sex-workers>; AJ Dellinger, "How Drones are Being Weaponized and Used to Stalk and Harass People" (September 19, 2019) Mic, online: <https://www.mic.com/p/how-drones-are-being-weaponized-used-to-stalk-harass-people-18784714>; BBC News, "Drone Stalker Jailed for Spying on Ex-Girlfriend" (November 20, 2020) BBC, online: <https://www.bbc.com/news/uk-wales-55018682>; Brian X Chen, "Your Doorbell Camera Spied on You. Now What?" (February 19, 2020) The New York Times, online: <https://www.nytimes.com/2020/02/19/technology/personaltech/ring-doorbell-camera-spying.html>.
On the privacy interests in data about one's location, see for example, Teresa Scassa, "Information Privacy and Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010) 7 Canadian Journal of Law and Technology 193.

[47] Ultimately, a privacy tort law examination is also important because while personal privacy in public space vis-à-vis government and commercial actors in Canada is regulated to varying degrees, the privacy torts have not been well developed in statute or case law in relation to interpersonal privacy invasions occurring outside private property and space.

[48] See e.g., the recent policing and eviction of a large encampment at Trinity Bellwood's Park in Toronto (a large and popular public park) on the legal basis that the City of Toronto owns the park and thus can enforce trespass notices at the park. E.g., Kerrisa Wilson, "Several arrests made after Toronto clears out large encampment at Trinity Bellwood's Park" (June 22, 2021) CP24, online: <https://www.cp24.com/news/several-arrests-made-after-toronto-clears-out-large-encampment-at-trinity-bellwoods-park-1.5480357>.

interpersonal encounters occur, yet much of the law meant to protect property interests or rights within their private property does not apply. In other words, a plaintiff cannot rely on property-based protections to address a privacy concern. In a sense, public space is a more legally egalitarian space in interpersonal interactions as neither individual in an encounter has more legal rights based in property than the other. That said, especially through the example of home surveillance systems, I also consider the interaction between public space and private property interests and the ways in which this shapes the current state of the privacy torts.

Some notable caveats arise in regards to the focus on this space. Significantly, this thesis deals with laws and concepts, like public space and its regulation, that are colonial constructs. This thesis addresses only the *status quo*, considering laws and technologies within the current Canadian legal system. Addressing the colonial impact of law and technology on public space experiences requires much more than a specific discussion of privacy and tort law, up to and including return of occupied lands as well as ongoing self-reflective and reflexive practices.[49] Indigenous legal orders also have laws and guidance for addressing interpersonal conflicts like the ones at issue here. This thesis makes only one small contribution to a much larger conversation about how technology-mediated interpersonal conflicts can be addressed within or beyond the different legal systems operating in these spaces and places. Additionally, this thesis does not directly consider the civil law system in Québec, which has developed a nuanced approach to privacy in public space, though I do draw upon insights from several notable judicial decisions emerging from Québec.[50]

---

[49] See Eve Tuck & K Wayne Yang, "Decolonization Is Not a Metaphor" (2012) 1(1) Decolonization: Indigeneity, Education & Society 1; Yellowhead Institute, "Land Back: A Yellowhead Institute Red Paper" (October 2019), online <https://redpaper.yellowheadinstitute.org/>; Jeffery G Hewitt "Land Acknowledgement, Scripting and Julius Caesar" (2019) 88 SCLR 27; S Xavier, J Hewitt, A Alvez, A Bhatia, B Jacobs & V Waboose, Decolonizing Law in the Global North and Global South (London UK: Routledge, 2021). See specifically, S. Xavier and J Hewitt's "Introduction" for more regarding the process of reflectivity and reflexivity.

[50] See e.g., *Aubry v Éditions Vice-Versa*, [1998] 1 SCR 591 [*Aubry*] (claimant successfully sues a newspaper for publishing a photo of her taken in a public space without her consent under the *Civil Code of Quebec* and the Quebec *Charter of Human Rights and Freedoms*); *Pia Grillo c Google inc.*, 2014 QCCQ 9394 (plaintiff successfully sues for damages under the *Civil Code of Quebec* and the Quebec *Charter of Human Rights and Freedoms*, after Google posted an image of her on Google Maps).

This thesis also treats 'public space' as a singular concept, but recognizes that not all public spaces are the same. People will have different reasons for accessing different spaces, and will use those spaces for different activities. For example, protests typically take place in city squares, streets, and on sidewalks in order to gain the attention of others, rather than in a quiet city park. Parks might be a place for respite away from busy public streets. Sidewalks are a safer place to congregate than a public road. Regulating or failing to regulate harmful conduct might have a greater or lesser impact on the use of a space depending on why and how people want to access that space. Public space is not a uniform concept — nevertheless, it is beyond the scope of this thesis to carry out an analysis of each various type of public space, and instead my hope is to contribute to some of the broader thinking around the usefulness of privacy torts in these various spaces.

The thesis also particularly considers urban and residential spaces and technologies. While some of the systems considered in this thesis might be deployed in rural areas, wilderness, or ocean spaces, this thesis considers how the technology is being developed and used predominantly in cities, towns, and other residential areas where people congregate or interact, and where interpersonal conflict might more commonly arise.

Methodology

The remaining chapters of this thesis employ various dimensions of doctrinal legal methodology to analyze the application of the privacy torts to interpersonal technology-mediated privacy conflicts in public space. However, in engaging this methodology I also draw on an eclectic range of theoretical insights to unpack some of the legal analysis and advance a reform argument.[51]

[51] As Julie Cohen has described in her important work on understanding embodied privacy in a technology-mediated world, "in any serious study of the role of law in the networked information society, methodological eclecticism is not an indulgence; it is a necessity" Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven CT: Yale University Press, 2012) [Cohen, *Networked Self*]. While this thesis engages one methodology, it similarly benefits from eclecticism of theoretical insights.

These insights stem from a range of legal research fields including feminist legal theory, law and geography, critical race theory, and Indigenous legal scholarship critiquing the colonial legal system's conceptualization of property. These theoretical lenses draw light to questions about what is public space, why is privacy un- or seldom-recognized in public spaces, what does the tort law analysis prioritize, and so on? At each stage through the later chapters, I explain why different theoretical view-points are helpful to the doctrinal legal analysis.

Doctrinal methodology has been described as "research into the law and legal concepts."[52] More precisely, doctrinal methodology can include different research approaches to understanding the law and its application to legal scenarios. Professors Terry Hutchinson and Nigel Duncan have identified four categories of doctrinal legal research: doctrinal (a "systematic exposition of the rules governing a particular legal category," and analyses of the relationship between these rules); reform-oriented research ("intensively evaluates adequacy of existing rules and … recommends changes to any rule found wanting"); theoretical research (which "fosters a more complete understanding of the conceptual bases of legal principles and of the combined effects of a range of rules and procedures that touch on a particular area of activity");[53] and fundamental research ("designed to secure a deeper understanding of law as a social phenomenon, including research on the … social or political implications of law").[54]

This thesis engages with each of these approaches to legal analysis. In the next two chapters, I engage in primarily the first understanding of doctrinal analysis. Chapter 2 involves a predominantly descriptive examination of the state of personal-use remotely-operated technologies that will be used as examples to drive the subsequent legal analysis – namely, drones and

---

[52] Terry Hutchinson and Nigel Duncan, "Defining and Describing What We Do: Doctrinal Legal Research" (2012) 17 Deakin Law Review 83 at 85 [Hutchinson and Duncan, "Doctrinal Legal Research"].
[53] Dennis Pearce, Enid Campbell and Don Harding, *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission* (Australian Government Publishing Service, 1987).
[54] Hutchinson and Duncan, "Doctrinal Legal Research" at 101-102.

sophisticated home surveillance systems. I also briefly consider the significant potential for combining facial recognition applications with either of the technological examples.

Chapter 3 involves doctrinal legal analysis of the current privacy torts as set out in statute and case law. I examine jurisprudence to determine what the law currently "is" as it applies in interpersonal privacy conflicts in public space. This analysis includes understanding the statutory provisions, including through their historical development and subsequent judicial interpretation, and understanding case law from provinces where there is a common law tort. I also engage in legal analysis of the hypothetical application of these statutes and common law legal tests to the technology-based examples set out in Chapter 2.

Chapters 4 and 5 engage theoretical and fundamental doctrinal research, seeking to more completely understand, through a theoretical lens, the conceptual basis for how courts have interpreted the privacy torts. These Chapters identify a significant gap in the law, and expands on these torts as socio-legal phenomena with significant social implications. Chapter 4 considers various critiques of the privacy torts as they exist in Canada right now, in particular drawing from critical literatures to better understand why the torts have evolved in the way that they have. Chapter 5 builds upon this critique through a theoretical understanding of public space privacy interests, and the rights that might be engaged by tort law. This theory assists with legal gap-filling, which is the focus of Chapter 6.

Chapter 6 employs reform-oriented research, recommending changes to the court's understanding of privacy in public space, building on the theory in Chapter 5 and drawing upon additional theory and jurisprudence around how the private law should evolve in line with *Charter* values. Ultimately, in Chapters 6 and 7, the thesis makes recommendations for how the courts could move forward with recognizing the importance of privacy in public spaces, particularly in light of the growing prevalence of personal use remotely-operated surveillance technologies.

Chapter 2: Remote, Personal Use Surveillance Technology and Privacy in Public Space

In order to ground the later analysis of the privacy torts, this chapter examines two examples of increasingly popular personal-use remotely-operated technologies. The examples explored below – drones and sophisticated home surveillance systems – do not reflect an exhaustive list of personal-use surveillance technologies. However, given their increasing popularity and range of affordances, these examples serve as relevant sites of inquiry into how the privacy torts could, or should, apply to interpersonal privacy relations that are increasingly mediated through remote technology. The below sub-sections provide an overview of each of these technological examples, how they work, how they physically engage public spaces and the people in public space, and how they might be used to collect and/or share information from these spaces.

Drones

Remotely-operated aerial devices, colloquially referred to as drones, are the most prevalent robotic/semi-autonomous system in use in public spaces right now in Canada.[55] As noted in the introduction Transport Canada has registered over 53,000 drones in Canada and more than 51,000 pilot certificates as of October, 2020.[56] The popularity and prevalence of drone technology is also expected to continue to grow in Canada and worldwide.[57]

---

[55] On terminology, see e.g.: Roger Clarke, "Understanding the Drone Epidemic" (2014) 30 Computer Law and Security Report 230 at 234 [Clarke, "Drone Epidemic"].
[56] Transport Canada, "Drone Strategy", *supra* note 8 at 9. Also, inferring from U.S. statistics, Transport Canada has estimated that a significant portion of drones will be used by private individuals for non-commercial purposes, see Canada Gazette, Part I, Volume 151, Number 28: Regulations Amending the Canadian Aviation Regulations (Unmanned Aircraft Systems), Regulatory Impact Assessment, online: <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-07-15/html/reg2-eng.php>.
[57] See e.g., Scott Thompson and Alana Saulnier, "The "Rise" of Unmanned Aerial Vehicles (UAVs) in Canada: An Analysis of Special Flight Operation Certificates (SFOCs) from 2007 to 2012" (2015) 41 Canadian Public Policy 207; Transport Canada, "Drone Strategy", *supra* note 8.

Polling, popular media, academic writing, and even Transport Canada's own language regarding drone regulation suggest that public concerns about privacy vis-à-vis drones exist in Canada. Polls from 2014[58] in Canada showed that comfort/discomfort with drones varied by context, in particular depending on who would be operating a drone and for what purposes. For example, 76.4% of respondents either somewhat or fully opposed the use of drones by individuals/hobbyists, compared to only 18.6% opposition to drone use by emergency responders. 76.4% of respondents opposed the use of drones by private investigators; 73.7% opposed industry and private company use; and 73.9% opposed journalists and media use, compared to 81.5% support for emergency responders, and 62.8% support for law enforcement use (37.2% oppose).[59] These results may of course have shifted over the years since this study, and drone regulation will be better informed with more up-to-date and nuanced understanding of the public acceptance or concern with drone technology. Nevertheless, Transport Canada continues to recognize that there is public discomfort with drone use in Canada, and that this reaction at least in part stems from privacy concerns. In fact, Transport Canada has shifted its position from asserting that its role is not to deal with privacy,[60] to more recently developing privacy guidelines for drone operators, which are discussed in greater detail below.

A drone is an amalgam of different technological components, including batteries, motors, sensors, actuators, software programming and algorithms, controllers, *etc.*[61] Each of these components has a unique history of technological development and specific implications for the operation and capabilities of the drone. For the purposes of this thesis, it is not necessary to explore the development of each of these individual components in-depth. Instead, I will explain the key

---

[58] Transport Canada has been conducting more recent polling, however I did not yet have access to these figures at the time of submission.
[59] Scott Thompson and Ciara Bracken-Roche, "Understanding Public Opinion of UAVs in Canada: A 2014 Analysis of Survey Data and Its Policy Implications" (2015) 3 Journal of Unmanned Vehicle Systems 156.
[60] See e.g., the discussion in Kristen Thomasen, "Beyond Airspace Safety", *supra* note 4.
[61] Adam Rothstein, *Drone* (New York: Bloomsbury, 2015) at 57 [Rothstein, *Drone*].

features and capabilities of the technology as a *system*, while also making note of the limitations that various components can place on the system.

I suggest that there are at least two fundamental features specific to drone technology that engage expectations of privacy, particularly in public spaces. These are: (1) the fact that it flies, (2) without a human on-board.[62] These features are common across the spectrum of drone applications.[63] I briefly discuss the technological underpinnings of these two key features of the drone, and the technical limitations of each, to outline what the technology can (and cannot) do, which I will build on in the later legal analysis. Additionally, the fact that drones can be equipped with a range of surveillance technologies including high-resolution cameras, heat detectors, audio recorders, and so on furthers this privacy impact in various ways. Foremost, these technologies can collect sometimes copious or detailed amounts of information and engage privacy through the collection and perhaps later use and distribution of information. Additionally, when someone encountering a drone is aware that the device *could* be equipped with surveillance technologies, whether it is or not, this can have a psychological impact whereby the person alters their conduct or experiences a loss of autonomy due to the mere presence of the drone. A drone equipped with no surveillance technology can also engage privacy considerations where it enters into someone's physical personal space. An added privacy consideration engaged by drone technology relates to the possibility of a security breach in which a third-party gains access to or takes control of the device

---

[62] In his assessment of the features and components of drone technology, Roger Clarke defined a drone as a device that is heavier than air, capable of sustained and reliable flight, with no human on board the device and a sufficient "degree of [self] control to enable performance of useful functions." (Roger Clarke, "What Drones Inherit from their Ancestors" (2014) 30(3) Computer Law & Security Review 247 at 253 [Clarke, "Ancestors"], and Clarke, "Drone Epidemic", *supra* note 55 at 236). I am relying on these same features, though categorize the first two and second two together. Also, I do not think balloons need to be excluded – important to the analysis in this thesis is the drone's capability to move throughout airspace without relying on the whims of the wind (i.e. with some capacity for intentionality). In this case, I would consider a remotely or computer piloted balloon to also fall within the scope of "drones."

[63] See generally: Dan Gettinger et al "The Drone Primer: A Compendium of Key Issues" (2014) Report by the Centre for the Study of the Drone, Bard College at 4-11 [Gettinger, "Drone Primer"]; Ciara Bracken-Roche et al "Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada," Report to the Office of the Privacy Commissioner of Canada (2014) at 8-14 [Bracken-Roche et al, "Surveillance Drones"].

and its information. The technical specifics of security and hacking concerns are beyond the scope of this thesis, but any third party engaged in hacking a drone could also be subject to a tort claim assuming they could be identified. The owner/operator and manufacturer may also be subject to claims regarding measures taken to avoid such security breaches.

Flight

Drone flight is made possible by some sort of propulsion mechanism, the type of which determines other factors like how long the drone can stay in the air or how precisely it can be controlled – each of which can have implications for privacy norms. Many of the widely commercially available drones use rotors for propulsion, such as the common quadcopter design that uses four rotors to support flight. Rotors are spinning blades that push down on the air to give the drone lift.[64] Rotors permit simple take-off and landing because the drone can simply lift off or return onto a surface, including a person's hand depending on the size of the drone. However, because rotor drones are not designed to glide (compared to a fixed-wing drone design, discussed below), rotor-style drones are also more dangerous if the power-source or communications malfunction. The drone could fall straight to the ground. The blades can also cause substantial physical injury.[65]

The use of rotors also allows the drone to fly while relying on small motors and batteries. Reliance on small components means the drone can also be smaller. The size of the device has social

[64] Based on the speed of the rotor rotation the drone can either ascend, descend or hover. By changing the direction of the rotor spin, the drone can also rotate, or tilt forward so the rotors push back against the air, moving the drone in a forward direction. Rhett Allain, "How Do Drones Fly? Physics, of Course!" (May 19, 2017) WIRED online: <https://www.wired.com/2017/05/the-physics-of-drones/>; Rothstein, *Drone, supra* note 61 at 36.

[65] Perhaps most infamously exemplified (at least for Toronto Blue Jays fans) when the pitcher for Cleveland's baseball team had to leave a playoff game against the Toronto Blue Jays because he had previously cut his finger on a drone blade and the wound re-opened mid-game. See e.g., Si Wire, "Bloody Finger Forces [Cleveland] Starter Trevor Bauer to Leave ALCS Game 3" (October 17, 2016), Sports Illustrated, online: <https://www.si.com/mlb/2016/10/18/trevor-bauer-finger-blood-indians-blue-jays>

implications as well as technological ones – a small drone can access spaces where one might not expect such a device (like near trees/woods) more easily than a larger or plane-like drone. When combined with stabilization technology, this small rotor design makes the drone easier to operate in good weather.[66] And the development of open-source rotor drone kits has allowed hobbyists to turn almost any object into a drone by affixing rotors, software and an autopilot unit to the device – making the technology more widely accessible, and in some ways harder for regulators to track and control.[67] The popularity of hobbyist-built drones is growing, and may present challenges for regulation, for instance with regard to the design or software of the drone.

Notably, rotor-operated drones can be quite loud. Due to the noise created by the rotors slicing through the air, commercially available rotor drones might not be used for close-range surreptitious (secret) surveillance, at least in the near future. However, when used for filming, depending on the quality of camera, the drone could operate at such a distance that the sound is not as noticeable, and thus could still discreetly collect information.

Alternatively, drones can be designed and operated using the same mechanisms of flight that on-board piloted airplanes use – with wings as opposed to rotors, and using energy to propel forward. These drones are referred to as fixed-wing drones. They do not require energy for lift or to hold themselves in the air, unlike rotor drones, so they can fly farther on a single battery charge and cover longer distances. This also means that a fixed-wing drone affixed with a payload like a camera can collect significantly more data on a single flight. Fixed-wing drones can also operate much more discreetly, as they do not rely on noise-generating rotors. However, fixed wing drones are not able to hover over a single location like a rotor drone, and launch and landing can be more complicated depending on the size of the drone. While rotor drones can ascend and descend from one place,

---

[66] It could make the device harder to control in bad weather, relative to a fixed-wing drone. Rothstein, *Drone, supra* note 61 at 37

[67] Rothstein, *Drone, ibid* at 39

fixed wing drones may require a runway or a launcher to get them in the air and may need a runway, parachute, or net for safe landing.[68]

Because of this added complexity in flying a fixed-wing drone, to date they have been less common for personal use compared to rotor drones.[69] Fixed-wing drones have been more prevalent in military applications and domestic law enforcement in North America, as well as various farming, mapping, and surveying uses where the longer flight times are advantageous (a use that could certainly be recreational, but is currently more often commercial or research-driven).[70] It is possible that future developments in drone technology will see a hybridization of these two mechanisms for flight, drawing on the advantages of each – better control and longer distances. For instance, Amazon's delivery drone prototype used a hybrid of fixed-wing and rotor design.[71] If this type of drone became available to the public, it could allow for different kinds of uses – ranging from creative filming and expression to longer-term stalking and harassment.

Drone propulsion requires a source of energy that must be carried on board the drone.[72] The energy source, therefore, affects both the design and size of the drone, as well as flight time. Most rotor drones rely on battery power. To date, energy storage in small batteries (that can be carried within a smaller sized drone) is limited, meaning flight times are capped and so the use of a drone to, for example, follow or track someone is also limited. Fixed-wing drones can use gas engines as a power source, offering much higher energy density (i.e. more energy in a smaller

---

[68] For a clear description and comparison of the types of drone technology see e.g., Andrew Chapman, "Drone Types: Multi-Rotor vs Fixed-Wing vs Single Rotor vs Hybrid VTOL" Australian DRONE Magazine (June 2016), and online at: <https://www.auav.com.au/articles/drone-types/>.

[69] Lora Kolodny, "Fixed-wing Drones Not Quite Taking Off in Commercial Market, a New DroneDeploy Study Finds" (August 15, 2016) TechCrunch, online: <https://techcrunch.com/2016/08/15/fixed-wing-drones-not-quite-taking-off-in-commercial-market-a-new-dronedeploy-study-finds/>. While this article is now a bit old, the recreational market continues to be dominated by rotor drones, likely given their smaller size and that they are much easier for a beginner (as well as a professional) to use and transport.

[70] For drone mapping technologies see e.g., Aeromao, online: <http://www.aeromao.com/>; senseFly, online: <https://www.sensefly.com/>.

[71] Amazon Prime Air, online: <https://www.amazon.com/Amazon-Prime-Air/b?node=8037720011>.

[72] With the exception of drones that are tethered to the ground and can be powered through the tether, but which of course then cannot travel as far due to the physical constraint of the tether.

substance/component) compared to other fuel sources.[73] Governments and industry have been developing fixed-wing drones powered by solar panels, with the hope that this renewable energy source will permit significantly longer flight times – at lengths of years rather than the current times of minutes or days.[74] The length of a drone operation can also be extended through the use of drone swarms, in which multiple drones perform an operation together, and where a new drone can take over for another with a depleted battery or power source.[75] Swarms are not yet in common use, in part because of the added layer of communication complexity over the use of a single drone – these drones must be able to communicate not only with the ground but also with the other drones in the swarm.[76] Communication capabilities are discussed further in the next sub-section.

Overall, flight is a key component to drone technology, limited in some ways by current capabilities, but these capabilities are likely to expand especially with corporate investment in research into profitable uses of drones for commercial functions, like the delivery of small goods. Google, Facebook, and Amazon, for instance, have entire research teams devoted to developing drone technology.

Remoteness from a Human Operator

A key feature of the drone that distinguishes it from other airspace technologies is the fact that there is no human on board the device.[77] This is often described terminologically as "unmanned,"

---

[73] Andrew Chapman, "Drone Types: Multi-Rotor vs Fixed-Wing vs Single Rotor vs Hybrid VTOL" (June 2016) Australian DRONE Magazine, online at: <https://www.auav.com.au/articles/drone-types/>.
[74] E.g., Tracy You, "China unveils 'anti-terrorist' drone: solar-powered aircraft can reach 65,000ft and stay in the air 'for years'" (June 2, 2017) Daily Mail, online: <http://www.dailymail.co.uk/news/article-4566614/China-s-solar-powered-drone-reaches-65-000ft-high.html>; Facebook was developing the Aquila drone to deliver Internet (and accordingly, access to Facebook) to places around the world without land access, but has since stopped development, see: Mark Zuckerberg, "The Technology Behind Aquila" Facebook, online: <https://www.facebook.com/notes/mark-zuckerberg/the-technology-behind-aquila/10153916136506634/>
[75] Clarke "Drone Epidemic", *supra* note 55.
[76] Bas Vergouw, Huub Nagel, Geert Bondt and Bart Custers, "Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments" in Bart Custers (ed), *The Future of Drone Use* (Springer, New York: 2016) at 42 [Vergouw et al, "Drone Technology"].
[77] Clarke "Drone Epidemic", *supra* note 55 at 232.

though this is not an entirely accurate descriptor because drones are still largely human-controlled, either through real-time remote control or through pre-programmed flight commands where the drone follows pre-set human instruction. Fully autonomous drones that operate independent of any human input are still largely hypothetical or experimental.[78] Nevertheless, developments in autopilot technology and drone software have already expanded the popularity and ease of use of drones and are expected to continue to do so. These developments also allow the device to operate at further distances from the human controller, which can have socio-legal implications including for transparency (who is flying the device; for what purposes?) and access (operating somewhere the pilot would or could not go themselves).

The absence of a human on board the device has several important implications in terms of both its capabilities and its limits. The capabilities of a drone relative to a human-on-board aircraft can be expanded in some ways. For example, the device does not need to be designed around a person – rather it can be designed with its purpose or the payload (i.e. anything it might be carrying, including a camera or other information collecting technology) in mind.[79] The drone can be much smaller than human-on-board aircraft because it does not have to hold or carry the weight of a person; it can hypothetically remain in-flight for longer (as energy sources permit) because there is no one in the drone to get tired or require a break; and it can be designed to operate in difficult or dangerous places, without putting a human pilot at risk - a central motivator in its initial military development.

---

[78] Clarke "Drone Epidemic", *ibid* at 233. John Villasenor previously argued that a drone is "an unmanned aircraft that can fly *autonomously*" (emphasis added). In his view remote controlled devices are not drones because they are flown by a human operator. He argues that this means they are not autonomous and therefore not "drones." See: J Villasenor, "What is a Drone Anyway?" (Apr 12 2012) Scientific American, online: <https://blogs.scientificamerican.com/guest-blog/what-is-a-drone-anyway/> (accessed May 16, 2017). This definition is narrow and would not capture the technology that is today commonly referred to as a drone: Roger Clarke "Drone Epidemic", *ibid* at 235. In this thesis, remoteness from a human operator is considered the important qualitative feature of the technology, as opposed to autonomy/automation.

[79] See e.g., Donna Dulo, *Unmanned Aircraft in the National Airspace: Critical Issues, Technology, and the Law* (American Bar Association, Washington DC: 2015) at chapter 3.

But because there is no human pilot on board the drone, safe operation relies on and can be limited by (1) the device's ability to collect data about its environment and (2) its ability to communicate accurately and promptly with a remote operator and other sources of operational information (e.g., GPS satellites).[80] Drones must be equipped with sensors and software that permit it to take-in and process information about the surrounding environment.[81] A variety of sensors and payloads can in principle be attached to drones, however the sensor-capabilities for any given drone will be restricted depending on the weight and size of the sensor or payload, relative to the size of the drone itself.[82] Accordingly, larger drones can be equipped with larger or more sensors and other payloads, compared to smaller drones, permitting more information to be taken in and potentially allowing for more complex operations.

Some of these attachments are central to the control and safe operation of the drone; others may be affixed to the drone for additional data collection or other purposes associated with the drone's operation. Many drones are equipped with cameras and microphones – which are particularly important for drones controlled by first-person view, in which the pilot operates the drone based on the video-feed collected by the camera. Cameras can also be infrared, and/or heat sensing, enabling night vision. Drones can be equipped with biological sensors that can trace microorganisms, chemical sensors that can measure chemical compositions/substances, or meteorological sensors to measure wind, temperature and humidity – these are not common in recreational use, but are

[80] HaiYang Chao, YongCan Cao, and YangQuann Chen, "Autopilots for Small Unmanned Aerial Vehicles: A Survey" (2010) 8(1) International Journal of Control, Automation, and Systems 36-44 at 37 [Chao et al, "Autopilots Survey"].
[81] Clarke "Ancestors", *supra* note 62 at 251.
[82] Vergouw et al "Drone Technology", *supra* note 76 at 30.

possible.[83] The data collected through the sensors can then be processed by an on-board computer and/or sent back to the human operator for processing and further instruction.[84]

Advances in autopilot programming also mean that much of the control of the drone can now be delegated to an onboard computer. In many commercially available drones, the human operator no longer has to control each aspect of the drone's balance and movement (the pitch, yaw, roll, throttle), or even take-off, ascent, descent, trajectory and landing.[85] These advances make drones accessible and usable by a broader population that otherwise lacks remote control experience, and also releases some of the operator's attention from control details allowing them to focus elsewhere – e.g., on controlling multiple drones or on payload controls. Different drones have different degrees of autopilot automation – for instance a drone might have automated yaw and pitch controls, but still need remote input for direction of movement, or it could be programmed to move from one point to another using GPS, but its payloads could be controlled by a human operator (like a military drone).[86] As autopilot systems continue to develop, so too might the range of drone applications and the breadth of use by the general population.

Drones are not the only remotely-operated technology entering into public spaces. Legal analyses of the remote nature of drones can overlap or intersect with that related to other robotic technology too, and accordingly, some of the conclusions in this thesis will expand to other public space robot systems. While many systems like sidewalk delivery robots (small systems remotely-driven along public sidewalks to deliver goods like food, groceries, or medications), or security robots (used to monitor premises in place of or in addition to human security guards) are largely

---

[83] Vergouw et al "Drone Technology", *supra* note 76 at 30. Additional non-sensor payloads can include wifi hotspots; equipment to aid with the transport of cargo like mail, supplies, meals, medicine, or contraband; flying advertisements like banners, or speakers; lights and light signals for crowd control; weapons or tear gas; pesticide for precision farming; video projectors; or LED lights for display/entertainment: Vergouw et al "Drone Technology", *ibid* 34-36.
[84] Clarke "Ancestors", *supra* note 62 at 248.
[85] Chao et al, "Autopilots Survey", *supra* note 80 at 37-38.
[86] Gettinger, "Drone Primer", *supra* note 63 at 3; Chao et al, "Autopilots Survey", *ibid* at 38.

commercially operated to date, other robot systems, like autonomous vehicles, may be marketed for personal use.[87] I will not go into detail about these other devices, other than to emphasize that while drones are the most prevalent example of remote/automated personal-use public space technology right now, the notion of remote or automated collection of information and invasion of spaces may become even more widespread as automation becomes more sophisticated and additional forms of robotic technology enter into public spaces. I have discussed some of the legal considerations emerging from these public space robot systems elsewhere.[88]

Canadian Drone Regulation

This sub-section briefly reviews the ways in which Canadian laws directly and specifically regulate drones. The state of Canadian drone regulation: 1) suggests a strong legislative interest in the technology, 2) affects what kinds of use – including privacy invasive use – might be already prohibited (and also, what is permitted and therefore may be arguably expected), and 3) provides groundwork for any potential technology-specific legislative change that might be needed in response to the legal challenges raised throughout the thesis.

The primary drone-specific rules in Canada are those set out by Transport Canada (TC).[89] The TC rules have changed substantially over the last decade, largely in response to the growing

[87] Automated vehicles (AV) are designed specifically for use on public roads. A substantial academic literature has emerged addressing AV, mostly focused on liability issues, though some have focused on privacy issues. Ontario has passed legislation permitting the operation of AV on roads in the province. As of the time of writing Ontario is the only Canadian province where AV can be operated. A number of states in the U.S. have also permitted AV operation and have various regulations in place for use and liability.

[88] See e.g., Kristen Thomasen, "Robots, Regulation, and the Changing Nature of Public Space" (2020) 51 Ottawa Law Review 275-312 [Thomasen, "Robots and Public Space"].

[89] The Minister of Transport (and by extension Transport Canada) has the authority to regulate all aspects of civil aeronautics in Canada, pursuant to the *Aeronautics Act*, RSC 1985, c A-2 [*AA*], which tasks the Minister with "the development and regulation of aeronautics and the supervision of all matters connected with aeronautics": s. 4.2(1)). The *AA* also dictates the procedures for the Minister to develop additional rules through Orders, Interim Orders, and amendments to existing regulations – each of which have been implemented recently with regard to drone regulation. Interim orders can be implemented pursuant to s. 6.41 (1) to deal with significant risks, direct or indirect, to aviation safety or the safety of the public. Several municipalities in Canada have also purported to regulate drones. It is possible that any municipal regulation could be challenged as unconstitutional (particularly where it contradicts the federal rules).

popular interest in the technology, and subsequent concerns about what more drones in the sky might mean for aviation safety. Transport Canada announced in June, 2015 an intention to make sweeping amendments to the existing drone provisions in the *Canadian Aviation Regulations*. Those changes took effect on June 1, 2019 and significantly altered the way in which Transport Canada approached drone regulation.

Previously TC had regulated drones based on category – commercial uses were heavily regulated; recreational (any non-state, non-commercial) uses were largely unregulated. The new approach did away with the distinct regulatory regimes for recreational and commercial-use drones, and instead adopted a weight- and location-based regime. The new regulations apply to all drones flown within the visual line of sight of the pilot (special permission is currently needed for beyond line of sight flights) and that weigh up to 25kg, regardless of the purpose of the flight.[90] In other words, recreational drone use is now regulated along with any other use. The new rules require drone users to register their device with Transport Canada through an online system, mark the drone with a registration number, and pass a knowledge exam. For advanced operations, operators must pass a flight review and be able to show proof of registration and pilot certificate on request.[91] The knowledge exams are highly technical and do not focus on the social aspects of drone use. Transport Canada explained that these changes were prompted by a need for safety (particularly,

---

The Supreme Court of Canada has in several decisions reaffirmed that aeronautics falls exclusively within federal jurisdiction. See *Quebec (Attorney General) v Lacombe*, [2010] 2 SCR 453 and *Quebec (Attorney General) v COPA*, [2010] 2 SCR 536. See also Kristen Thomasen, "Drones in Canada: Who Can Regulate What?" (November 5, 2015) CLTS, online: <https://droittech.uottawa.ca/nouvelles/drones-canada-who-can-regulate-what-why-potatoes-might-be-good-drone-regulation>.

[90] Beyond line-of-sight operations and operations with heavier drones still require special permission from Transport Canada. Specific rules apply based on the following categories: "basic operations" (flown in uncontrolled airspace, more than 30m away from bystanders, never over bystanders); "advanced operations" (flown in controlled airspace, or over bystanders, or within 30 horizontal meters of bystanders); "micro drones" (under 250g, must be flown in line of sight, flown responsibly and never put people or aircraft in danger); "drones over 25kg" (require special permission). Transport Canada, "Find your Category of Drone Operation" (February 19, 2021), online: <https://www.tc.gc.ca/en/services/aviation/drone-safety/find-category-drone-operation.html>.

[91] For each category of operation, Transport Canada has set out a distance requirement prohibiting drone flights close to individuals (with increasing distances based on the weight of the drone).

reducing the potential risk to manned aviation posed by drones) and regulatory predictability, as well as addressing the administrative burden imposed by the increasing number of commercial drone operations that required Transport Canada approval (many of which are now regulated by this regime instead).[92]

While the drone-specific regulations do not address the social impacts of drone use near people, Transport Canada has recently posted privacy guidelines for drone users on its website.[93] The guidelines encourage drone operators to be aware of privacy laws, as well as other offences that may go beyond privacy including voyeurism, mischief, nuisance and other provincial or municipal laws. The guidelines set out the following privacy principles for recreational drones: be accountable (the pilot is responsible for information collected by her drone); limit collection (including blurring faces and licence plates in video and photos); obtain consent; store information securely; be open and responsible about your activities. The website refers commercial operators to *PIPEDA* and its provincial equivalents. And it cites privacy guidelines for government drone operators including conducting Privacy Impact Assessments as required by the *Privacy Act* and Treasury Board Secretariat policy.

Notably though, the guidelines are voluntary, and do not provide actual recourse for individuals whose privacy has been invaded by a personal-use drone. Subsequent chapters will also reveal that the current state of privacy regulation between private individuals is unclear or unable to address many potential privacy concerns related to drone use, so the reference to following the law might not be helpful in actually curbing some privacy invasive uses. More important than any incidental privacy protection arising from drone regulations – especially since these regulations may

---

[92] Canada Gazette, Part I, Volume 151, Number 28: Regulations Amending the Canadian Aviation Regulations (Unmanned Aircraft Systems) (July 15, 2017), online: <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-07-15/html/reg2-eng.php>.

[93] Transport Canada, "Privacy Guidelines for Drone Users" (May 28, 2019) online: <https://www.tc.gc.ca/en/services/aviation/drone-safety/privacy-guidelines-drone-users.html>.

continue to relax as the technology becomes safer and more reliable – is the impact of these rules on the assessment of where and when people can expect privacy. Namely, where drone regulation permits the use of a drone, an operator could argue that therefore anyone in that space ought to expect that the drone may be operating, or even collecting information, and therefore should not expect privacy in that space. While this has not been argued in Canada yet (there have been no drone privacy cases to-date), subsequent chapters consider the role of expectations in the privacy analysis, which could be affected by drone regulations in their current framing.

Drone Privacy Literature

There is a general consensus within Canadian and US academic literature that drones raise privacy concerns, with differences of opinion as to what those concerns entail, whether they are addressed by current laws, and if not, how to address them.[94] Drone technology engages privacy on at least two levels. First, drones have a physical presence and can invade physical, personal space, and which can be privacy invasive of one's physical or bodily privacy, even if no information is collected.[95] Second, drone technology can collect, process, and transmit an array of information depending on the payloads in use, putting informational privacy interests at stake. Even where no data is collected but someone has a perception that data is being collected, an individual may feel a sense of privacy loss. This is examined in the privacy literature in regard to the panoptic effect of

[94] See e.g., Office of the Privacy Commissioner of Canada Research Group "Drones in Canada: Will the Proliferation of Domestic Drone Use in Canada Raise New Concerns for Privacy" (2013) Accessed 2 June 2014 at https://www.priv.gc.ca/ information/research-recherche/2013/ drones_201303_e.asp.; Ryan Calo, "The Drone as Privacy Catalyst" (2011) 64 Stanford Law Review 29; Rachel L. Finn, David Wright, Anna Donovan, Laura Jacques, Laura and Paul De Hert, *Privacy, Data Protection and Ethical Risks in Civil RPAS Operations: Final Report for the European Commission* (Brussels: European Commission, 2015). But see: Morrison, Caren Myers "Dr. Panopticon, or, How I Learned to Stop Worrying and Love the Drone" (2014) 27 Journal of Civil Rights and Economic Development 747.
[95] Roger Clarke, "The Regulation of Civilian Drones: Impacts on Behavioural Privacy" (2014) 30 Computer Law & Security Review 286; Ryan Calo, "Robotics and the Lessons of Cyberlaw" (2015) 103 California Law Review 514.

drones and other surveillance technologies, that can affect individual behaviour due to a sense (even if incorrect) of being watched.[96]

There have been two general responses to these privacy concerns: the majority of which focus on calls for targeted laws to fill specific gaps in legal protection,[97] while some have called for a broader rethinking of privacy frameworks or underlying privacy theory more generally.[98] A small sub-set of this literature focuses on the Canadian context, predominantly recommending targeted legal responses to address some of the identified weaknesses in privacy laws. Authors have especially focused on the use of drones by government agencies, and to a somewhat lesser degree, by companies. Only one article to-date (as of time of submission) has briefly considered the applicability of the emerging common law tort of privacy in Ontario to drone use, despite the growing popularity of personal drone use.[99]

---

[96] See e.g., Ciara Bracken-Roche et al "Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada," Report to the Office of the Privacy Commissioner of Canada (2014).

[97] In particular, much of the U.S. literature emphasizes the adoption of drone-privacy laws or statutes to address these challenges. See e.g.,: Troy Rule, "Airspace in an Age of Drones" (2015) 95 Boston University Law Review 155 (investigating the application of property and trespass law to drones, ultimately advocating for legislation giving landowners strict rights to exclude aircraft from a clearly defined column of low-altitude airspace directly above their land. While not specifically about the privacy implications of drones, the article offers a thorough overview of the US drone law and policy framework, and assess law relevant to the presence of drones in certain quasi-public spaces (i.e. private property visible to the public); Chris Schlag, "The New Privacy Battle: How the Expanding Use of Drones Continues to Erode our Concept of Privacy and Privacy Rights [Note]" (2012-2013) 13 Pittsburg Journal of Technology Law & Policy 1 (arguing that US laws fail to guard against privacy invasions from both publicly and privately operated domestic drones. Argues for a baseline federal consumer protection law to ensure drone-use practices by law enforcement agencies and private parties do not violate reasonable expectations of privacy); Gregory S. McNeal, "Drones and Aerial Surveillance: Considerations for Legislators" *Brookings Institution: The Robots Are Coming: The Project on Civilian Robotics,* November 2014 Pepperdine University Legal Studies Research Paper No. 2015/3 (makes five core recommendations for how legislators can protect privacy with drone-specific regulations); A. Michael Froomkin, and Zak Colangelo, "Self-Defense Against Robots and Drones" (2015) 48 Connecticut Law Review 1 (explores the application of U.S. trespass, property and privacy self-defence rights to drones and other robotic intruders); John, Villasenor, "Observations from Above: Unmanned Aircraft Systems and Privacy" (2013) 36 Harvard Journal of Law & Public Policy 457 (an in-depth consideration of the American constitutional, statutory, and common law frameworks that will inform privacy rights with respect to observations from unmanned aircraft. The author argues the Constitution will provide more protection against government UAS privacy abuses than many anticipate, and emphasizes that there are several common law and statutory protections that will limit non-government entities from violating privacy with UAS).

[98] Clarke, "Behavioural Privacy", *supra* note 95; Calo, "Drone as Privacy Catalyst", *supra* note 94; Paul Holden, "Flying Robots and Privacy in Canada" (2016) 14 Canadian Journal of Law and Technology 65-105 [Holden, "Flying Robots"]

[99] Holden, "Flying Robots," *ibid.*

One of the foundational analyses of drones and privacy in Canada is a report prepared by a team of researchers for the Privacy Commissioner of Canada.[100] The report determined that drones engage the privacy interests of Canadians in particular because of the data collection capabilities of the technology. The report considers the *Privacy Act* which applies to federal government agencies, *PIPEDA,* which applies to commercial activities, and to a lesser extent, constitutional protections afforded under s. 8 of the *Canadian Charter* that apply to constrain state actors.[101] It concludes that while these laws apply to drone use, there are application and enforcement weaknesses that need to be addressed. Common weaknesses in these privacy protections arise because people may not know they are being watched, collected information might not come within the meaning of "personal" or "biographical core" information and therefore its collection not would not be protected under these privacy laws, and where consent is required for collection, it may be difficult or impractical to obtain.[102] The report alludes to but does not deeply consider the implications of public location on the available legal protection.[103]

A more recent piece by Paul Holden expands on this privacy analysis, by considering the application of the torts of trespass, nuisance, and intrusion upon seclusion, in addition to *PIPEDA*, to drone use.[104] Holden concludes that none of these doctrines are fully prepared to address the privacy challenges raised by drones, in particular with regard to data aggregation and privacy in public. He suggests that the tort of intrusion upon seclusion holds promise for privacy protection, if the courts interpret it broadly, though he does not detail a reformed interpretation.

---

[100] Bracken-Roche et al, "Surveillance Drones", *supra* note 63.
[101] *Privacy Act* RSC 1985, c. P-21; *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5; *Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.
[102] Bracken-Roche et al, "Surveillance Drones", *supra* note 63 at 51-3. The report also notes that while the *Privacy Act* applies to government departments that use drones, and requires departments to perform a Privacy Impact Assessment, where the RCMP has used drones, a FOIA request revealed that they had not performed any PIA: Bracken-Roche et al, "Surveillance Drones", *supra* note 63 at 49.
[103] Bracken-Roche et al, "Surveillance Drones", *ibid* at 48, 50.
[104] Holden, "Flying Robots," *supra* note 98.

The federal and Ontario privacy commissioners have each also released reports on drone privacy. In sum, these reports conclude that drones raise informational privacy concerns, that the federal and provincial privacy statutes will apply to drone use by government and commercial actors, and that the legal system must be prepared to address new challenges raised by this technology.[105] Neither of the reports touch upon personal drone use, which is logical as such use does not fall within the purview of the legislation overseen by these Commissioners.

Beyond legislative gap filling, some authors have also called for a rethinking of some of the core legal analysis in different legal doctrine in Canada. For instance, Professor Graham Mayeda has touched upon drone privacy issues primarily as a catalyst to propose a new approach to the judicial analysis of the *Charter* s. 8 reasonable expectation of privacy analysis, which governs privacy relations between government and individuals.[106] He argues that the s. 8 analysis should recognize that privacy is highly contextual, particularly where human relations are mediated by new technology. With regard to drones in particular, this analysis is more specifically tailored to law enforcement invasions of privacy and does not address personal use drones. However, as later chapters will examine, the privacy torts that can regulate interpersonal privacy conflicts also rely on variations of a reasonable expectation of privacy analysis. Accordingly, an argument that this analysis should be contextual and that technology should be considered part of that context, is helpful here as well.

Professor Ciara Bracken-Roche has argued that drones, including personal drones, "reinforce asymmetries in power and visibility that contribute to a politics of verticality."[107] By

---

[105] Office of the Privacy Commissioner of Canada, "Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?," Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada (March 2013), online: <http://www.priv.gc.ca/information/researchTrecherche/2013/drones_201303_e.asp>; Ann Cavoukian, "Privacy and Drones: Unmanned Aerial Vehicles" (August 2012), online: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-drones.pdf>.

[106] Graham Mayeda, "My Neighbour's Kid Just Bought a Drone… New Paradigms for Privacy Law in Canada" (2016) 35(1) National Journal of Constitutional Law 59.

[107] Bracken-Roche, "Politics of Verticality," *supra* note 11.

politics of verticality she is referring to both the symbolic and the practical reinforcement of power through access to the bird's eye view though drone technology. Bracken-Roche accordingly argues that surveillance concerns must be a part of the policy and regulatory discussion of drones, though they currently are not.[108] While not specifically examining the privacy torts, her argument about the power dynamic of an overhead view is relevant when considering the potential harms that tort law might seek to remedy in the event of a court action. This thesis builds on Bracken-Roche's argument, suggesting ways in which such surveillance concerns could be taken into account in tort law. [109]

Some authors have gone even further and called for (or cited that drones might prompt) widespread reform of privacy law in response to the privacy challenges raised by drones (as well as other emerging surveillance technologies) in order to bring privacy laws in line with new technological realities – though none of these calls has been specific to the Canadian legal context.[110] These calls in part rely on the fact that drones can be used to surveil, discreetly and pervasively,

---

[108] Bracken-Roche and I have submitted a similar argument to Transport Canada as a part of its public consultation on changes to its drone rules.

[109] Authors have also discussed more broadly the notion of robotics in public spaces. See my own contribution in relation to the Canadian context – Kristen Thomasen, "Robots and Public Space", *supra* note 88. Additionally, Woo, Wittington, and Arkin have considered the law and policy of urban robotics in the U.S., including considering the privacy impacts in public spaces with a very specific focus on U.S. doctrine that is distinct from Canadian law. Jesse Woo, Jan Whittington & Ronald Arkin, "Urban Robotics: Achieving Autonomy in Design and Regulation of Robots and Cities" (2020) 52 Connecticut Law Review 319. They ultimately argue that cities and local governments should be empowered to develop local privacy regimes to address the data collection and surveillance issues related to robot systems in public space. They argue that any federal action on privacy regulation should allow for local regulation to exist as well – a concern more specific to the U.S. pre-emption doctrine. A key consideration for the authors, also relevant here, is that it is the residents of urban environments who will feel the impact of robot data collection and surveillance, especially early on in the development of these systems. And so, local considerations and concerns should drive regulatory responses. See also, for example, Guangda Zhang, Hai-Ning Liang & Yong Yue, "An Investigation of the Use of Robots in Public Spaces" (Paper delivered at the 2015 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Shenyang, 8 June 2015); Mason Marks, "Robots in Space: Sharing Our World with Autonomous Delivery Vehicles" (Paper delivered at We Robot, University of Miami School of Law, Coral Gables, FL, 12 April 2019) [unpublished], online: <http://robots.law.miami.edu/2019/wp-content/uploads/2019/03/Mason-Marks-Robots-in-Space-WeRobot-2019-3-14.pdf>.

[110] Calo, "Drone as Privacy Catalyst", *supra* note 94; Roger Clarke, "Appropriate Regulatory Responses to the Drone Epidemic" (2016) 32 Computer Law and Security Report. Calo (2011) considers the U.S. perspective and Clarke focuses on Australia, though also touches on European and U.S. perspectives. The handful of Canadian drone privacy literature has sought to identify gaps in various aspects or areas of Canadian privacy law, but has not yet comprehensively reviewed Canadian legal responses to drone privacy conflicts and has not considered what a rethinking of privacy law might look like or how it would proceed in Canada.

public and publicly viewable places with increasing ease and frequency.[111] However, the literature calling for a rethinking of privacy in public spaces in response to drones has not yet comprehensively identified or explained what this reform should entail and how it should be approached, particularly with regard to the Canadian context. My thesis contributes to this growing literature, by considering how and why the Canadian privacy torts should address privacy concerns raised by remotely-operated systems, including drones, in public space. Drones raise particular concerns, including through their aerial and remote functioning.

Personal-Home Surveillance Systems

In order to further nuance the tort analysis in this thesis, I also consider a second personal-use technology, home surveillance systems. These systems raise some similar and some distinct privacy concerns, which can help to further flesh out the doctrinal and theoretical analysis of the torts carried out through the remaining chapters. Home surveillance devices have existed for a long time. But they have more recently become increasingly sophisticated and integrated both within the home architecture and with social networks beyond the home. There are several home surveillance systems commercially available for personal use, but for the purpose of specificity, this sub-section focuses on one example of an integrated home surveillance system produced by Amazon, called Ring. I focus on Ring because it is the most elaborate example of a home surveillance *system* currently available in North America. It constitutes an integrated network between various technologies, individuals, and even law enforcement agencies.[112] Ring is, at its core, a personal

[111] *Ibid.*

[112] The integration between law enforcement and companies raises significant transparency concerns, which are now deepened by the added presence of a private individual carrying out the surveillance perhaps on behalf (explicitly or by implication) of the company and/or law enforcement agency. See Teresa Scassa, "Law Enforcement", *supra* note 13.

surveillance device, and is being developed as an increasingly sophisticated surveillance tool.[113] This is in contrast with drone technology which can have other important social uses unrelated to surveillance (and accordingly can directly engage other important interests and values that must be considered along with privacy).

Amazon Ring is in widespread use in the US, and anecdotally appears to be growing in popularity in Canada too.[114] The technology centers around a door-bell video surveillance device, which is available commercially for just over $100 in Canada. Amazon purchased this product from a California based start-up[115] and made it available to customers in part, perhaps, to address thefts of Amazon packages from house frontages.[116] It is designed to permit homeowners to monitor activities in front of their homes – dropping off and possible theft of packages, who is at the door, who is in front of or passes by their home, *etc.* The device can also be accompanied by other home surveillance or monitoring systems like child monitors and even drones, as well as surveillance-camera equipped motion sensor lights and other features outside the home. Ring's child monitors have been subject to high profile hacking incidents, raising privacy and security concerns within the

---

[113] See e.g., WIPO: WO2019133764A1, "Locating a person of interest using shared video footage from audio/video recording and communication devices" inventors: James Siminoff, Mark Troughton, Aviv Gilboa, Darell SOMERLATT, Alex Jacobson (2018), Google Patents, online, <https://patents.google.com/patent/WO2019133764A1/en>.

[114] Business assessments suggest Ring is the most popular of the home surveillance systems: "Amazon's Ring Leads Google's Nest as 16% of US Homes Adopt Video Doorbells: Strategy Analytics" (February 13, 2020) Business Wire, online: <https://www.businesswire.com/news/home/20200213005824/en/Amazon%E2%80%99s-Ring-Leads-Google%E2%80%99s-Nest-16-Homes>; over 400 police services in the US have also entered into partnerships with Amazon Ring – discussed at greater length below: Drew Harwell, "Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns" (August 28, 2019) The Washington Post, online: <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true>.

[115] For a brief history of Ring (previously, DoorBot), see e.g., Susan Adams, "The Exclusive Inside Story of Ring: From 'Shark Tank' Reject to Amazon's Latest Acquisition" (February 27, 2018) Forbes, online: <https://www.forbes.com/sites/susanadams/2018/02/27/amazon-is-buying-ring-the-pioneer-of-the-video-doorbell-for-1-billion/?sh=dec1594706c2>.

[116] According to Ring's patent history, this is a goal pushing forward further sophistication and development. See e.g., Matt McFarland, "Amazon Considers AI-Powered Doorbell Cameras to Stop Package Theft" (May 10, 2019) CNN Business, online: < https://www.cnn.com/2019/05/10/tech/amazon-package-theft/index.html>.

home for the owner of the system, which are beyond the scope of this thesis but notable to broader discussions of the privacy and security impacts of home surveillance systems.[117]

Many characteristics of the Ring doorbell are similar to other home surveillance systems – namely it produces a video feed of the space surrounding an owner's property, including in many cases, public sidewalks and roads in front of the property, and in some cases the homes or other structures across the street. The system stores video so the owner can access and review it later. The marketing of the device is very much focused on abating (or arguably, stoking fear of[118]) crime, particularly theft, unwanted entry into the home, and even privacy intrusions into the home.

Further, Amazon had indicated interest in associating the Ring system with its facial recognition system Rekognition.[119] This would allow homeowners to be notified if specific persons of interest entered into their video footage. It would also make the search of hours of footage, potentially by homeowners, law enforcement, and/or Amazon more streamlined and automated (while also engaging many of the concerns, weaknesses, and problems with facial recognition that are outlined below). Amazon more recently announced a pause on its development of FRT in response to the Black Lives Matter movement across the United States in the spring and summer of 2020. It is unclear whether the FRT program will resume and what that will mean for Amazon Ring. I specifically consider the implications of FRT for both drones and home surveillance systems briefly below.

---

[117] For example, a class action lawsuit has been filed in negligence, invasion of privacy, and contract and competition law as a result of security breaches in the Ring system: *John Baker Orange v Ring LLC and Amazon.com Inc.* Statement of Claim, US District Court Central District of California, Case No: 2: 19-cv-10899, online at: <documentcloud.org/documents/6593079-JOHN-BAKER-ORANGE-v-RING-LLC-and-AMAZON-COM-INC.html>.

[118] See e.g., Joshua Benton, "The Doorbell Company that's Selling Fear" (May 1, 2019) The Atlantic, online: <https://www.theatlantic.com/ideas/archive/2019/05/amazon-owned-ring-wants-report-crime-news/588394/> (exploring Ring's move to hire journalists to prepare and distribute crime news to neighbourhoods as part of an effort to increase fear of crime despite statistics showing dropping crime rates).

[119] Sam Biddle, "Amazon's Ring Planned Neighbourhood "Watch Lists" Built on Facial Recognition" (November 26, 2019) The Intercept, online: <https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/>.

There are at least two additional features of Ring technology that raise particular interpersonal privacy in public considerations, and make it a helpful example to deepen the privacy analysis in this thesis. These are: the association of Ring with a social media application called Neighbors; and the association of the Ring system with explicit police partnerships across the U.S. and potentially in Canada in the future.

Neighbors App

In addition to the home surveillance device, Ring also includes an integrated neighbourhood data and commentary sharing platform called Neighbors. To date Neighbors is only available in the U.S., though it may come to Canada with the increasing popularity of the device as well as the recent prospect of Amazon partnering with police departments in Canada (discussed further in the next sub-section). I consider this streamlining of sharing here in relation to the privacy torts as a future possibility, and as a part of the norms and culture built up around Ring and modern home surveillance. Other neighbourhood sharing apps in Canada like NextDoor are already used by neighbours to share their Ring footage, so while using another app may not be as frictionless, it is certainly still a possibility associated with sophisticated home surveillance systems.

Neighbors allows residents to "get real-time crime and safety alerts from [their] neighbors and local law enforcement."[120] It allows individuals to seamlessly share video footage from their device with other neighbours in their area, and with law enforcement, voluntarily or through a prompt sent by law enforcement when investigating a crime or reports of crime. The app creates an "incident map" which shows crimes, or reports of suspected crimes or suspicion, by law enforcement and other app users, in one's area. It allows neighbours to communicate with one another about concerns around activities or different people in their neighbourhood. This raises a

[120] Apple, App Store Preview, online: <https://apps.apple.com/us/app/neighbors-by-ring/id1218902777>.

connected concern that Amazon is creating a culture of fear about crime in conjunction with its marketing of Ring, presumably to sell more products, that could lead to greater suspicion and associated surveillance of supposed 'strangers'[121] in public spaces.[122] This seamless sharing between neighbours raises privacy concerns for those captured in video not only in regard to collection of information, but now also in regard to the subsequent use of that footage and potential consequences associated with that use (e.g., law enforcement or interpersonal policing/vigilantism). Amazon's promotional videos make clear that the video captures footage from beyond the property line, even focusing on this fact in some of its advertising.[123]

Amazon has also recently extended Ring's neighbourhood network through a system called Amazon Sidewalk, which includes the ability for neighbours to share bandwidth with one another so that in the event one neighbour's Internet goes down, their Ring system can continue to function by drawing from another neighbour.[124] Sidewalk appears to be another step in the direction of integrating neighbourhood surveillance networks and infrastructure, in support of state and commercial interests but through the conduct of individuals.[125]

Further, the Neighbors app is not just meant for interpersonal sharing and commentary but, as noted, is also designed to allow streamlined sharing of footage with law enforcement. While state collection and use of information is beyond the focus of this thesis (though I will later examine

---

[121] See e.g., Sara Ahmed, who brings a critical lens to the concept of "stranger" that is directly relevant here as well: *Strange Encounters: Embodied Others in Post-Coloniality* (Routledge, Oxfordshire, UK: 2000).

[122] Professors Chris Gilliard, Bonnie Stewart, and others have signaled these concerns about a culture of fear associated with Ring and its marketing, see e.g., Chris Gilliard, "Caught in the Spotlight" (January 9, 2020) Urban Omnibus online: <https://urbanomnibus.net/2020/01/caught-in-the-spotlight/>; Bonnie Stewart, "One Ring to rule them all: Surveillance 'smart' tech won't make Canadian cities safer" (January 21, 2020), The Conversation, online: <https://theconversation.com/one-ring-to-rule-them-all-surveillance-smart-tech-wont-make-canadian-cities-safer-129747>.

[123] E.g., shows that owners can see if someone from a sidewalk failed to clean up after their dog on their front property/lawn.

[124] Amazon Sidewalk, online: <https://support.ring.com/hc/en-us/articles/360032524592-Opting-In-and-Out-of-Sidewalk>; Ring, "Amazon Sidewalk Information", online: <https://support.ring.com/hc/en-us/articles/360032492292-Amazon-Sidewalk-Information>.

[125] The individualist focus of tort limits this mechanism from dealing with systems and architecture directly, but tort can be impactful indirectly through, e.g., threat of significant financial liability in certain circumstances like a class action.

some case law addressing constitutional limits on state searches), this integrated connection with law enforcement raises the stakes of interpersonal privacy concerns related to Ring and similar devices.[126]

Ring is a System that includes Law Enforcement

Ring is marketed in the U.S. in part through partnerships with police services. At the time of writing, Amazon had entered into agreements with over 400 U.S. police departments to provide those departments with Ring doorbells that police could distribute to local residents.[127] On at least one occasion, a police unit was contractually obliged to encourage residents to adopt the Ring system.[128] The mayor and police service of Windsor, Ontario were in discussions with Amazon about the potential of entering into Canada's first police partnership, prior to the pandemic.[129] It is unclear if these discussions are ongoing.

This integration with law enforcement is of course not a feature of the physical device, rather it is an important component of the home surveillance *system*. Ring's approach to marketing has made explicit that policing is a part of the interpersonal surveillance system that is centered around a video doorbell but certainly not limited to just that video technology.[130] The explicit inclusion of policing in the surveillance system arguably increases the stakes of information

---

[126] See also Scassa, "Law Enforcement," *supra* note 13.
[127] Lauren Goode and Louise Matsakis, "Amazon Doubles Down on Ring Partnerships with Law Enforcement" (January 7, 2020) WIRED, online: <https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/>.
[128] Caroline Haskins, "Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement" (July 25, 2019) Motherboard, online: <https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement>.
[129] "Windsor Partnership with Amazon Ring Doorbell Could Do More Harm than Good, Experts Say" (January 23, 2020), CBC Windsor, online: <https://www.cbc.ca/news/canada/windsor/windsor-amazon-ring-partnership-could-do-harm-experts-say-1.5437144>.
[130] For instance, by recruiting police officers as brand ambassadors, see e.g., Tyler Sonnemaker, "Amazon Ring Recruited LAPD Officers as Brand Ambassadors to Help Sell its Products Through Influencer Marketing" (June 17, 2021) Business Insider, online: <https://www.businessinsider.com/amazons-ring-recruited-lapd-officers-as-brand-ambassadors-report-2021-6>.

collection such that now there might be state power behind the interpersonal concerns caught on video. But it also places, at least, a marketing emphasis on the fact that Ring is part of a crime prevention and policing system that includes interpersonal surveillance and policing. This incorporates an additional interpersonal and power dynamic into a potential privacy conflict in public space, wherein an individual who is filmed in public by a Ring camera is disempowered not only from their ability to prevent such surveillance, but also relative to the Ring owner who can now connect seamlessly with a network of neighbours and law enforcement for support. This plays an important part of the forthcoming legal analysis.

Ring Engages Public Space Specifically

The whole point of a Ring doorbell system is to watch and collect information about what is happening in the public-facing direction of an individual's private home and property. The device sits at a physical boundary between public and private, and is designed to monitor and enforce that boundary. This technological system inherently engages considerations about public space, because it is perceived and designed as a way for private homeowners and residents to monitor and defend against intrusions into their property from the people who may access or approach their property from public space. This is true even where Ring is used in an apartment building or condominium, for instance, as a way to monitor people and occurrences in the semi-public shared hallways and other spaces outside a private unit. Accordingly, Ring (as an example of an extensive home surveillance system) raises many of the same themes of privacy concerns as drone technology, and other public-facing personal use technologies, which are explored throughout this thesis. In particular, these technologies engage a space in which people may have an interest not to be under surveillance yet, to date, can rely on little if any tort recognition of this interest (further examined in Chapter 3).

Of course, depending on the residence - e.g., its structure and set back from public sidewalks and roads - the surveillance system can be positioned so that it only captures information from within the private property line, or so that it films for example, a backyard. For the purpose of this thesis, I am focused on instances where the camera captures footage and other information about the public spaces in front of a private residence. Several of the insights from the legal analysis here can also be relevant to cameras angled within private property, however, that will not be my analytical focus within the thesis.

Ring Privacy Literature Review

Ring is relatively new, having been introduced by Amazon in 2018 (though it was originally founded in 2013), but in its relatively short time of use has already been subject to critique, including long-essays, op-eds, and investigative reports. The device has been critiqued for a range of issues including that it does not actually work to reduce crime,[131] and that it can be easily hacked.[132] Of greatest import to the analysis in this thesis have been critiques regarding the privacy implications of the technology, and the ways in which it facilitates oppressive interpersonal power dynamics, including racial profiling and stereotyping.

Professor Chris Gilliard has written about personal use technologies, like Amazon Ring and Neighbors, and the ways in which these technologies reinforce social oppression in the U.S. Many of his concerns translate to Canada as well, with the exception that some of our privacy laws, in particular the data privacy laws that would apply to Amazon, are more stringent here. His focus, like that of this thesis, shifts from the corporate and law enforcement agents' use of smart technologies

[131] Cyrus Farviar, "Cute Videos, But Little Evidence: Police Say Amazon Ring Isn't Much of a Crime Fighter" (February 15, 2020) NBC News, online: <https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026>.
[132] See e.g., *John Baker Orange v Ring LLC and Amazon.com Inc,* supra; Sara Morrison, "All those hacks got Amazon's Ring sued" (December 27, 2019) Recode, online: <https://www.vox.com/recode/2019/12/27/21039517/amazon-ring-hacking-lawsuit>.

to examine the ways in which technologies are being designed as "digital monitoring tools for the concerned citizen."[133] In particular, he emphasizes how these technologies create "different spatial experiences" for people on either end of the device, and for people of different races and classes who are subjected to this remote and sometimes pervasive gaze.[134]

Neighbours watching out for and communicating with one another about activities in a neighbourhood is not a new phenomenon. Groups like Neighbourhood Watch have been subject to some critique for their tendency toward profiling and drawing lines of inclusion and exclusion.[135] But this also is not the precise social relationship that Ring is replicating. Distinct from when people watch out for each other, the creation of surveillance footage though technologies like Ring, Gilliard emphasizes, "often encourages "solutions" that far outstrip the level of [an] infraction." For example, if a relatively minor incident – Gilliard gives the example of teenagers throwing an egg at a car – were not caught on film, likely no one would bother to report it to police. But once there is tangible surveillance footage, those who possess the footage feel compelled to use and share it, turning what would otherwise be a minor incident into a potentially serious high stakes encounter with law enforcement for the egg thrower (or anyone mistaken as the thrower).[136] Notably, even

---

[133] Gilliard, "Caught in the Spotlight", *supra* note 122.

[134] *Ibid.* See also Teresa Scassa, "Police Service Mapping as Civic Technology: A Critical Assessment" (2016) 5(3) International Journal of E-Planning Research 13 (discussing how U.S. mindsets around crime and crime mapping can be embedded in the design of U.S.-made/used technologies, and when the technology is imported into Canada, these visions of crime are imported as well).

[135] See for example, Sara Ahmed, *Strange Encounters, supra* note 121 (examining the ways in which Neighborhood Watch and the notion of neighbourhoods can other those not considered neighbours, and values and devalues lives according to a colonial neighbour/stranger dichotomy); Eve Darian-Smith, "Neighborhood Watch – Who Watches Whom? Reinterpreting the Concept of Neighborhood" (1993) 52 Human Organization 83 (questioning the ways in which the notion of neighbourhood can be co-opted to serve individual and institutional interests that the program was initially conceived to eliminate); Dennis P. Rosenbaum, "The Theory and Research Behind Neighborhood Watch: Is it a Sound Fear and Crime Reduction Strategy?" (1987) 33 Crime & Delinquency 103 (considering, among other things, whether Neighborhood Watch might actually (erroneously) increase neighbours' fears of crime).

[136] Recent reporting has highlighted that some police agencies are now over-burdened by footage produced by Ring cameras, and that this undermines any actual law enforcement effectiveness that might stem from individuals having a Ring system. See e.g., Cyrus Faviar, "Cute videos, but little evidence: Police say Amazon Ring isn't much of a crime fighter" (February 15, 2020) NBC News, online: <https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026>. The vast amount of data, which is overburdensome for individual officers to sort through, may feasibly be cited to justify the incorporation of facial recognition software into the Ring systems in the future.

though Gilliard emphasizes the distinction between Neighbourhood Watch and Ring, he also points out that Ring formerly drew a direct analogy to Neighborhood Watch. Gilliard reminds readers that Ring markets itself in this way "without considering the connotation of that phrase in a world where Trayvon Martin was killed by a racist acting as a "neighborhood watch.""[137] Ring and home surveillance systems more generally cannot be understood outside the scope of the history of interpersonal policing and vigilantism in the US, and which exists in Canada as well.[138]

Gilliard connects Ring, and other personal use surveillance technologies, to the notion of "security theater": "practices that present the illusion of increasing security or safety, but have no meaningful effect." He explains:

> More than providing any real deterrence, Ring militarizes public space by helping construct a web of police surveillance that would be otherwise impossible. Individual homeowners would likely balk if police asked to put cameras in front of every person's house. Sold by Amazon and ostensibly owned and controlled by homeowners, those same cameras are embraced.[139]

The notion of interpersonal policing of public space and of the boundaries of one's private space feeds into broader social power dynamics around who belongs in a neighbourhood, who has a right to use public spaces, and what are the consequences of contravening neighbourhood norms and expectations. Gilliard further connects Ring with broader discussions about hypersurveillance of racialized people and communities in public spaces, and the different ways in which these

---

[137] Gilliard, "Caught in the Spotlight," *supra* note 122.

[138] In Canada, see e.g., Gina Starblanket & Dallas Hunt, *Storying Violence: Unravelling Colonial Narratives in the Stanley Trial* (ARP Books, Winnipeg, Manitoba: 2020) at 15 [*Storying Violence*] (discussed at greater length in Chapter 4); Constance Backhouse, *Colour-Coded: A Legal History of Racism in Canada, 1900-1950* (University of Toronto Press, Toronto: 2007); in the US concerns about interpersonal policing and vigilantism also have a long and devastating history. Recently Ahmaud Arbery was murdered by Gregory and Travis McMichael in an act of interpersonal policing, see e.g., Sean Boynton, "Ahmaud Arbery: Murder Charges Laid After Case of Slain Black Man Sparks Outrage in US" (May 7, 2020) Global News online: <https://globalnews.ca/news/6919350/charges-laid-ahmaud-arbery-shooting/>.

[139] Not to mention, Ring's viral videos further encourage residents to find crime in their video, because crime videos can become viral content.

technologies only serve to fuel more anxiety and less enjoyment of public space for both the watcher and the watched:[140]

> … as with Ring, powerful and connected surveillance tech in the hands of "regular" citizens ramps up fear with constant notices of "invasions" by outsiders. We have already seen what this looks like in viral videos of "BBQ Becky" or "Pool Patrol Paul": hypervigilant policing of Black users of public spaces. Expanded surveillance capabilities only magnify these effects. Black and brown folks are well aware of the likelihood of being watched when they enter predominantly white and wealthy communities, even when they are residents of that community. But the ability to track and identify people whenever they cross an invisible barrier raises the stakes — not only in the case of being falsely identified by technology, but also in the case of being correctly identified but falsely implicated in illegal activity.[141]

With regard to Ring in Canada, Professor Bonnie Stewart published an op-ed in response to the prospect of a Windsor police force partnership with Ring, arguing that the partnership should be rejected in the city, and across Canada, in large part for the same reasons emphasized by Gilliard in the US context.[142] She also emphasizes the distinction between people monitoring or watching-out for each other directly, and a corporate surveillance infrastructure like Ring that facilitates the "datafication" of our daily lives. Similar to Gilliard, she is concerned that Ring will have particularly inequitable outcomes, as "notifications about so-called suspicious persons feed race and class biases and encourage vigilante behaviours."[143] Ring raises concerns not just about interpersonal privacy, but the particular dynamic of more socially powerful individuals taking on the surveillance and policing of marginalized communities.[144] Ring and other home surveillance technologies

---

[140] See also, Rani Mola, "The Rise of Fear-Based Social Media like Nextdoor, Citizen, and now Amazon's Neighbors" (May 7, 2019) Recode, online: <https://www.vox.com/recode/2019/5/7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors>.
[141] Gilliard, "Caught in the Spotlight", *supra* note 122.
[142] Bonnie Stewart, "One Ring to rule them all: Surveillance 'smart' tech won't make Canadian cities safer" (January 21, 2020) The Conversation, online <https://theconversation.com/one-ring-to-rule-them-all-surveillance-smart-tech-wont-make-canadian-cities-safer-129747>. Professors Stewart, Natalie Delia Deckart, Mita Williams and I also organized a community panel to discuss the implications of Ring, along with guest speaker Professor Chris Gilliard: "Safer Communities in a 'Smart Tech' World: Resisting Ring in Windsor, Ontario" online: <http://noringplease.ca/>.
[143] Stewart, "One Ring", *ibid.*
[144] See e.g., the citations at *supra* note 135.

potentially amplify these concerns through the combined ease of collection of greater quantities of information in a permanent and easily sharable form.

Regulation of Ring/Home Surveillance in Canada

Unlike drone technology, there is no national technology-specific regulation limiting the use of Ring or other home surveillance systems in Canada. This is likely for good reason, as drones fall within the scope of the federal government's jurisdictional authority over airspace, but home surveillance systems would likely be provincially or municipally regulated. Some municipal by-laws may regulate the use of surveillance cameras beyond the perimeter of one's property, though these are haphazardly applicable across the country. For example, the City of London, Ontario prohibits visual surveillance as a fortification of property that could impede city, law enforcement, or emergency personnel from accessing property.[145] It is not clear from the by-law how a surveillance system would impede access to the property. However, a similar by-law exists in Hamilton, Ontario which was initially passed in response to the presence of biker gang clubhouses that used surveillance systems to maintain perimeter security.[146] It is imaginable that a surveillance system may be used to determine when to employ other restricted fortifications, or to alert occupants to the entry of law enforcement onto the property so that they may attempt to obstruct them, destroy evidence, or flee.

While these by-laws may prevent certain uses or designs of home surveillance systems defined in the by-law as "excessive"[147], it is not targeted at addressing interpersonal public space

---

[145] *Fortification of Land By-law* PW-8 2002, online: <https://london.ca/by-laws/fortification-land-law-pw-8>.
[146] *City of Hamilton By-Law No. 10-122; A By-law to regulate the fortification of land and protective elements applied to land and to prohibit excessive fortification of land and excessive protective elements being applied to land in relation to the use of land within the City of Burlington, By-Law No. 108- 2002* (Burlington, ON) also has similar by laws.
[147] E.g., observation towers (1.1(b)), and the by-law does restrict "excessive protective elements" on a home including video cameras, night vision systems, and electronic surveillance devices that can view or listen beyond the perimeter of land: *Fortification of Land By-law* PW-8 2002, s. 1.1(c).

surveillance, so will not serve as a restrictive by-law in all cases. Municipal-level regulation may be pertinent in an interpersonal home-based surveillance conflict where the person surveilled seeks to specifically terminate the surveillance beyond the homeowner's property. However, the privacy torts will remain relevant as well if the surveilled individual wishes to seek any further interpersonal remedy, including compensation. Local laws may also be employed by plaintiffs to argue that a defendant's conduct is unreasonable.

The use of Ring would of course also come within any technology neutral regulations, much like the drone. This thesis specifically examines the application of one such area of technology-neutral law – the privacy torts. The collection and use of footage from the device by either Amazon, or law enforcement agencies might also engage technology-neutral regulation including *PIPEDA* and s. 8 of the *Charter*, though the fact that collection occurs through the private homeowner first can complicate this relationship. A deep legal analysis of these issues is outside the scope of this thesis, however, Chapter 6 does consider the application of *Charter* s. 8 in public space, which may be applicable to law enforcement use of Ring footage.

The Further Prospect of Personal-Use Facial Recognition Technology

This sub-section briefly expands on the possible application of facial recognition technology to the technologies noted in the above sections. Software-based facial recognition technology (FRT)[148] can be applied to information or images collected by drones, Ring, or other personal surveillance technologies. While this thesis considers drones and home surveillance architecture specifically, FRT is so potentially invasive of interests in anonymity, obscurity, and other forms of privacy, and so potentially applicable to the use of the technologies examined in this thesis, that it is

[148] The concerns raised by FRT can apply to other forms of biometric recognition too, like gait recognition. To date, FRT has been the only form of recognition technology promoted or hypothesized for personal (rather than state or commercial) use, so this thesis focuses on FRT, but some of the concerns briefly highlighted here can certainly apply to recognition systems more widely.

worth briefly explaining its potential impact as a subsequent application to images collected by personal surveillance technologies. This potential alignment between personal use technologies and FRT applications only serves to amplify privacy concerns and the urgency to address the legal recognition and vindication of privacy interests in public space.

FRT is a biometric technology that maps a person's facial structure and features, and can be used to match images with data points from previous images of that person for identification purposes.[149] FRT has already been used by law enforcement and commercial agencies in Canada. A recent revelation of RCMP and other law enforcement and commercial use of the company Clearview AI's FRT application brought the privacy concerns associated with FRT to public attention in Canada. Additionally, the Privacy Commissioner of Canada's recent report on the use of FRT in Canadian shopping malls drew attention and significant outcry regarding the unfettered use of such technology.[150] However less well-known FRT systems, like FindFace which is designed to match images of female escorts and pornography actors to their social media accounts, or Pim Eyes which allows for a search of the Internet based on a submitted photograph, also employ FRT more specifically for personal-use.[151] Clearview AI has also suggested it may develop into personal-use

---

[149] Lucas Introna & Helen Nissenbaum, "Facial Recognition Technology: A Survey of Policy and Implementation Issues" (2010) Report for the Center for Catastrophe Preparedness and Response (New York: New York University, 2009)

[150] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia* (October 28, 2020) PIPEDA Findings #2020-004, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/>.

[151] See e.g., Kevin Rothrock, "Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses" (April 26, 2016) arsTechnica, online: <https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/> (explaining the use of FindFace to identify and subsequently harass women who appear in pornography); EJ Dickson, "How facial recognition technology could bring a slutshaming nightmare" (May 31, 2019) Rolling Stone, online: <https://www.rollingstone.com/culture/culture-features/facial-recognition-technology-porn-stars-sexism-841743/>; see also S.L. Nelson, "Sex work and social media: Policy, identity, and privacy in networked publics and counterpublics" (2019) 8(1) Lateral: Journal of the Cultural Studies Association (examining privacy strategies and tactics utilized by sex workers).

technologies, though it has on other occasions said it would not do so. Regardless of whether Clearview AI provides personal-use FRT, more widespread personal-use FRT seems possible.

FRT is notoriously unreliable, particularly with respect to inaccuracies identifying people of colour, and women of colour specifically. The data sets used to train FRT programs have not included a diversity of images and have resulted in greater accuracy for images of white men, because the systems have been trained using similar data.[152] But both accurate and inaccurate identification through FRT can have significant, potentially devastating, implications for the individual being identified, depending on the circumstances. Inaccurate identification can lead to false arrests, charges, and the trauma that accompany these experiences.[153] Accurate FRT can also be devastating, as demonstrated through the personal experiences of the women identified using FindFace, as but one example.[154]

FRT is not inherently a public space technology like Amazon Ring or (in many ways) drone technology. Nevertheless, it engages significant considerations in public space – *especially* when it is combined with either of the above two technologies. Among other things, it threatens what Professors Evan Selinger and Woodrow Hartzog have referred to as one's ability to remain private through *obscurity*.[155] For instance, the practical difficulty or impossibility of identifying every person

---

[152] See e.g., Joy Buolamwini & Timnit Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification" (2018) 81(1) Proceedings of Machine Learning Research 1-15 (demonstrating racial and gender bias that leads to particularly inaccurate responses for Black women in several high profile FRT systems).

[153] There have been numerous instances of this, including in Detroit as a result of the city's Project Greenlight FRT program. See e.g., Drew Harwell, "Wrongfully Arrested Man Sues Detroit Police Over False Facial Recognition Match" (April 13, 2021) The Washington Post online: <https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/>; see also the activism work of Tawana Petty and others in Detroit, e.g. Tawana Petty, "Defending Black Lives Means Banning Facial Recognition" (July 10, 2020) WIRED online: <https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/>.

[154] Kristen Thomasen and Suzie Dunn, "Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canadas Decision in R v Jarvis" in Jane Bailey, Asher Flynn, Nicola Henry (eds) *Handbook on Technology-Facilitated Violence and Abuse: International Perspectives and Experiences* (Bingley, UK: Emerald Publishing Ltd, 2021) [Thomasen & Dunn, "Reasonable Expectations of Privacy"]

[155] Evan Selinger and Woodrow Hartzog, "Obscurity and Privacy" in Joseph Pitt and Ashley Shew (eds) Routledge Companion to Philosophy of Technology (London, UK, Routledge: 2016) [Selinger & Hartzog, "Obscurity"] (explaining the concept of obscurity as a form of privacy/privacy expectation); Evan Selinger and Woodrow Hartzog, "The Inconsentability of Facial Surveillance" (2019) 66 Loyola Law Review 101 ["Selinger & Hartzog, "Inconsentability"] (arguing that legal protections against the use of FRT cannot be based on consent. Consent is a broken mechanism

one encounters in a day provides a form of privacy protection. We can maintain anonymity and privacy because it would be costly and difficult to go through so many identification processes. FRT can eliminate these cost and other practical boundaries, making it possible to identify theoretically anyone in public space who has other publicly available and identifiable images.[156]

Accordingly, there is a growing literature on the privacy implications of FRT, which focuses especially on commercial and state uses of the technology (logically, since these actors have been the primary adopters of FRT to date).[157] This literature emphasizes that current laws (with a particular academic focus on US laws) insufficiently respond to the privacy and other social concerns raised by the technology, and calls for urgent reform.[158]

To date, there have been no technology-specific regulations adopted in Canada regarding the use of facial recognition technology by private individuals. Numerous cities and some states in the United States have adopted laws restraining the use of FRT, though these are generally limited to use by public/government actors.[159] There is a strong community and activist resistance to the use of

---

because the individual risks are too opaque to make an informed choice, and the concept overlooks collective autonomy and obscurity interests).

[156] This is how Clearview AI established its database, by scraping publicly available images from social media sites online to create what has become a widely distributed FRT tool in Canada and the US. Clearview AI claimed that this practice was legal; however, Privacy Commissioners in Canada have found it in contravention with commercial privacy legislation in Canada. See: Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, PIPEDA Findings #2021-001 (February 2, 2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

[157] See e.g., Buolamwini & Gebru, "Gender Shades", *supra* note 152; and Selinger & Hartzog, "Inconsentability", *supra* note 155; Alessandro Acquisti, Ralph Gross, Frederic D Stutzman, "Face Recognition and Privacy in the Age of Augmented Reality" (2014) 6(2) Journal of Privacy and Confidentiality 1-20; and so on, the literature is ever expanding.

[158] E.g., A. Michael Froomkin, "The Death of Privacy?" (2000) 52 Stanford Law Review 1461 (discussing a range of technologies that threaten to undermine expectations of informational privacy including FRT, but refuting the notion that privacy is accordingly dead, instead highlighting ways in which individuals and the law can and continue to respond to protect privacy vis-à-vis commercial and state information collection); Zahra Takhshid, "Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort" (2020) 1 Buffalo Law Review 139 (calling for a Tort of Unwanted Broadcast to provide a remedy when one's picture/image is intentionally and widely broadcasted on social media without consent, in part called for given the ways in which such images can be used, including by or for training FRT – citing specifically to Clearview AI); and "Selinger & Hartzog, "Inconsentability", *supra* note 155.

[159] See e.g., Julie Carr Smyth, "States Push Back Against Use of Facial Recognition by Police" (May 5, 2021) ABC News online: < https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175>.

FRT throughout the US as well.[160] However, none of the restraints adopted in the US have so far addressed personal-uses of FRT either. I note FRT briefly here because of the implications this application has, especially when combined with drones or home surveillance architecture, to deepen and broaden privacy invasive personal uses of increasingly automated technologies in public space.

Conclusion

The main attributes of technologies like drones and home surveillance systems are instructive when considering interpersonal privacy in public space. These technologies make the surveillance of public spaces by individuals easier. Ring and similar systems in some ways expand what individuals could already do but likely would not, given the time investment (e.g., pervasively film, and share widely within the neighbourhood), and drones expand upon what individuals could do absent the technology by providing new angles and access to spaces.[161] Automation and corporate incentives make these technologies relatively cost accessible; automation makes the technologies simpler and more practical to use; connectivity between systems makes sharing and analyzing vast quantities of collected information more seamless; and their remotely-operated nature make them more useful for long term surveillance (e.g., Ring can perpetually monitor in front of a home) and/or less transparent and perhaps more discreet surveillance (e.g., a drone can operate high in the airspace, and far enough from its pilot that an individual cannot identify the human operator). These technological affordances build on those already available in public spaces (e.g., people taking pictures in public or using home surveillance are not new, but such activities are easier and more

[160] Early evidence suggests that facial recognition systems are being adapted to use on faces with masks, and since the beginning of the COVID-19 pandemic error rates associated with mask use have been declining. See e.g., Mei Ngan, Patrick Grother, and Kayee Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms" (November 2020) NISTIR 8331, available online: <https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report_6b.pdf>.
[161] Bracken-Roche, "Politics of Verticality," *supra* note 11.

extensive and sophisticated now). However, as the next chapter will show, despite the possibility of technology-mediated interpersonal privacy conflicts having existed for some time, tort law in Canada has not recognized a right to privacy in public space. The next chapter examines the statutory and case law addressing the application of the privacy torts in public spaces. The subsequent chapters argue that it is doctrinally inappropriate and substantively inequitable to deny privacy interests in public spaces, and these chapters consider how some of the nuances created by drones, home surveillance systems, and other remotely-operated technologies in public space might be considered within the scope of Canadian privacy tort law.

Chapter 3 – The Privacy Torts Currently Fail to Address Privacy Claims in Public Space

Having considered two technologies that currently engage privacy interests in public space, as well as the cautions and concerns of experts about further potential conflict, this chapter considers how the privacy torts might respond to such interpersonal conflicts. This chapter engages in a doctrinal analysis of the statutory and common law privacy torts across Canada. As there have not yet been any tort actions brought in response to drones, and relatively few in response to home surveillance systems, this chapter presents a largely hypothetical analysis of what the courts might say in response to technology-mediated public space privacy conflicts.

Generally speaking, with some exceptions, courts have been unwilling to apply the privacy torts to conduct occurring in public space or engaging publicly visible information. On the whole, the current privacy tort jurisprudence suggests that a person cannot reasonably expect privacy in public space. And without a reasonable expectation of privacy, one cannot claim their right to privacy has been infringed or that they have suffered compensable privacy harm. As I will argue further in Chapter 4, this seemingly all-or-nothing approach to privacy in public space - wherein, once someone is publicly visible, they can no longer expect any form of privacy - is a normative choice by the courts, which has a long historical trajectory, and is also increasingly criticized within academic writing. I will later argue that this is not the only choice available to courts in terms of how to understand the privacy torts in relation to public space privacy conflicts, including those mediated by technology. But the initial analysis in this chapter is more descriptive in nature, attempting to discern when and why tort might be or might not be a mechanism for addressing the types of privacy considerations raised in Chapters 1 and 2.

Before moving into the specific analysis of the provincial torts, it is worth noting some general themes about the privacy torts in the Canadian common law legal system. First, tort liability

for privacy-harm is determined provincially. Several provinces have enacted statutory torts. I will begin with an analysis of these statutory provisions and their interpretations by the courts. Courts in some other provinces have recognized common law privacy torts, which I focus on next. And some provinces have no statutory tort and have not yet recognized a common law tort, meaning individuals in those provinces would need to persuade their courts to recognize a new tort. The fact that common law torts exist in some provinces lends persuasive support to such recognition in other common law provinces. Further, professor Emily Laidlaw has argued that the absence of a privacy tort cause of action in a province presents an opportunity for that province to be more innovative in developing privacy statutory actions, should it choose to do so.[162] The Supreme Court of Canada (SCC) has not yet ruled on the common law torts, leaving it to trial and provincial appellate court judges to interpret the common law. However, the SCC has commented on B.C.'s statutory tort to say that courts should give the statutory tort provisions a "broad and generous" interpretation. The SCC has also made some pronouncements about the quasi-constitutionality and special importance of privacy in Canada that should be influential to the ongoing development of both common law and statutory torts. I examine these SCC pronouncements and what they can mean for tort law moving forward in the reform analysis later, in Chapter 6.

A second note about the torts, and the analysis below, is that most provinces understand privacy in tort law to include up to four types of harms (or in the case of Ontario, four distinct torts). This division of privacy torts into four categories stems from and loosely tracks the US jurisprudence, where "privacy torts" is an umbrella concept for four separate actions (compiled by Professor William Prosser, which I will refer to as the "Prosser Torts"):

---

[162] Emily Laidlaw, "The Future of the Tort of Privacy" (March 30, 2021) *The Canadian Bar Association National Magazine*, online: <https://www.nationalmagazine.ca/en-ca/articles/law/opinion/2021/the-future-of-the-tort-of-privacy>; see also Emily Laidlaw's forthcoming paper on the application of the privacy torts online (draft on record with author).

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[163]

In some jurisdictions these torts are not each treated as distinct actions but rather are partially subsumed within an action for "violation of privacy." For example, statutory claims for "violation of privacy" address not only surveillance or observation (intrusion upon seclusion type concerns), but also the subsequent use of private information (e.g., disclosure, and perhaps, false light). In other provinces, like Ontario, these are treated as distinct torts each with their own legal test and elements for the plaintiff to establish.

In this thesis, I have elected not to focus on the fourth tort listed above – appropriation of name or likeness. This tort addresses the commercial use of one's identity for profit. This tort goes beyond the scope of interpersonal privacy conflicts that I am specifically focused on here. Subsequent use of a person's image for commercial profit is certainly a concern that may become increasingly significant given the proliferation of personal use surveillance technologies. For instance, viral videos produced with Ring cameras are relevant to those who might be captured on video, however, the *commercial* profit dynamic of the subsequent dissemination of those images is beyond the scope of the thesis. Other scholars have persuasively argued that misappropriation of personality does not actually deal with *privacy* harms, but rather with *reputational* harms and commercial interests.[164] For the purposes of analytical clarity and space in this thesis, the below

[163] At para 18 in *Jones*, *supra* note 27, Justice Sharpe recognizes the four so called "Prosser Torts" (named for professor Prosser who identified these four threads in the U.S. tort jurisprudence in the 1960's, and which have been subsequently adopted across the U.S., and have informed both the statutory and common law torts in Canada). For the early categorization of these torts by see: William L Prosser, "Privacy" (1960) 48 California Law Review 383.
[164] See e.g., Ignacio Cofone and Adriana Roberston, "Privacy Harms" (2018) 69 Hastings Law Journal 1039-1098.

analysis focuses on the first three of the above four tort concepts, whether as standalone common law causes of action, or as aspects of a statutory tort claim.

Statutory Privacy Torts

The governments of British Columbia, Saskatchewan, Manitoba and Newfoundland have each enacted legislation providing a statutory cause of action in tort for violations of privacy.[165] Additionally, several provinces have enacted legislation dealing specifically with the non-consensual distribution of intimate images.[166] The statutory tort protections addressing "violations of privacy" are similar across the four provinces, with some nuances.[167] Each province has recognized a tort that is actionable without proof of damages (actionable *per se*).[168] In BC, Saskatchewan, and Newfoundland, a violation of privacy is actionable against someone who "wilfully" and "without claim of right" violates a plaintiff's privacy.[169] In other words, these are intentional torts. Perhaps notably, Manitoba's *Act* does not use the term "wilful," but instead makes it a tort to "substantially, unreasonably and without claim of right" violate the privacy of another person.[170] This could, as I discuss below, allow even greater interpretive flexibility to the courts when dealing with technology-mediated privacy intrusions (though to date, has not).

Each of the provincial statutes also provide some non-exhaustive examples of *prima facie* violations, as well as a number of defences to the tort (in the case of BC, these are described as

---

165 *Privacy Act*, R.S.B.C. 1979, c. 336 [BC *Privacy Act*]; *The Privacy Act*, R.S.S. 1978, c. P-24 [Saskatchewan *Privacy Act*]; *The Privacy Act*, R.S.M. 1987, c. P-125 [Manitoba *Privacy Act*]; and *Privacy Act*, R.S.N. 1990, c. P-22 [Newfoundland *Privacy Act*].
166 See Hilary Young and Emily Laidlaw, "Nonconsensual Disclosure of Intimate Images (NCDII) Tort" (August 2019) Uniform Law Conference of Canada, Newfoundland and Labrador, online: <https://ulcc-chlc.ca/ULCC/media/EN-Annual-Meetings/Nonconsensual-Disclosure-of-Intimate-Images-Images_1.pdf>.
167 This similarity is in part due to each province building on the preceding provincial statutes, as well as due to the Conference of Commissioners on the Uniformity of Laws. See e.g., L.R. MacTavish, "Uniformity of Legislation in Canada – An Outline" (1947) 25 Canadian Bar Review 36.
168 BC *Privacy Act*, s. 1(1); Saskatchewan *Privacy Act*, s. 2; Manitoba *Privacy Act*, s. 2(2); Newfoundland *Privacy Act* s. 3(1).
169 BC *Privacy Act*, s. 1(1); Saskatchewan *Privacy Act*, s. 2; Newfoundland *Privacy Act*, s. 3(1).
170 Manitoba *Privacy Act*, s. 2(1).

examples of conduct that is not considered a violation of privacy).[171] The *Privacy Act*s in Saskatchewan, Manitoba and Newfoundland specifically define available remedies, including that the court can award damages to a successful plaintiff, grant an injunction, order specific performance (namely, return of articles or documents), or other remedies as appropriate.[172] British Columbia, Saskatchewan, and Newfoundland specify considerations for a court to take into account when assessing whether there has been an invasion of privacy.[173] Manitoba does this as well but for the purposes of assessing damages.[174]

Notably, none of the statutes define "privacy" nor do the statutes provide a specific test for determining when there has been a privacy violation, beyond the non-exhaustive list of *prima facie* examples and considerations for the court.[175] Additionally, none of the statutes explicitly limit the application of the torts to private spaces. And in fact, the examples cited in the statutes of *prima facie* violations could be read to suggest that privacy torts may arise in public space; for instance, by stipulating that privacy can be violated by eavesdropping or surveillance, *regardless* of whether there is also a trespass,[176] leaves open the interpretation that private-property boundaries are not required for something to be considered 'private' under the statute.[177]

---

[171] Examples of *prima facie* violations are set out in s. 1(4) of the *BC Privacy Act*, s. 3 of the *Saskatchewan Privacy Act*; s. 3 of the Manitoba *Privacy Act*; and s. 4 of the Newfoundland *Privacy Act*. Exceptions (e.g., conduct not considered a violation of privacy) are set out at s. 2 of the *BC Privacy Act*. Defences are set out in s. 4(1) of the Saskatchewan *Privacy Act*; s. 5 of the Manitoba *Privacy Act*; and s. 5(1) of the Newfoundland *Privacy Act*.
[172] Saskatchewan *Privacy Act*, s. 7; Manitoba *Privacy Act*, s. 4(1); Newfoundland *Privacy Act,* s. 6(1) and s. 7.
[173] BC *Privacy Act*, s. 1(3); Saskatchewan *Privacy Act*, s. 6(1); Newfoundland *Privacy Act*, s. 3(2).
[174] Manitoba *Privacy Act*, s. 4(2).
[175] In the debates preceding the adoption of the Saskatchewan *Privacy Act*, there is a discussion about the absence of a definition of privacy, with the accompanying explanation that there was a concern that any definition might be "indefinite or somewhat general", and thus discretion is left to the courts. The Legislative Assembly of Saskatchewan, Thursday March 21, 1974, at 1685.
[176] BC *Privacy Act* s. 1(4); Saskatchewan and *Manitoba Privacy Acts*, s. 3(a); Newfoundland *Privacy Act*, s. 4(a).
[177] Of course, this is but one of the possible interpretations of this statutory wording. It could also be interpreted to mean that surveillance of a private space through, for instance technology that can sit outside the property, is still a violation. Arguably though, these are not mutually exclusive interpretations. The courts have not resolved this particular question, to date.

However, as the below analysis will show, the BC courts have explicitly tended away from an interpretation of the statutory torts that would recognize privacy harms in public space. Manitoba and Newfoundland have relatively little jurisprudence dealing with public space conduct, so it is not yet definitive how the courts in those provinces would approach privacy in public space. In Saskatchewan, one appellate court decision suggests a broader interpretation of that provincial tort could be possible, compared to BC. Generally speaking, if the courts do not recognize the application of the statutory torts in public, then seemingly no plaintiff experiencing privacy harm from interpersonal, technology-mediated, conduct in public space could seek recourse through these statutory torts. This has not been definitively determined by the courts, but the jurisprudence to date leans (I will argue, problematically) in this direction.

A Brief Note on Legislative History

It is unsurprising that the provincial statutory torts share many attributes in common, including many instances of identical phrasing. The provinces sequentially built on one another's developments. BC was the first province to adopt a provincial statutory privacy tort, and in fact led the Commonwealth countries in doing so in 1968.[178] The BC tort was adopted before the province recorded a Hansard, but drawing from secondary sources, it appears that the *Act* was developed in response to growing concerns about technology-mediated surveillance and eavesdropping.[179] The original discussions about the BC *Privacy Act* were centered on civil liberties and curbing the impact of surveillance.[180] However, political critique was levelled against the *Act* even soon after its adoption

[178] See e.g., Nancy Brown, "Detective Invaded Privacy" The Daily Colonist, Victoria BC, Saturday December 13, 1969 page 1 (available through online archive: <www.britishcolonist.ca>); British Columbia Law Institute, *Report on The Privacy Act of British Columbia* (February 2008), BCLI Report No. 49, online: <http://www.bcli.org/sites/default/files/Privacy_Act_Report_Website.pdf> [BCLI, *Report on the Privacy Act*].
[179] BCLI, *Report on the Privacy Act*, at 1-4.
[180] For instance, when the Act was introduced as a Bill in its first reading, the Attorney General was quoted as saying, in regards to the objectives of the Act, that it "may do a good deal to forestall Big Brother in 1984", among other references to curbing intrusive and unwanted surveillance. See BCLI, *Report on the Privacy Act*, at 4.

for being relatively "toothless" in responding to such conduct.[181] Its initial conception though certainly signals or suggests an intent to address pervasive forms of technology-mediated surveillance.

Secondary sources have not explicitly addressed if the BC *Privacy Act* was specifically modelled off of the US tort doctrine.[182] The Attorney General of BC at the time referred to the *Act* as "novel" and "revolutionary."[183] Nevertheless, early court decisions certainly interpreted the *Act* with explicit reference to the US tort law, and relied on the four Prosser torts in doing so.[184] The provincial statutes that followed drew on BC's example and thus adopted similar provisions into their respective provincial protections as well.

Manitoba followed BC's lead, adopting its *Privacy Act* in 1970, similarly prompted by concerns about technology-mediated surveillance. However, there was particular concern in the debates about state-led surveillance, which makes some sense given the *Charter* protections against unreasonable searches had not yet been adopted.[185] Saskatchewan adopted its Act in 1974, and based it "largely on the *Privacy Acts* … in existence in British Columbia and Manitoba."[186] The preceding debates again centered around addressing the concerns of emerging surveillance technologies, and, as in the other provinces, filling a gap in the common law where privacy was not directly

---

[181] Newspaper columns for example convey concerns from politicians about the *Act* being "toothless" and having been interpreted too narrowly by the courts. For example, Alex Macdonald (NDP Vancouver East) said this after it was revealed that Judge Bernard Isman had been followed by a private detective. "Laws Trample on Privacy" *Daily Colonist*, Victoria BC Saturday January 30, 1971 page 8 (available through online archive: www.britishcolonist.ca).
[182] At least one academic author has referred to the US doctrinal influence in the development of the *BC Privacy Act*, see e.g., John D McCamus, "The Protection of Privacy: The Judicial Role" in Rosalie Abella and Melvin Rothman (eds) *Justice Beyond Orwell* (Éditions Y. Blais, Montreal: 1986).
[183] BCLI, *Report on the Privacy Act*, at 4, citing to "New Bill to protect privacy," The Province (26 January 1968), in British Columbia, Legislative Assembly, Sessional Clipping Books: Newspaper Accounts of the Debates (microform).
[184] See e.g., *Davis v McArthur* (1969), 10 DLR (3d) 250 (BCSC); rev'd 17 DLR (3d) 760 (BCCA) – the first case heard under the BC *Privacy Act*, involving a husband suing a private investigator who was hired by the plaintiff's wife to collect information about him for their divorce proceedings. Both the trial judge and appellate court drew heavily on the US conceptualization of privacy torts to interpret the *Act*.
[185] See e.g., The Legislative Assembly of Manitoba, Thursday May 14, 1970, 8:00am, at 1964-1968; The Legislative Assembly of Manitoba, Thursday June 18, 1970, 2:30pm, at 2957-2958.
[186] The Legislative Assembly of Saskatchewan, Thursday March 21, 1974, at 1684-85.

protected.[187] Finally, Newfoundland adopted its legislation in 1981, with similar concerns in mind about technology-facilitated surveillance and the gaps in the common law to address this.[188] In all four provinces, unwanted surveillance, particularly that mediated by surreptitious audio and video recording technologies, was a concern that prompted the adoption of the statutes. While the governments each recognized that in some instances of surveillance, like CCTV inside a store, might be permissible, this assessment had to be context dependent. For instance, in debates in Manitoba, the Attorney General clarified that while CCTV in a shop might not come within the scope of the tort, CCTV cameras in a changeroom or bathroom certainly would.[189] It is for the courts to assess this context; though this should be done with awareness of the original legislative intent to address unwanted surveillance.[190] I did not read any discussions in the parliamentary debates that specified that the torts should not apply in public spaces; and in fact, there were several references specifically to concerns about long-term monitoring that would engage a person's conduct in public space and that the *Privacy Acts* were intended to address and prevent.[191]

Building on the origins of these *Acts* from concerns around technology-based surveillance and associated loss of individual privacy, the following subsections consider in more detail whether the statutory torts would or could be called upon to address technology-mediated interpersonal privacy intrusions in public spaces – for instance where a drone is used to collect images, or to invade personal space, or where a Ring or similar device captures images of a person's daily movements through a neighbourhood, or where those images are subsequently shared on neighbourhood discussion boards. For the purpose of this analysis, I focus specifically on the

---

[187] *Ibid.*
[188] At 3159-61.
[189] The Legislative Assembly of Manitoba, Thursday May 14, 1970, 8:00am, at 1968.
[190] See e.g., Ruth Sullivan, "Statutory Interpretation in a Nutshell" (2003) 82 Canadian Bar Review 51-82 at 61-62.
[191] For instance, this was what prompted B.C. to adopt legislation (e.g., BCLI, *Report on the Privacy Act*, at 1-4), and arose again in for instance Manitoba's debates (The Legislative Assembly of Manitoba, Thursday May 14, 1970, 8:00am, at 1964).

substantive privacy issue, taking for granted that an individual plaintiff knows that information about them has been collected or shared, and that the plaintiff is able to identify the defendant. In particular in the case of a drone encounter, due to the remoteness of the device from an identifiable operator, identity of the operator might be difficult or impossible to ascertain in practice, which presents an additional access to justice barrier for the plaintiff.[192]

British Columbia

Of the four common law provinces with statutory privacy torts, British Columbia's statute has received by far the most judicial consideration.[193] Accordingly, I begin with a consideration of what BC's statute, and cases decided under it, say about technology-mediated intrusions in public space.

Like the other statutes, BC's *Privacy Act* stipulates that: it is a tort for a person to *wilfully* and *without claim of right* violate the *privacy* of another.[194] Whether a violation has taken place is assessed through a two-step analysis: was the plaintiff entitled to privacy and, if so, did the defendant breach the plaintiff's privacy?[195] I examine what the courts have said about each of these italicized elements below, and what these would mean in a public space privacy conflict.[196]

---

[192] I discuss this issue further in a law review article, Thomasen, "Beyond Airspace Safety", *supra* note 4.
[193] In addition to the discussion in this section, the courts have affirmed that: the tort is *in personam*, it cannot be brought on someone else's behalf (*Facilities Subsector Bargaining Association v British Columbia Nurses' Union*, 2009 BCSC 1562 (CanLII)); and that a corporation can be sued for having invaded privacy - the word "person" in s. 1(1) is not defined, and where the term is used without express qualification it can include a corporation (*Madco Investments Ltd. v Western Tank & Lining Ltd.*, 2017 BCSC 219 at para 69 referring to *Interpretation Act*, RSBC 1996, c. 238));
[194] *BC Privacy Act*, s1(1).
[195] See *Getejanc v Brentwood College Assn.* (2001), 6 CCLT (3d) 261, 2001 BCSC 822 (CanLII) at para. 16.
[196] The courts in BC have said that there is no additional, co-existing common law tort of invasion of privacy available in the province, however the BCCA recently called this into question leaving open the door for a claim under a common law cause of action (see the Ontario discussion for more detail on other common law privacy torts): *Tucci v Peoples Trust Company*, 2020 BCCA 246. But see: *Hung v Gardiner*, 2002 BCSC 1234 (CanLII) (affirmed 2003 BCCA 257 (CanLII)) at para. 110; *Bracken v Vancouver Police Board*, 2006 BCSC 189 (CanLII) at para. 28; *Demcak v Vo*, 2013 BCSC 899 (CanLII) *Mohl v University of British Columbia*, 2009 BCCA 249 (CanLII) at para. 13; *Turkson v TD Direct Investing, A Division of TD Waterhouse Canada Inc.*, 2016 BCSC 732 (CanLII) at para. 180, aff'd 2017 BCCA 147 (CanLII); and *Tucci v Peoples Trust Company*, 2017 BCSC 1525 (CanLII) at para. 49; *Ari v Insurance Corporation of British Columbia*, 2015 BCCA 468 (CanLII) at para. 8.

Ultimately, the tort as it is currently interpreted is not likely to be helpful in resolving or vindicating public space privacy conflicts. The BC courts have rejected claims of privacy violations occurring in public or publicly-visible space on the basis that a plaintiff cannot reasonably expect privacy when publicly visible. Where increasingly remote and automated systems are mediating such conflict, the "wilfulness" requirement of this tort might also be complicated for a plaintiff to prove. Additionally, while the tort does address wilful and non-consensual sharing of personal information, given the BC courts' current conceptualization of public space as a place with little or no privacy, the sharing of information collected from public space might also not be captured by this tort. I review each element of the tort in turn below.

Wilful Violation

Wilfulness is the first element in the BC statutory tort. In *Hollinsworth v BCTV*, Lambert J interpreted the element "wilful" to mean acting in a way that is intentionally privacy invasive:

> […] the word "wilfully" does not apply broadly to any intentional act that has the effect of violating privacy but more narrowly to an intention to do an act which the person doing the act knew or should have known would violate the privacy of another person.[197]

It is not enough that the defendant's conduct is intentional. Their conduct has to intentionally, and not incidentally or accidentally, violate the plaintiff's privacy.[198] Lambert J did include an objective component to this analysis, such that an act that a person "should have known

[197] *Hollinsworth v BCTV, A Division of Westcom TV. Group Ltd.*, [1998] BCJ No. 2451(BCCA) at para 29 [*Hollinsworth*].
[198] It has to be more intentional than an honest mistake: *St. Pierre v Pacific Newspaper Group Inc. and Skulsky*, 2006 BCSC 241 (Plaintiff unsuccessfully claimed a breach of privacy when defendant mistakenly published his picture in a story about terrorism; the court found it was an honest mistake on the part of the newspaper at paras 50-53). But, in *Bracken v Vancouver Police Board et al.*, 2006 BCSC 189 at paras 56-57 the court clarified that an honest mistake *as to the application of the law* does not allow the defendant to claim the violation was not "wilful". The defendant needs to show on the facts that he did not believe privacy would be violated, rather than that he mistakenly believed he had a legal authority to violate another's privacy.

would violate the privacy of another person" could meet the wilfulness requirement. However, appellate courts have recently questioned whether to maintain this objective component.

Hunter JA recently discussed Lambert J's interpretation of the "wilful" element in *Duncan v Lessing*.[199] After highlighting that Lambert J did not give any citation for his definition of "wilfully" (and calling the basis for this original framing into question), Hunter JA went on to explain that the "inclusion of the objective standard "should have known" may not capture the deliberateness that is implicit in the word "wilfully""[200]:

> The term "wilfully" appears in many statutes and is usually defined as meaning deliberately, intentionally or purposefully. It is not necessary for the purposes of this appeal to define with precision the definition of the term, but it can be said with some confidence that "wilfully" does not mean accidentally.[201]

Reading these together, a defendant's conduct would only meet the wilful requirement when it intentionally, deliberately, or purposefully violates another's privacy. The courts in BC appear to be tightening this requirement, making it harder for plaintiffs to establish. This requirement serves to limit the tort's application to specifically intentional and not negligent or careless acts of surveillance, which provides an important limit on the scope of potential liability under the *Act*. It also incidentally creates some balance against any potential concern that recognizing privacy in public space would lead to over-litigation of, or a chilling effect on, activities that might result in incidental information collection (e.g., taking a group photograph with third parties incidentally visible in the background. Depending on the context, those third parties could generally not successfully sue for violation of their privacy, as taking their image was not wilful).

Seemingly, using a device for the intended purpose of collecting information or invading someone's personal space should meet this element of the tort. A remote-system that incidentally

---

[199] *Duncan v Lessing*, 2018 BCCA 9.
[200] *Duncan v Lessing, ibid* at para 84.
[201] *Duncan v Lessing, ibid* at para 86.

collects footage or information in the context of an operation that is conducted for another purpose may not meet the requirements of this tort. Where a drone, for instance, is used to intentionally gain access to images of a person in a public space, the wilful requirement should be theoretically met. However, proving this level of intent might be particularly challenging given the remote nature of the technology. For instance, the court might be asked to determine whether a defendant operated a drone in a particular public space to capture images of the plaintiff, or whether the plaintiff simply happened to be present and visible. The plaintiff may need to persuade the court of technicalities that could be hard to prove, e.g., whether the defendant could see the plaintiff through the drone payloads *before* engaging in filming, *etc*. Incidents like stalking, harassment, and sexual/voyeuristic filming, should be more straightforwardly caught within this element, and may be established through the drone's own footage, though even such video evidence is not infallible for the plaintiff and depends on a judge's interpretation of the interaction.[202]

Purportedly, establishing a home surveillance system to specifically capture video of the ongoings in front of a home or property should come within the wilfulness requirement – the camera is in place to intentionally collect such footage. Other cases in BC involving the use of security cameras to surveil a specific property have not been contentious in terms of the wilfulness requirement.[203] But, courts in other contexts have held that information collected by a video is not

---

[202] As Alexa Dodge has shown in the context of sexual assault and harassment criminal prosecutions: Alexa Dodge, "The digital witness: The role of digital evidence in criminal justice responses to sexual violence" (2017) Feminist Theory 1.

[203] See e.g., *Wasserman v Hall*, 2009 BCSC 1318. However, given the homeowner's distance from the camera at the time of collection (both physical, but also in the sense of not overseeing its functioning and making decisions about what information to collect), courts may be faced with counter-arguments by defendants who claim they never intended to capture whatever specific activity might occur in front of their home (e.g., they didn't mean to film *that* plaintiff, or *that* occurrence). Defendants have delegated filming and information collection to the device. Such delegation of human conduct to a machine could lead judicial decision-makers to view the human defendant as less legally or morally culpable: See e.g., Jason Millar and Ian Kerr, "Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots" in Ryan Calo, Michael Froomkin, Ian Kerr (eds) Robot Law (Cheltenham, UK: Edward Elgar Publishing, 2016). However, in instances like use of Amazon Ring, this should not impede a claim, as the whole purpose for installing the device is to capture footage of others. In privacy cases involving Ring, intent has not been as issue for the plaintiff (other elements of the tort have presented different challenges): see *Zeliony*, *supra* note 17.

really 'collected' until it has been viewed by a human – overlooking the ways in which the awareness of a technological gaze can affect those under surveillance.[204] In most analogous cases, this element has not presented the greatest challenge to the plaintiff, but it is notable that some particular kinds of arguments could arise that would make a privacy claim more practically complicated.

Wilfulness in a Subsequent Disclosure

The creation of an easily shared record through technology-based surveillance raises the further legal question of whether the privacy torts can address harms associated with subsequent sharing of information about a plaintiff. The example of the Ring home security system in particular highlights this concern, as such sharing is specifically streamlined and advertised in connection with a Ring system. As noted, a marketed feature of the Ring system is that the ability to share images with neighbours and law enforcement is a part of Ring's claim to make homes and neighbourhoods safer. Similar concerns can of course apply to drones, as has been exemplified in recent incidents where footage collected by drones has been non-consensually shared online.[205]

Section 1(1) of the BC *Privacy Act* has been interpreted to apply to non-consensual sharing or disclosure of a plaintiff's private information. In terms of the wilfulness requirement in the disclosure of someone else's information, the courts will assess whether the defendant intended to violate the plaintiff's privacy in the act of disclosing the impugned information (a similar analysis to

---

[204] Ian Kerr, "Schrödinger's Robot: Privacy in Uncertain States" (2019) 20 Theoretical Inquiries in Law 1 [Kerr, "Shrödinger's Robot"] (arguing that privacy can be violated by robotic/AI-based observation and analysis even without direct human involvement or intervention).

[205] A startling example is that of Brian Bates in Oklahoma City who uses a drone to collect images of sex workers while working, including in public spaces, and uploads those images online. He self-describes as the "drone vigilante" and has shared video with law enforcement leading to criminal charges and convictions against sex workers. He used to do the same using his cell phone camera, but has noted "it was safer to use a drone than walk up to the vehicle." He also claims that he does not violate the law in the way he uses his drones, even when he was asked specifically about privacy in an interview with Vice News reporter Jordan Pearson: Jordan Pearson, "Meet the 'Drone Vigilante' who Spies on Sex Workers" (April 4, 2016) Vice News, online: <https://www.vice.com/en/article/kb7zga/drone-vigilante-brian-bates-johntv-oklahoma-spies-on-sex-workers>.

that noted above for the collection of information). For instance, in *Bracken v Vancouver Police Board et al,*[206] the plaintiff sued for a violation of privacy after a government agency disclosed the plaintiff's home address to the Vancouver police upon their request. The court found that this disclosure met the wilfulness element, as Ms. Bracken's personal information was requested (and then disclosed) intentionally and knowing it would violate her privacy.[207] Ultimately the plaintiff's claim failed though, because the disclosure was authorized by law.

The courts have also interpreted the wilfulness threshold in the context of disclosure to be fairly high. A reasonable oversight or mistaken belief leading to a disclosure can satisfy the court that a defendant did not intend to invade privacy and thus was not wilful. For example, *Hollinsworth* involved disclosure of video of the plaintiff on the evening news. Mr. Hollinsworth's claim failed on account of the defendant's mistaken but honest belief that the defendant had permission from Mr. Hollinsworth to disclose the video. The defendant thus did not intend to violate the plaintiff's privacy.[208] In the BCCA's decision, it was also relevant that, because the defendant had an honest and reasonable belief that they had Mr. Hollinsworth's permission to disclose, the "without claim of right" element was also not met.[209] This element is discussed further below, but it is notable here that the elements in the s. 1(1) tort have been interpreted to work together in the court's analysis. Where the defendant reasonably believes she has a claim of right to reveal information, then she might also not be wilful in her violation of the plaintiff's privacy. This may also be pertinent in cases where the plaintiff's information was collected from public space, such that the defendant believes she is not violating privacy by sharing the information because the plaintiff has shared that information already with the general public.[210]

---

[206] *Bracken v Vancouver Police Board et al*, 2006 BCSC 189 (CanLII) [*Bracken*].
[207] *Bracken, ibid* at paras 55-57.
[208] *Hollinsworth v BCTV, supra* note 197 at para 29.
[209] *Hollinsworth v BCTV, ibid* at paras 30-31.
[210] As I discuss further, the courts in BC have determined that it is not a violation of privacy to collect information that is publicly visible (e.g., to film someone who is in a public place), because that person cannot expect privacy in that

In *St. Pierre v Pacific Newspaper Group* the defendant newspaper reprinted a photograph of the plaintiff with a caption suggesting the plaintiff was a terrorist. While the plaintiff had earlier consented to the picture being taken, the court found he clearly had not implicitly consented to this subsequent publication.[211] But the violation in this case was still considered not to be wilful – the court found the disclosure occurred due to a reasonable oversight when the newspaper mistakenly used the plaintiff's image; the defendant did not intend to violate the plaintiff's privacy.[212]

Accordingly, a plaintiff who seeks to vindicate an unwanted disclosure or sharing of their information with others may turn to s. 1(1) to ground a claim. They will have to show that the defendant intended to violate their privacy by disclosing their information. Wilfulness limits the scope of the tort such that, for instance, sharing an image on a social media platform that shows third parties in the background may not fall within the scope of the tort, as there may be no intention to violate the privacy of third parties.[213] However, the disclosure of an image collected by, for instance, a Ring camera with the intention of singling out an individual as suspicious or concerning would seem to meet the wilfulness threshold, particularly where the sharing is connected to negatively opining about the person. More contentious cases will arise where a surveillance system itself automatically shares an image. For instance, a hypothetical case where Ring or a similar system automatically analyzes footage to identify individuals who frequent an area to create "watch lists" or

---

place. I note here that these elements can work together in ways that might complicate a plaintiff's case, for instance where there is no wilfulness to invade privacy because the defendant assumed the plaintiff had no privacy to violate, the subsequent sharing of that information might also fall outside the scope of wilfulness.

[211] Defamation could of course also be a live issue in a situation like this, depending on the circumstances (it was in *St. Pierre* as well).

[212] *St. Pierre v Pacific Newspaper Group Inc. and Skulsky*, 2006 BCSC 241 (CanLII) at para 45.

[213] Such an interpretation would be in line with what the Supreme Court of Canada has said in the Quebec legal context with regard to images of third parties in the background of a photograph: *Aubry, supra* note 50 (involving a claim for violation of privacy under the Quebec *Charter of Human Rights and Freedoms* s. 5 after a magazine printed a photo featuring the showing the plaintiff sitting on the steps of a building in a public place. The Court held that the right to privacy includes the right to control the use made of one's image, and thus there can be liability when a photo is published without consent and where the person can be identified).

flag suspicious activity would engage these considerations.[214] As noted above though, the courts have read the elements of s. 1(1) together such that a defendant home owner may claim they were not wilful in violating the plaintiff's privacy because there was no privacy to violate, given the plaintiff's location in a public space. This argument may engage the second or third elements of the tort, which are discussed further below.

Claim of Right

The second element of the BC statutory tort requires that the defendant be acting "without claim of right." A "claim of right" under s. 1 has been interpreted to mean an honest belief on the part of the defendant that she had a legal justification or excuse for her privacy-engaging action.[215] Such a belief justifies their conduct and renders it non-tortious. There are various ways in which this element may be engaged in technology-mediated privacy disputes, relating to how and why the technology is being adopted.

For instance, a defendant might argue that having Transport Canada permission to fly a drone, or operating within the scope of the Transport Canada rules amounts to a legal justification for particular drone use, and perhaps filming. This argument has arisen in the US context where an individual claimed he was not invading another's privacy because he was flying within the Federal Aviation Administration rules, however that claim was never settled by the courts.[216] If a BC court accepts such an argument, then many occasions where privacy is seemingly engaged in public space might fail to meet the second element of this statutory tort. However, such an argument ought to

---

[214] The Intercept reported that Amazon had such plans after reviewing internal Amazon documents: Sam Biddle, "Amazon's Ring Planned Neighbourhood "Watch Lists" Built on Facial Recognition" (November 26, 2019) The Intercept, online: <https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/>.
[215] *Hollinsworth, supra* note 197 at para 30. If the image is used in the context of neighbourhood discussion or gossip, it would not fall within the ambit of this section. The plaintiff would have to argue that sharing in this way amounted to a violation of privacy under s. 1 of the *Act*.
[216] See e.g., *Boggs v Meredith*, *supra* note 3.

be rejected. The Transport Canada regulations do not specifically address filming or privacy so should not be understood to permit violations of privacy. On the other hand, a defendant who is provided with and encouraged to use a Ring device by law enforcement could potentially argue for a claim of right on the basis of participating in a law enforcement program. Though, notably, claim of right allows for a mistake of fact but not a mistake of law so a mistaken claim that this course of events creates legal permission should not be accepted.[217]

Further though, a defendant who installs a home security system like Ring in response to theft or property damage might claim the legal right to protect the home – an argument like this has succeeded under the Manitoba privacy statute (discussed and critiqued below). Nevertheless, in the context of the technologies examined here, this element (like wilfulness above) might ultimately be resolved for the defendant on the basis that the privacy conflict engages conduct in public space. A defendant might argue a claim of right to operate in public space, through reliance on technology-specific laws and regulations, or through a broader entitlement to engage in such technology-mediated public space conduct (e.g., protecting a home from the outside world; engaging in expressive conduct in a public space; *etc.*). The third and final element of the tort may prove to be the most significant to the sorts of privacy conflicts examined in this thesis.

Violation of Privacy

The final element of the s. 1(1) tort – violating another's privacy – has received the most judicial interpretation of the three elements. Like the other provincial statutes, BC's *Privacy Act* does not define 'privacy'. It leaves considerable discretion to courts to determine whether a plaintiff can expect privacy in a given situation, stating that "the nature and degree of privacy to which a person

[217] *Bracken v Vancouver Police Board et al*, 2006 BCSC 189 (CanLII).

is entitled in a situation or in relation to a matter is that which is *reasonable* in the circumstances, giving due regard to the lawful interests of others."[218] And, when the court is determining whether a defendant's conduct is a violation of another person's privacy, the court should give regard to the "nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties."[219]

Nothing in the BC *Privacy Act* explicitly excludes the possibility of privacy in public space. But since the earliest claims arising under it, the courts have interpreted the *Act* in this way. The BC courts adopted dictionary definitions of "privacy" to facilitate the early analysis of whether a plaintiff had privacy in a given situation (only where the plaintiff is found to have privacy will the court then go on to consider whether the plaintiff violated that privacy). These dictionary definitions focus on notions of *seclusion* and *withdrawal* from society, public interest, or scrutiny; as well as the right to be left alone and freedom from unwanted publicity. For example, in the first case decided under the statute, *Davis v McArthur*, the trial judge Seaton J. drew upon definitions from US case law and the *Oxford English Dictionary* that defined privacy as "[t]he state or condition of being withdrawn from the society of others, or from public interest; seclusion."[220] On appeal of that decision, the BC Court of Appeal adopted a definition of privacy from Black's Law Dictionary, 4th ed.:

> The right to be let alone, the right of a person to be free from unwarranted publicity…The right of an individual (or corporation) to withhold himself and his property from public scrutiny, if he so chooses.[221]

While it is imaginable that one could seek to be left alone or free from publicity and public focus while in public spaces, the courts have tended away from recognizing such privacy

---

[218] BC *Privacy Act,* s. 1(2), emphasis added.
[219] BC *Privacy Act*, s. 1(3).
[220] *Davis v McArthur* (1969), 1969 CanLII 757 (BCSC), 10 DLR (3d) 250, 72 WWR 69 (BCSC).
[221] *Davis v McArthur* (1970), 1970 CanLII 813 (BCCA), 17 DLR (3d) 760, [1971] 2 WWR 142 (BCCA).

expectations as reasonable (and thus compensable) under the BC *Privacy Act*. There are relatively few decisions from BC that consider the application of the statutory tort in public spaces, compared to decisions dealing with conduct in private spaces or concealed/secluded matters. However, the majority of these decisions have held that the public or publicly visible location of an alleged violation undermines any reasonable privacy interest the plaintiff might claim to have.[222] In other words, the courts have said that a plaintiff cannot reasonably expect privacy in public. By contrast, acts like peeping into highly private spaces like bathrooms and bedrooms have resulted in not only compensatory, but also punitive damages against defendants.[223]

For example, in *Silber v British Columbia Television Broadcasting System Ltd*,[224] the plaintiff alleged that the defendants violated his privacy when they filmed an altercation between the plaintiff and a reporter on the plaintiff's business parking lot. The court determined that the location where the filming took place was the "salient feature" in assessing whether the plaintiff had any privacy interest.[225] The parking lot was visible to the public, in a busy neighbourhood. And while Mr. Silber had a property right to exclude trespassers from the premises, the court noted that the character of

---

[222] *Milner v Manufacturers Life Insurance Company,* 2005 BCSC 1661 (no expectation of privacy vis-à-vis private investigators taking photographs and videos of the plaintiff in her home but visible from the street, and of her children on the front lawn) [*Milner*]; *Silber v British Columbia Television Broadcasting System Ltd.* (1985), 25 D.L.R. (4th) 345 (BCSC) (no expectation of privacy in the filming of an altercation taking place on a business parking lot that was visible and accessible to any member of the public); *Milton v Savinkoff* (1993), 18 CCLT (2d) 288 (BCSC) (no violation of privacy in the dissemination of intimate photographs accidentally left by the plaintiff in the pocket of the defendant's coat – though the outcome in this case has been criticized); *Harding (Re)*, 2014 LSBC 29 (photographs taken at a facility that is publicly accessible and under video surveillance does not breach the provisions of the *BC Privacy Act*). With respect to public information, see: *Niemela v Malamas*, 2015 BCSC 1024 (no expectation of privacy permitting injunction against online posts about one's business, as work is "in general a public aspect of a person's life" (para 45)); *Fouad v Wijayanayagam*, 2015 BCCA 272 (seeking public information is not a violation of the *BC Privacy Act,* even if one's motivation for seeking the information is nefarious), but see *Griffin v Sullivan*, 2008 BCSC 827 (CanLII) (invasion of privacy to reveal personally identifying information connecting plaintiff to his anonymous and sensitive publicly visible online posts).

[223] *L.A.M. v J.E.L.I.*, 2008 BCSC 1147 paras 41-42 (determining that video surveillance of a bathroom is even more invasive because defendant can keep a permanent copy of the footage and can continue the invasion by revisiting the tapes. The court awarded punitive damages of $35,000 in addition to compensatory damages); *T.K.L. v T.M.P.*, 2016 BCSC 789 ($25,000 in aggravated damages for covert filming plaintiff in the bathroom, for a total of $85,000 in damages). See also *Lee v Jacobson* (1992), 87 DLR (4th) 401 (BCSC) reversed (1994), 120 DLR (4th) 155 (BCCA) but reasoning reaffirmed in *Malcolm v Fleming*, [2000] BCJ No 2400 (SC).

[224] *Silber*, *supra* note 222.

[225] *Silber, ibid* at para 17.

the property was much like a public place. Therefore, the court determined that the plaintiff could not expect privacy in that location.[226] In this case, just being publicly visible was enough to undermine any reasonable expectation of privacy (and thus any tort compensation) vis-à-vis unwanted filming.

Relying on *Silber* and other decisions, the BC Supreme Court re-affirmed in *Milner v Manufacturers Life Insurance Company* that the location of an impugned violation of the *Privacy Act* was "key" to the determination of whether the plaintiff had a privacy interest.[227] In *Milner*, the defendant insurance company hired private investigators to take photos and videos of Ms. Milner, who was on disability leave from her workplace. The investigator was hired to determine if Ms. Milner was or was not entitled to insurance coverage for her leave (i.e., whether she was making a valid claim). Ms. Milner did not raise arguments regarding photos of her in public places, and so that was not considered in the decision. The court had to assess whether photographs of Ms. Milner and her daughter in her house, and photographs of her children on her front lawn when she was not present, taken by private investigators parked on a public street, violated her privacy under the BC *Privacy Act*.

While the *Act* instructs courts to assess a plaintiff's privacy interest 'in all the circumstances', in this case the court again relied predominantly on one circumstance - public location/visibility. The plaintiff had no privacy interest with respect to the video surveillance of her in her home, because anybody walking by could have also seen into the home, and she ought to have known there could be video surveillance from an investigation.[228] Similarly, her sons had no expectation of privacy on the front lawn because they were in a publicly visible place. Ms. Milner's daughter who

---

[226] Citing to Laskin CJC's dissent in *Harrison v Carswell*, [1976] 2 SCR 200 at 207-208, in which Laskin CJC states that property like a shopping center – while privately owned – is much closer in character to public roads and sidewalks than it is to a private dwelling.
[227] *Milner, supra* note 222.
[228] *Milner, supra* note 222 at paras 83-85.

was also caught on video surveillance inside the home did, however, have an expectation of privacy which was violated by the surveillance, on the basis she was not under investigation and in particular because the video included footage of her removing her shirt. However, Ms. Milner's daughter was not a party to the action so no damages were awarded.[229] Notably again, the fact of being publicly visible – even when in a private space – was considered enough to undermine any reasonable expectation of privacy for Ms. Milner. This decision does not consider the impact of ongoing surveillance on a whole family, and takes as a given that when an individual makes a workplace disability insurance claim, they give up any expectation of privacy in public or publicly visible space.

In *Wasserman v Hall*[230] the court again turned to the publicly visible nature/location of an impugned privacy violation to determine whether a defendant's conduct was tortious under the BC *Privacy Act*. This case involved neighbours with a variety of disputes, one of which was Mr. Wasserman photographing the Halls in their backyard and aiming a surveillance camera at their home. In considering the provisions of the BC *Privacy Act*, and reaffirming the decision in *Milner*, the court said, "it seems obvious that a person's reasonable expectation of privacy in his or her own home is ordinarily very high whereas surveillance in a public place would be substantially less so."[231] The court accordingly determined that the Halls had no reasonable expectation of privacy "when working on or in the immediate area of the fence line but did, at all times, have a reasonable expectation of privacy when inside their own home."[232] No special attention was paid to the fact that through the use of a surveillance camera, a permanent recording of the Halls was created.

A similar set of facts (but less detailed analysis) arose in *Azak v Chisholm*[233] involving various claims arising from a dispute between neighbours. The privacy claim arose from an allegation that

---

[229] *Milner, ibid* at para 94.
[230] *Wasserman v Hall,* 2009 BCSC 1318 [*Wasserman*] (NB *Wasserman* only refers to *Heckert*, below, in regard to damages)
[231] *Wasserman, ibid* at para 75.
[232] *Wasserman, ibid* at para 77.
[233] *Azak v Chisholm*, 2018 BCSC 1051 [*Azak*].

the defendant installed video surveillance cameras that were directed at the plaintiff's property and interfered with his family's use and enjoyment of the property. The plaintiff and his wife testified that they always worried whether they were being watched or taped. The court accepted the defendant's evidence that the cameras were installed to prevent theft and not aimed at the plaintiff's property, or if they had been, it was a small part of the front parking area, and if the plaintiff was concerned with the cameras, he would have said something sooner.[234]

By contrast, in *Heckert*[235] the court determined that the defendant had violated the plaintiff's privacy when the defendant conducted surveillance of an apartment hallway. The landlord defendant placed a video camera in the communal hallway directed in a manner to particularly capture anyone entering and exiting Ms. Heckert's apartment. The BCSC determined that Ms. Heckert had a right to be left alone upon entering and exiting her apartment.[236] Even though the court considered the hallway to be public, Ms. Heckert was entitled to "be free from the scrutiny of a surveillance camera recording her every movement in and out of her suite especially where the positioning of the camera allows the person watching the video a view that is disturbingly intrusive."[237]

The court in *Heckert* considered the import of location on privacy expectations, and noted that the determination of a privacy interest cannot depend *solely* on the location of the impugned act. The court reasoned that, because a number of decisions including *Silber* and *Milner* in BC (*Wasserman* had not been decided yet), and *Druken* in Newfoundland (discussed below) found that a plaintiff had *no* expectation of privacy on *private* property, then privacy is not inherently tied to property (or else, being on private property on its own should be enough to always guarantee privacy). Though, I would note that in these noted cases, the courts relied on public *visibility* to determine there was no

---

[234] *Azak, ibid* at paras 96-97.
[235] *Heckert v. 5470 Investments Ltd,* 2008 BCSC 1298 [*Heckert*].
[236] Citing the Supreme Court of Canada's decision in *R v Wong*, [1990] 3 SCR 36 at 62.
[237] *Heckert, supra* note 235 at para 86.

expectation of privacy, drawing back to the idea that privacy is synonymous with withdrawal or seclusion from others/society, which is often associated with being confined within one's home. Meanwhile the court in *Heckert* noted that Supreme Court of Canada said in *R v Wong*[238] that while the location of an impugned invasion is an important factor, it is not determinative – for instance a person in a public restaurant might not reasonably expect that her private conversations are being recorded by state agents. Location alone was not the determining factor in whether the plaintiff could expect privacy.

The *Heckert* decision can support an optimistic contention that a plaintiff could have a privacy interest in a public or shared space depending on the circumstances. This interpretation could be readily narrowed though. For instance, the hallway location at issue in *Heckert* is not visible to *any* member of the public broadly, only to those with access to the hallway, which could be connected with a private-property based reason for being present in the building (either accessing one's home or visiting the home of another). Further, the court's concerns about her comings and goings were specifically connected with her private suite. Should these private-property related features be taken as significant to the future application of this case, it could narrow the application of the decision. In other cases, since *Heckert*, where an individual is in public or publicly visible, the court has again found that their visibility undermines any claim of privacy.[239] For the most part in BC, when conduct occurs in public or publicly visible space, the courts have treated that as fatal to the plaintiff's case.

---

[238] *R v Wong*, [1990] 3 SCR 36 at 62 [*Wong*] (Lamer CJC in dissent, later adopted by the Supreme Court of Canada in *R v Colarusso*, [1994] 1 SCR 20 at 38, 52-64 and *R v Edwards,* [1996] 1 SCR 128 at para 31).

[239] E.g., *Wasserman, supra* note 230 was decided after *Heckert, supra* note 235. See also: *TransMountain Pipleline ULC v Mivasair*, 2018 BCSC 1909 (an individual who is participating in a protest intended to draw attention cannot have an expectation of privacy concerning his conduct at that protest); *Duncan v Lessing*, 2018 BCCA 9 (parties engaged in civil litigation must expect some intrusions into their personal information and privacy, as information must be shared to aid with the truth-finding function of the court process).

Disclosure of Information

There is relatively little case law dealing with the disclosure of information or images collected from public space. However, from the little that exists, the courts have to date suggested that the fact that information is public may prove fatal to a claim for a privacy violation in regards to the subsequent sharing of that information as well. In *Milton v Savinkoff,* the BCSC held there was no violation of privacy when the defendant disseminated an intimate photograph of the plaintiff after she accidentally left the photo in the pocket of the defendant's coat. The court held that the plaintiff had implicitly waived her privacy in the photo by leaving it in the defendant's coat pocket and not retrieving it sooner.[240] The court also referred to the fact that she had not asserted a privacy interest over the photograph when she had it developed from film.[241] The court asserts an all-or-nothing notion of privacy here, wherein once a plaintiff makes something visible to one person, they forfeit their privacy vis-à-vis anyone even if subsequent sharing is non-consensual. This is an analysis stripped of context. It is in contradiction though to *obiter* in cases like *St. Pierre*, where the plaintiff's knowledge that his photograph had been taken by a newspaper did not amount to an implied consent to use that photograph on future occasions. The *Savinkoff* decision is also in contradiction to the growing consensus in other provinces (and potentially soon in BC[242]) that non-consensual sharing of an intimate image amounts to a privacy violation. Savinkoff is accordingly open to highly persuasive critique. Few other decisions in B.C. give guidance here though. In *Fouad v. Wijayanayagam*, for example, the BCCA held that an inquiry to obtain information that amounts to public information (e.g., professional qualifications) did not amount to a violation of privacy.[243] The court suggests again that when something is already public, the plaintiff will struggle to ground a

[240] *Milton v Savinkoff* (1993), 18 CCLT (2d) 288 (BCSC).
[241] *Milton v Savinkoff, ibid* [fourth from final paragraph, not numbered].
[242] Samantha McCabe, «BC Makes First Moves Against 'Revenge Porn'» (May 13, 2021) The Tyee, online : https://thetyee.ca/News/2021/05/13/BC-Makes-First-Moves-Against-Revenge-Porn/> (accessed Feb. 13, 2022).
[243] *Fouad v Wijayanayagam*, 2015 BCCA 272 (CanLII).

privacy claim even for its further dissemination. In addition to the wilfulness requirement discussed above, it is possible that a plaintiff will have some difficulty proving a violation of their privacy under the statute for a disclosure of information taken from a public space.

Saskatchewan

Under Saskatchewan's *Privacy Act*[244], like the BC *Privacy Act*, it is a tort to willfully violate the privacy of another person, without claim of right. As in BC, the term willfully has been interpreted to mean intention to do something invasive (not merely to intentionally do something that incidentally violates privacy).[245] The Saskatchewan *Act* provides four examples of *prima facie* violations, including: "auditory or visual surveillance of a person by any means including eavesdropping, watching, spying, besetting or following and whether or not accomplished by trespass"; listening to or recording a conversation; use of a person's name or likeness for financial gain; or use of someone's letters, diaries, or other personal documents without express or implied consent.[246] This is more detail of what can *prima facie* constitute a tort under the statute than provided in BC's *Privacy Act*. The *Act* also does not explicitly or directly limit the application of the tort to private spaces or information.

The legislature recently amended Saskatchewan's *Privacy Act* to include new sections 7 and 8 to explicitly create liability for the non-consensual distribution of intimate images.[247] The Saskatchewan *Privacy Act* now makes clear that consenting to an intimate photograph or film does not amount to consent to its subsequent distribution.[248] When an intimate image is distributed, among other things, the court is also instructed to presume there was no consent for the distribution

---

[244] *The Privacy Act*, RSS 1978, c P-24 [Saskatchewan *Privacy Act*].
[245] *Peters-Brown v Regina District Health Board*, 1995 CanLII 5943 (SKQB).
[246] Saskatchewan *Privacy Act*, s. 3(a)-(d).
[247] *The Privacy Amendment Act*, 2018, SS 2018, c 28. This act was assented to May 9, 2018.
[248] Saskatchewan *Privacy Act*, s 7.4.

unless the defendant can establish reasonable grounds to believe they had ongoing consent.[249] While the application of these sections is specific to intimate images, at least one important specification in these sections – that consent to one form of conduct does not equate to blanket consent to any subsequent related conduct – may, as an underlying theory of consent and privacy expectation, influence the courts' interpretations of privacy expectations more broadly throughout the statute. It is not yet clear if that will be the case or if this interpretation will be specific to intimate images, though there is precedent in other areas of law that could also support the broader interpretation, as I discuss at greater length in Chapter 6.

The Saskatchewan *Privacy Act* lists a number of considerations for determining whether conduct has violated a plaintiff's privacy. Like in BC, the statute says the "nature and degree of privacy to which a person is entitled […] is that which is reasonable in the circumstances."[250] Relevant circumstances include (non-exhaustively): the nature, incidence and occasion of the impugned act; the effect of that act on the social, business or financial position of the plaintiff; any relationship between the parties; and the conduct of the plaintiff and defendant both before and after the impugned incident.[251] It is "questionable" in Saskatchewan whether a common law tort of invasion of privacy also exists.[252] Nothing in the *Act* specifically limits its application to technology-facilitated privacy violations in a public space, so long as the court is willing to recognize that a plaintiff is entitled to privacy in public. There have been relatively few cases considering the provisions of the Saskatchewan *Privacy Act*, and within that jurisprudence even less analysis of the

[249] Saskatchewan *Privacy Act*, s. 7.5, refers to this as "reverse onus." That terminology is actually inaccurate because it always falls to the defendant to prove consent as a defence (see defences, s. 4(1)(a)). Nevertheless, the statute now makes clear that the defendant cannot prove consent without establishing reasonable belief.
[250] *Ibid* at s. 6(1).
[251] *Ibid* at s. 6(2).
[252] *Peters-Brown v Regina District Health Board*, 1995 CanLII 5943 (SK QB)

application of the tort in public spaces, so it is not yet clear how the courts will interpret the *Act* in such circumstances.[253]

In a leading decision under the *Act*, *Bigstone v St. Pierre,*[254] the Saskatchewan Court of Appeal considered the scope and application of the Saskatchewan *Privacy Act* broadly. The Court adopted the Black's Law Dictionary definition of privacy, like in BC, interpreting privacy in this case as "freedom from attention, intrusion or interference."[255] The definition could feasibly be interpreted to include unwanted attention or interference in public space as well as in private space – there is nothing inherently exclusive to private space here.

The Court also stated, perhaps importantly in the context of this thesis, that unlike the *Charter*, which acts as a shield to limit state actions, the Saskatchewan *Privacy Act* serves as a sword, meant to allow compensation for a violation of privacy.[256] This "suggests that the privacy [that] the *Act* protects may be more extensive, and different in some respects, than privacy under the *Charter,"* necessitating a different analytical approach to evaluate whether an expectation of privacy has been violated.[257] In fact, the court in *Bigstone* goes on to observe that the listed *prima facie* violations "speak of a privacy interest that is both more broad and less intimate than the *Charter* concepts, which would, for example, *not prohibit surveillance in a public place under most*

---

[253] A couple of lower court decisions tangentially relate to the issue under examination here, but do not clearly help in understanding how an interpersonal privacy conflict might be resolved in public space. In *Pelletier v Collins*, 2012 SKQB 318 (a motion to dismiss, involving a dispute between neighbours) the Queen's Bench held that it is not a tort pursuant to the Saskatchewan *Privacy Act* to spy on someone's house when they are not present as the *Act* only addresses the surveillance of a person (para 44). The plaintiffs also claimed personal surveillance but provided insufficient detail to support the claim, which was ultimately struck. In *Ratt v Tournier*, 2014 SKQB 353 – a student sued the vice principal of their school after the VP looked at a text message on his phone. The court held it was not a violation of privacy because this conduct falls within the scope of the VP looking out for the safety of the plaintiff as would a reasonable and prudent parent (the VP owes a corresponding duty of care to the students).

[254] *Bigstone v St. Pierre,* 2011 SKCA 34 [*Bigstone SKCA*] (a motion to dismiss an allegation of violation of privacy).

[255] *Bigstone SKCA, ibid* at para 22. "*Black's Law Dictionary*, 9th ed. provides the following definitions of privacy: "The condition or state of being free from public attention, to intrusion into or interference with one's acts or decisions. Autonomy privacy – An individual's right to control his or her personal activities or intimate decisions without outside interference, observation or intrusion. Informational privacy – A private person's right to choose to determine whether, how and to what extent information about oneself is communicated to others, especially sensitive and confidential information."

[256] *Bigstone SKCA, ibid* at para 21.

[257] *Bigstone SKCA, ibid* at para 21.

circumstances."[258] Notably, *Charter* concepts of privacy have also expanded and become more nuanced since *Bigstone* was decided in 2011, further supporting this interpretation of the *Act,* as I discuss at length in Chapter 6.

Bigstone further stipulates that section 3 of the *Act*, which sets out *prima facie* violations, casts a wide net with no suggestion that a plaintiff's "core biographical information" must be engaged for there to be an infringement (where the *Charter* would more typically require that for an informational violation).[259] So the court here is interpreting the *Act* to apply more broadly than the *Charter* privacy protections available at the time, which could support its application in public space, in contrast to the interpretation of the *Act* in BC. There was, notably, a dissent in this decision in which Smith JA disputes such a broad interpretation of the Saskatchewan *Privacy Act.*[260] It is not yet clear if the dissent would have traction in future cases to limit some of the breadth interpreted into the *Act* in the majority decision. To date, the law in Saskatchewan appears broader and more nuanced than in BC.

Ultimately, the *Bigstone* decision only dealt with a motion for dismissal (the dismissal was denied) not involving circumstances of a violation of privacy in a public space, so much of the insight from the decision is *obiter*. Only future decisions will confirm if the broad interpretation taken by the majority in *Bigstone* applies to alleged intrusions occurring in public spaces.[261] At the very least, such an application of the *Act* seems quite possible.

---

[258] *Bigstone SKCA, ibid* at para 23, emphasis added. The Court of Appeal emphasizes that the interests under the *Act* are broader than, for example, those set out in *R v Tessling,* 2004 SCC 67 at para 23.
[259] *Bigstone SKCA, ibid* at paras 24-26.
[260] In dissent, Smith JA says: "I do not agree that such an extraordinary expansion of the notion of legally protected privacy interest is the purpose or intent of this section, or of the *Act* in general. It is not the intention of the *Act* to make merely investigating, seeking to find out, accessing, or gathering information about a person an actionable violation of that person's privacy, in the absence of the conduct described in s. 3, or other unusual circumstances. Certainly s. 3 is not itself this broad." *Bigstone SKCA, ibid* at para 57.
[261] One recent case involving a claim over disclosure of information, and interpreting *Bigstone,* provides little insight: *Asm Sabbir Ahmed v Canadian Light Source Inc.,* 2018 SKQB 320 (successful motion to dismiss claim for disclosure of documents permitted within scope of employment contract).

On the other issues addressed above, such as disclosure of information collected from public space, and the degree of intention/willfulness required to meet the elements of the tort, the Saskatchewan jurisprudence has yet to give any definitive indication. While it is common for courts to look to other provinces to facilitate their interpretation of their own provincial statutes, especially when they are so similar in wording, *Bigstone* suggests that Saskatchewan courts may be open to different interpretations of their *Act* than seen in BC.

Manitoba

While Manitoba's statute is similar in many ways to the other provincial statutes, it has some notable differences in its wording. An actionable violation of privacy occurs when "a person *substantially*, *unreasonably*, and without claim of right, violates the privacy of another person."[262] Notably, the statute does not require "wilfulness." A possible interpretation of this provision includes that a reckless or negligent violation of privacy to be captured by the scope of the tort. This seems broader than the other provincial statutes, particularly BC, given the courts' narrow interpretation of wilfulness. However, the courts have not yet been asked to consider this interpretation, according to published cases. And there are still limits to the tort's scope in Manitoba, which might in some ways be more restrictive compared to other provinces even in the case of an intentional, or wilful, violation. In particular, Manitoba's *Act* requires that the defendant *substantially* violate the privacy of the plaintiff. The courts have not yet commented on whether this raises the threshold of the test for a plaintiff, but that interpretation seems likely (Ontario has a similar requirement in common law, discussed below). The issues noted above about the possible treatment of, *e.g.*, brief filming by a single Ring camera could be relevant here to a court's analysis, potentially

[262] *The Privacy Act*, CCSM c P125, s. 2(1) emphasis added [Manitoba *Privacy Act*].

suggesting that the tort does not apply to such conduct by a defendant (as it does not on its own *substantially* violate privacy).

In fact, in one motion to dismiss arising from an action for violation of privacy in respect of the use of a Ring camera (the first Ring privacy case in Canada, and the first case of a dispute between neighbours over shared or publicly visible space decided under the Manitoba *Privacy Act*), the court held among other things that if there was a violation of the plaintiff's privacy from the camera, it was not "substantial."[263] In this case, *Zeliony v Dunn*, the plaintiff and defendant shared a common entryway to their respective condominium and storage units. After the defendant's motion sensor light had been repeatedly tampered with, he installed a Ring doorbell camera to determine who was responsible. The plaintiff, whose movements through the shared hallway caused her to move past the Ring camera, unsuccessfully sued for a violation of privacy.

The court's finding that the plaintiff's privacy was not violated was based on several factors. There was no evidence of constant surveillance of the plaintiff. The defendant, on request from the condominium association, had set the motion detection for the camera (which would trigger it to record) to 5-feet, meaning it would only turn on when someone approached within 5-feet of his door. And, the images were stored in the cloud for 60 days and then deleted.[264] While the court held that there was no doubt the plaintiff could expect privacy entering and leaving her condominium and storage unit (referring to the *Heckert* decision from BC), in this case the collection of information was not "substantial."[265] This case underscores that even where a court might accept that the defendant has engaged a plaintiff's expectation of privacy, the plaintiff might fail in their claim if they cannot show that a violation was "substantial." I return to this decision again below, as

[263] *Zeliony, supra* note 17 at para 34.
[264] *Zeliony, ibid* at para 31.
[265] *Zeliony, supra* note 17 at para 34.

the court also commented on the contextual analysis for determining a reasonable expectation of privacy and possible claims of right on the defendant's part that can defeat an action under the *Act*.

The Manitoba *Privacy Act* also sets out examples of *prima facie* violations similar to those in the Saskatchewan *Privacy Act*, with one noteworthy distinction. In section 3(a), the Manitoba *Privacy Act* provides that privacy may be violated "by surveillance, auditory or visual, whether or not accomplished by trespass, *of that person, his home or other place of residence, or of any vehicle*, by any means including eavesdropping, watching, spying, besetting or following." Accordingly, a privacy violation does not have to target the plaintiff personally, but may involve or implicate her home or vehicle as well. The provision, like in Saskatchewan, seems applicable to *things* related to the plaintiff, which might implicate their location or movements, or might be seen as extending the scope of private spaces beyond the home to include vehicles as well.[266] Most charitably this provision might extend the scope of the *Act* to include some activities in public spaces, connected to the plaintiff's vehicular movement for example.[267] However, as noted below, the court's interpretation of the *Act* has followed a similar tone to other provinces in finding that when something is in public there is little or no reasonable expectation of privacy. While I was not able at the time of writing to locate any cases dealing with disclosure of information under Manitoba's *Privacy Act*, the analysis on disclosures set out for the two provinces above might be influential here too, given the similarity in the wording and framing of the *Acts*.

The Manitoba *Privacy Act* does not list any specific considerations for the court when assessing whether there has been an invasion of privacy. It does however, set out similar considerations to those in the Saskatchewan *Act,* but for the purpose of assessing damages. The legislature has therefore left the determination of when a plaintiff may expect privacy to the courts.

---

[266] *Manitoba Privacy Act*, s 3(a).
[267] For instance, as the Supreme Court of Canada found in *R v Wise*, [1992] 1 SCR 527.

There is very little case law considering the *Manitoba Privacy Act* and only *Zeliony v Dunn* touches on the question of privacy in semi-public spaces. As noted above, the court in *Zeliony* relied on the BC decision *Heckert* to confirm that a plaintiff could expect privacy in a shared or public space, depending on the circumstances. The court also said that while location is relevant to the REP analysis, it is not exhaustive of the analysis. In *Zeliony v Dunn*, the court confirms that the analysis of a plaintiff's privacy should be contextual. In that case, because the shared entryway where the alleged violation took place was accessible to others, the plaintiff's expectation of privacy was considered diminished (though not non-existent). Additionally, there was no evidence that the camera actually captured footage from the inside of her condominium or storage unit (turning some attention to the notion that a violation of secrecy or private-property would incur a greater expectation of privacy, even with all other factors being the same). Further, the context in that case included the fact that the plaintiff had been tampering with the defendant's property, which was the reason he installed the Ring camera – this also weighed against the plaintiff's *privacy* claim.[268] The court treats the motive for using the camera separately in its reasons, but here also considers property protection as part of the contextual analysis of the plaintiff's reasonable expectations of privacy.

Finally, the Manitoba *Privacy Act* stipulates that a defendant has committed a tort only where the violation of privacy is "unreasonable" and "without claim of right."[269] In *Zeliony*, the court held that the defendant had a claim of right – described by the court as that of "lawful right of defence of his property."[270] The court also held that this contributed to the reasonableness of his conduct, along with the ways in which he limited the extent of information collected (e.g., limiting the motion

[268] *Zeliony, supra* note 17 at paras 31-32.
[269] Manitoba *Privacy Act*, s. 2(1).
[270] *Zeliony, supra* note 17 at para 34.

sensor to 5-feet, and eventually turning it off).[271] Ultimately, the *Zeliony* decision arose from a motion to strike and could be overturned in the future. But to date, it is the clearest indication of a court's reasoning with regard to the application of the statutory privacy torts to a Ring camera.[272]

Most significantly, the court's interpretation of "claim of right" in *Zeliony* goes to the heart of Ring's marketing – namely the protection of property. The court drew a specific distinction between surveillance of a particular individual (which would be more problematic), and surveillance to protect property (which it considered more reasonable). However, in many cases – as in *Zeliony* – those two scenarios may in practice be indistinguishable. By surveilling the front of one's property, one might by necessity surveil specific people whose daily schedules bring them into that space, like Ms. Zeliony in this case. The court's distinction here may prove to be useful to defendants in the types of scenarios imagined in this thesis, without perhaps capturing the contextual reality of what this means for other members of the public, as I discuss further in the chapters to follow.

Zeliony v Dunn recognizes that in the context of home security systems, "claim of right" might undermine a claim for a specific instance of, or even repeated, recording. As a motion to dismiss decision, this case is not determinative, however as the first case to deal with this issue, it may be influential in future decisions, and even in dissuading potential plaintiffs from bringing similar claims in the future.

---

[271] *Zeliony, ibid* at para 33.

[272] Another challenge to the use of Amazon Ring in a condominium arose recently in *Lupuliak v Condominium Plan No 8211689*, 2022 ABQB 65 in which the plaintiff sought an injunction to continue to use a Ring doorbell, and a condominium board sought an injunction to have her remove it. Other unit owners objected to its use, and claimed it violated the condominium by-laws. The court agreed with the condominium board and granted its motion. The case was not decided under privacy laws but clearly engaged privacy concerns of the other unit owners, see e.g., paras 18, 39.

Newfoundland and Labrador

The Newfoundland statutory privacy tort employs similar wording to BC and Saskatchewan.[273] The Newfoundland *Privacy Act* also outlines considerations for the court when assessing the nature and degree of privacy to which an individual is entitled. An individual can expect privacy that is "reasonable in the circumstances" with regard to the "lawful interests of others" and with regard to "the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties."[274] The *Act* protects the privacy of an "individual" defined as a natural person in section 2, and lists some *prima facie* violations, including the surveillance of an "individual," whether or not accomplished by trespass.[275]

The Newfoundland Trial Division has accepted that there is also a common law right to privacy available in the province, in addition to the statutory right. The key difference between the common law action and that set out in the Newfoundland *Act* is that under common law the plaintiff must prove her damages.[276]

There has not yet been any judicial consideration of the application of this statutory tort (or the common law tort) in public space. The closest the court has come to addressing publicly visible information/space was in the case *Hagan v Drover*.[277] The defendant company was photocopying the outside of envelopes sent to the plaintiff. The court did not refer specifically to the fact that the outside of the envelopes were visible to others as crucial to the determination, rather the court held that having regard to the defendant's legal rights and the employment relationship between the

---

[273] *Privacy Act*, RSNL 1990, c P-22 s. 3(1) [Newfoundland *Privacy Act*]. Also, unlike the other provincial statutes, the Newfoundland *Privacy Act* has a paramountcy clause such that where the *Act* is in conflict with another statute, it will prevail (s. 9).
[274] Newfoundland *Privacy Act*, s. 3(2).
[275] Newfoundland *Privacy Act*, s. 4(a).
[276] *Hagan v Drover*, 2009 NLTD 160 [*Hagan v Drover*], affirming *Dawe v Nova Collection Services (Nfld) Ltd.* (1998), 160 Nfld & PEIR 266 (NLPC); *Hynes v Western Regional Integrated Health Authority*, 2014 CanLII 67125 (NL SCTD). Section 7(1) of the *Act* says: "the right of action for violation of privacy under this *Act* and the remedies under this *Act* are in addition to, and not in derogation of, another right of action or other remedy available otherwise than under this *Act*."
[277] *Ibid.*

parties, the plaintiff "could not have had a reasonable expectation of privacy in the outside of envelopes from other financial institutions addressed to her at [her employer's] office which appeared to conflict with her contractual obligations."[278] This decision ultimately gives little guidance on the application of the tort in public spaces/information.

Like Saskatchewan, Newfoundland has also adopted statutory tort remedies for the non-consensual distribution of intimate images. The *Intimate Images Protection Act* has been in force since November 15, 2018. Section 4(1) sets out that it is a tort to distribute "an intimate image of another person without the other person's consent."[279] The *Act* does not require proof of damages.[280] And like Saskatchewan's provisions, the *Act* places the onus on the defendant to prove the image was distributed with consent.[281]

There is little judicial interpretation to assess with certainty how the Newfoundland *Privacy Act* will apply in the context of emerging technologies and public space. While there is nothing in the *Act* that excludes its operation from public space, the courts may find precedent from other provinces persuasive, including BC with the most statutory case law, and Ontario (discussed below) with the most common law tort authority. And Manitoba's *Zeliony v Dunn* may prove persuasive in terms of home surveillance systems specifically. In drawing upon any of these cases, the court might be more inclined to find limited, if any, application of the statute to public space-engaging conduct.

---

[278] *Hagan* at para 156.

[279] RSNL 2018, c I-22 [Newfoundland *Intimate Images Protection Act*]. Intimate images (visual recordings, including photo, film, or video) are those in which the person depicted is nude or engaged in explicit sexual activity, which were recorded in circumstances that gave rise to a reasonable expectation of privacy with respect to the image and the person depicted retained an expectation of privacy at the time it was distributed (s. 2).

[280] Newfoundland *Intimate Images Protection Act* s. 5.

[281] Newfoundland *Intimate Images Protection Act* s. 7. Importantly, s. 6 of the *Act* confirms that the person depicted in the intimate image does not lose an expectation of privacy with respect to that image simply because he or she consented to the recording of that image or provided that image to another person if that other person "knew or ought reasonably to have known that the person depicted in the intimate image did not consent to the further distribution of the intimate image." This Act reflects a trust-based theory of privacy – where we can share images with some people based on our relationship with them, without losing our expectation of privacy vis-à-vis others. This is distinct from a risk-based theory of privacy where the risk that another person will do what they wish with an image obliterates any further expectation of privacy. No actions have been brought under this Act as of the time of writing.

Conclusion on Statutory Torts

In most of the public-space engaging decisions under the statutory torts, courts have limited the interpretation of the torts such that they seldom apply to conduct occurring in public or shared spaces. Some decisions have explicitly denied that the torts could apply in public space. The statutes outline a number of considerations for courts to balance, some of which have been interpreted to further undermine the application of the statutory torts to the scenarios imagined in this thesis, especially with regards to "claims of right" and the protection of private property through surveillance. In the next two chapters, I suggest that the kind of reasoning exemplified in BC and in *Zeliony* is supported by an underlying trajectory of judicial conceptualization of privacy in association with property and secrecy. But this approach is not inevitable and need not guide the interpretation of the statutes. I will also argue that there are both theoretical and doctrinal reasons why this conceptualization of public space must change. Such change could render the torts more relevant to interpersonal public space privacy conflicts; whereas the current interpretations of the statutory torts render them largely unhelpful and inapplicable to such scenarios.

Common Law Privacy Torts

Most provinces have not enacted statutory privacy torts. In some of those provinces, though, the courts have recognized common law privacy torts instead. Ontario was the first province to recognize intrusion upon seclusion as a common law privacy tort, and until recently was the only province to recognize the common law torts of publication of a private fact,[282] and false light.

[282] While several provinces, as noted, have statutes recognizing non-consensual distribution of intimate images as a tort.

Prior to 2012, case law in Ontario showed an increasing judicial willingness to suggest or imagine that a privacy tort could exist.[283] This approach was finally confirmed in the Ontario Court of Appeal's 2012 decision *Jones v Tsige*, which made clear that at least in Ontario there is a common law tort of intrusion upon seclusion. *Jones* also opened the door for recognizing the other Prosser torts.[284] Other courts have since drawn on *Jones* when considering whether a common law tort exists within their jurisdiction, so this precedent and its interpretation are important not only for Ontario but more broadly as guidance for other jurisdictions.

Ontario – Intrusion Upon Seclusion

The facts of *Jones v Tsige* did not implicate privacy interests in public spaces. The conflict in *Jones* arose when the defendant Ms. Tsige used her position at a bank to access Ms. Jones' personal banking records on 174 occasions. Sharpe JA, writing for the Court, explained that these facts "[cried] out for a remedy."[285]

Sharpe JA reviewed case law and legislation from across Canada and in other jurisdictions to support his decision to recognize the new tort of intrusion upon seclusion in Ontario.[286] Sharpe JA also briefly notes that recognizing the new tort would develop the common law in line with Canadian *Charter* values, specifically the right to privacy – I explore the potential import of *Charter* values at length in Chapter 6, below.[287] But in order to define the parameters of the new Ontario tort, Sharpe JA drew directly from the US framing of privacy torts – particularly the "general right of the individual to be let alone" as described by Professors Samuel Warren and Louis Brandeis' in

[283] See e.g., *Somwar v McDonald's Restaurants of Canada Ltd.*, [2006] OTC 28 (Superior Court) (wherein Stinson J was unwilling to strike a tort claim for invasion of privacy because it was not clear there was no such action available in Ontario).
[284] *Jones*, *supra* note 27
[285] *Jones*, *ibid* at para 69.
[286] See *Jones, ibid* at paras 39-46.
[287] See *Jones, ibid* at paras 43-46.

their often-cited article, "The Right to Privacy"[288], and the U.S. *Restatement (Second) of Torts*[289] framing of four distinct privacy torts as identified by Professor William Prosser.[290]

Sharpe JA set out the following elements for the tort of intrusion upon seclusion:

1) The defendant's conduct must be intentional (including reckless);
2) the defendant must have invaded, without lawful justification, the plaintiff's private affairs;
3) and a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.[291]

In order to mitigate concerns that the recognition of the new tort might prompt a floodgate of litigation, Sharpe JA explained that there should be a narrow judicial application of intrusion upon seclusion as follows:

> A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy. Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: *it is only intrusions into matters such as* one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as *highly offensive*.[292]

On the facts of *Jones*, the court determined that Ms. Tsige had indeed intruded upon Ms. Jones' seclusion. Sharpe JA capped non-pecuniary damages (i.e. damages for non-economic harm) for the intrusion upon seclusion tort at $20,000 for the most extreme cases, providing only a brief statement that non-pecuniary damages should be "modest but sufficient to mark the wrong that has been done" to explain this significant damages cap (that notably, does not exist for any other privacy

---

[288] S.D. Warren & L.D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193 [Warren & Brandeis, "Right to Privacy"].
[289] *Restatement (Second) of Torts* (2010) at 652B.
[290] See *Jones, supra* note 27 at paras 17-18. See also, William L. Prosser, "Privacy" (1960), 48 California Law Review 383.
[291] *Jones, ibid* at para 71.
[292] *Jones, ibid* at para 27, emphasis added.

tort).[293] Sharpe JA found the facts in *Jones* constituted a middle ground, awarding Ms. Jones $10,000 in damages.[294] This limit on damages has significant import for plaintiffs in both strategic and practical terms – only certain lawsuits may be worth the financial, labour, and emotional costs for a plaintiff to bring forward, where damage awards are capped in such a way.

Overall, *Jones* recognizes a tort of intrusion upon seclusion, and through its explicit reliance on the U.S. framing of privacy torts, opens the door to the subsequent judicial recognition of other Prosser torts as well. However, on several occasions in the decision – particularly the requirement of a significant invasion, the way in which such an invasion is explained by limited examples in the decision, and the cap on damages – Sharpe JA seeks to narrow the scope of the tort's application.[295] As the next subsection shows, the narrow scope of the tort has contributed to an interpretation that it generally does not apply to conflicts and conduct arising in public space.

Application of Jones *to Conduct in Public Space*

Two cases involving conduct in physical public space suggest a possibility for the tort's application in public spaces, however these decisions are limited in their precedential value and thus may be of limited application to the scenarios investigated in this thesis. Beyond these two decisions, relatively few cases have involved an application of *Jones* to conduct occurring in public space. Several cases dealing with publicly available (especially digital) information suggest that the intrusion tort might not vindicate harms once something is shared or public.

---

[293] *Jones, supra* note 27 at para 87.
[294] *Jones, ibid* at paras 89-90.
[295] Reflecting what might be considered "judicial containment anxiety" – the judicial impulse to contain the scope of a new action, see Lisa M. Austin, "Privacy and Private Law: The Dilemma of Justification" (2010) 55 McGill Law Journal 165.

The first of these two cases arising in public space is *Vertolli v YouTube LLC*.[296] In this case, the co-defendant filmed the plaintiff, a police officer who pulled him over, and posted the footage on YouTube. YouTube refused to take the footage down because the footage did not violate the company's privacy policy. YouTube brought a motion to dismiss the plaintiff's action for intrusion upon seclusion, however the court refused to dismiss the action on the basis that it was not plain and obvious that filming a police officer in these circumstances was not an intrusion. As an unsuccessful motion to dismiss, the decision carries relatively little precedential weight, compared to a decision on the merits. But the fact that the court did not explicitly rule out that there could be an intrusion in public space is nevertheless notable (e.g., *Somwar* involved an unsuccessful motion to dismiss which later influenced the Court in *Jones* to recognize the intrusion tort[297]). This decision does not thoroughly engage with the context of the filming though, it rather focuses on the general question of whether an intrusion could never be found in public (such that the claim should be struck). In regards to the actual context of the filming in *Vertolli*, there is a notable power dynamic at issue between a police officer and someone whom the officer has detained, which should form a relevant part of the contextual analysis of whether the officer expected privacy, should the decision go further.[298]

The second of these two decisions is a Small Claims Court decision recognizing privacy in public - *Vanderveen v Waterbridge Media Inc*.[299] The defendant produced a sales video for a developer in Ottawa that included a scene showing the plaintiff jogging for approximately two seconds. The

---

[296] *Vertolli v YouTube LLC*, 2012 CanLII 99832 (ON SCSM) [*Vertolli*].
[297] See *Jones, supra* note 27 at paras 30-32, considering the decision in *Somwar*.
[298] Broader context here includes that Vertolli is now under investigation for allegedly posting Islamophobic materials on Facebook, see Steven Zhou, "Toronto-Area Cop Under Investigation for Alleged Islamophobic Posts" (August 7, 2020) Vice News, online: <https://www.vice.com/en/article/y3zbev/toronto-area-cop-under-investigation-for-alleged-islamophobic-posts>. While this is not directly relevant to the facts of the case discussed above, it is relevant to a larger conversation about police encounters and accountability, in which filming may be a component. The potential accountability mechanism served by filming and sharing information in this context must be balanced in the legal analysis, perhaps through a defence or in the REP discussion itself, as elaborated further in Chapters 6 and 7.
[299] *Vanderveen v Waterbridge Media Inc*., 2017 CanLII 77435 (ON SCSM) [*Vanderveen*].

plaintiff asked to be removed from the video, but the defendant refused. The court found that this conduct by the producers amounted to an intrusion upon seclusion, referring to *Jones* as well as to the Quebec *Civil Code* and related precedent.[300] While in principle this is a relevant case for the analysis in this thesis, seeming to vindicate subjectively felt privacy harms in public space, it suffers from at least two weaknesses. As a small claims court decision, it does not carry any precedential weight, though could be persuasive in future cases. More significantly, the judge appears to mistake two different branches of the Prosser privacy torts (intrusion upon seclusion, and misappropriation of personality[301]), and he applies law from different legal orders not engaged in the interaction, and is not precise in the application of the intrusion upon seclusion test. Accordingly, this case can likely be easily set aside by future courts. Nevertheless, the judge in this case touched upon the kinds of privacy concerns that can arise with public filming. The legal confusion in the decision may also signal the need for greater clarity around how courts should approach such an analysis. Chapters 6 and 7 offer some arguments in this regard.

Other Ontario court decisions have applied *Jones* in the context of publicly accessible or visible information, and generally found that because the information was publicly available, the plaintiffs had no reasonable expectation of privacy in it and therefore no tort claim. While information is of course different from physical public space in some important ways, the underlying privacy theory here – that one can only reasonably expect privacy in information they have kept secret or concealed – could easily be applied to public space too. For instance, reasoning by analogy might suggest that by virtue of entering into a space where one will be seen by others, a plaintiff no longer can reasonably expect not to be seen, and thus cannot bring claims related to that visibility or exposure. There are ample critiques of such a theory, which I explore further in the chapters to

---

[300] *Vanderveen, ibid* at para 16.

[301] E.g., "I am satisfied that the elements of intrusion upon seclusion […] apply to capturing the persona or likeness of an individual and using it for commercial purposes without consent.": *Vanderveen, ibid* at para 17.

follow, but it nevertheless remains evident in some judicial reasoning relating to the privacy torts. And as noted, the decision in *Jones* specifically narrowed the application of the intrusion upon seclusion tort in such a way that the limited application in public space flows naturally from the reasoning. For instance, *Jones* suggests only intrusions into highly secret spaces or information like diaries, private correspondences, and highly sensitive records will satisfy the requirements of the tort.[302] It is imaginable that most courts would accordingly not find intrusions where a plaintiff has shared their information (or visibility) with others.

For instance, *Broutzas v. Rouge Valley Health System* involved a class certification motion.[303] Hospital employees had accessed hospital records of patients who had given birth, and sold the patients' names and contact information to RESP sales representatives. The affected patients sought to bring a class action for a range of breaches including intrusion upon seclusion. The court denied certification for the intrusion cause of action, explaining that "there is intrusion but little, if any, seclusion."[304] In rendering this decision, Perell J. said of *Jones* that

> the tort of intrusion on seclusion is only for significant invasions of personal privacy. … The Court of Appeal was at pains to make it clear that recognizing intrusion on seclusion as a cause of action would not open the floodgates of claims based on invasion of privacy.[305]

Accessing and disclosing patient contact information in this case was not considered invasive (let alone "highly offensive") because contact information is in the public domain, and Perell J found that there is no reasonable expectation of privacy in information – such as the birth of a child, at issue in that case – that is publicly available and routinely disclosed to strangers.[306] This decision

---

[302] *Jones, supra* note 27 at para 72.
[303] *Broutzas v Rouge Valley Health System,* 2018 ONSC 6315 [*Broutzas*].
[304] *Broutzas, ibid* at para 1, and para 128.
[305] *Broutzas, ibis* at para 138, emphasis added.
[306] The court held that: "a reasonable person would not find the disclosure of contact information without the disclosure of medical, financial, or sensitive information, offensive or a cause for distress humiliation and anguish. The contact

implicitly takes an all-or-nothing approach to privacy, wherein once information is shared with someone, it loses privacy vis-à-vis anyone. The names and contact information here were publicly accessible. But what was truly at issue for the plaintiffs appears to have been the connection between this purportedly public information and the fact they had just given birth – a connection that was made available by the defendant; as well as perhaps a desire not to be contacted by marketers at an already stressful time. These considerations did not arise in the court's analysis, let alone nuance the fact that contact information is public.[307]

In *Baldwin v Morningstar*, the defendant corrections officers looked up the prior criminal conviction history of one of the plaintiffs and shared that information with the plaintiff's girlfriend's ex-partner.[308] Based on this information, the ex-partner then sought sole custody of his son and involved Child and Family Services in a custody matter. The court held that the defendant's access to the plaintiff's criminal conviction history through a work system was not an intrusion upon seclusion because the conviction information was already on the public record. In fact, the court noted that the corrections system provided less information than could be found on the Internet. Accordingly, the court dismissed the plaintiff's intrusion action. This decision seems to suggest that a plaintiff has lost any reasonable expectation of privacy in information once it is available publicly online regardless of the other circumstances. The court did not consider for example, the relationship dynamic of corrections officers using their employment to access information about the plaintiff, nor the context of intentionally sharing information within the scope of a custody dispute.

---

information that was the objective of the intrusion in the immediate case was not private, there was not a significant invasion of privacy, and the invasion of privacy was not highly offensive to an objective person": *Broutzas, ibid* at para 151. Also: "Save during the first trimester, the state of pregnancy, and the birth of child is rarely a purely private matter. The news of an anticipated birth and of a birth is typically shared and celebrated with family, friends, and colleagues and is often publicized. The case at bar is illustrative. All the proposed representative plaintiffs were not shy about sharing the news of the newborns.": at para 153. The court apparently sees no obvious distinctions between sharing a birth announcement with loved ones and sharing it with sales representatives.

[307] See, e.g., *Broutzas, ibid* at para 174.

[308] *Baldwin v Morningstar,* 2019 ONSC 1276.

This is despite the fact that these matters might have supported the drawing of an analogy to the reasoning in *Jones* wherein a partner in a relationship dispute used her employment to access the plaintiff's records and share with an ex-partner.

The *Baldwin* approach, like in *Broutzas*, points again at a theory of privacy where once information is available to someone, expectations of privacy are lost vis-à-vis anyone, regardless of the circumstances of its collection and use. Such an approach strips the inquiry of contextual factors, which might be pertinent to either the analysis of "private affairs" or in a case like this, of the "highly offensive" element. Other decisions have also held that where information is lawfully available to the public or on the public record, then accessing, using, or publishing that information is not an intrusion upon seclusion.[309] This reasoning by analogy could mean anyone visible to others in public and the use of publicly available information (e.g., through FRT applications that match images to public social media profiles) would not be addressed within the scope of the intrusion tort. These cases set aside consideration of significant additional contextual factors (relationships, power-dynamics, the privacy impact of associating pieces of information otherwise held separately[310], *etc*) once it is determined that the impugned information is publicly accessible.

Similarly in *Larizza v Royal Bank of Canada*[311] a motions judge held that credit checks do not give rise to a reasonable expectation of privacy because they contain information about dealings with third parties – the information is already known to those third parties and thus cannot give rise to an

---

[309] See e.g., *Bresnark v Thomson Reuters Canada Limited*, 2016 ONSC 5105 (no intrusion where an article is printed about the plaintiff citing information from a public court record); *Leung v. Shanks*, 2013 ONSC 4943 (information provided by a plaintiff to a defendant as part of a business relationship cannot be said to have been obtained without legal justification); *Singh-Boutilier v Ontario College of Social Workers and Social Service Workers*, 2015 ONSC 5297 (statutory authority to publish information means no actionable tort for publishing it).

[310] Something that Professors Woodrow Hartzog and Evan Selinger, for instance, have referred to as "obscurity." See e.g., Woodrow Hartzog and Evan Selinger, "Obscurity: A Better Way to Think About Your Data Than 'Privacy'" (January 17, 2013) The Atlantic, online: < https://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/>. See also Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Harvard University Press: 2018).

[311] *Larizza v The Royal Bank of Canada*, 2017 ONSC 6140.

expectation of privacy.[312] Also, in *Wiseau Studio et al. v Richard Harper* the court held that interviewing a third party about the plaintiff's national origins in a documentary was not an intrusion upon seclusion.[313] This conduct did not meet the "highly offensive" requirement, such that it is not "highly offensive" to seek out this information, particularly when it is already known to others – blending the "private affairs" and "highly offensive" analyses together. It is worth noting the important background to this case - the plaintiff is actor Tommy Wiseau, who had notoriously withheld telling people his national origins, and particularly had made a point of not sharing that information publicly. Nevertheless, the fact that he had spoken openly on set about where he was from was enough in the court's assessment to undermine the claim for intrusion upon seclusion.[314] The fact that Wiseau is a public figure who put his national origin in question is also a relevant fact in the assessment of liability in a case like this, but the court did not even reach this level of contextual analysis. It was unnecessary because the determination that the information was shared openly with others was fatal to the intrusion claim.

Accordingly, there is substantial jurisprudence in Ontario that may weigh against the application of the intrusion upon seclusion tort to any interpersonal privacy conflict that arises in public space, whether mediated by technology or not. In large part, this is due to a judicial precedent that stipulates, generally, that once something or someone is visible to others, they can no longer

---

312 The court cites to *Powell v Shirley*, 2016 ONSC 3677 aff'd 2018 ONCA 632 for this same holding (finding that plaintiff failed to prove a credit check invaded her 'private affairs' or that it was highly offensive).

313 *Wiseau Studio et al v Richard Harper*, 2017 ONSC 6535

314 See also: *Grech v Scherrer*, 2018 ONSC 7206 (defendant wants to introduce surveillance video he collected of the plaintiff as evidence to defend a different (non-privacy) claim. Plaintiff challenges whether the videos should be admitted arguing they amount to an intrusion upon seclusion. The court admits 3 of 8 videos as evidence (others excluded as not relevant). At paras 34-35 the court holds that there was no intrusion upon seclusion because there was no trespass, the defendant filmed activities between two neighbours outside of the plaintiff's home, where they could be seen by other neighbours or passersby (which "significantly detracts from the degree of privacy which could reasonably be expected"), and while one video shows the kitchen window into the plaintiff's home, it films plaintiff gesturing at the defendant so the court holds that the plaintiff obviously intended for the defendant to see this. While not directly dealing with a privacy tort claim, this decision provides another interpretation suggesting that the tort of intrusion upon seclusion does not apply in public space. See also *Robert v. Assis*, 2017 ONSC 1685 (involving an intrusion claim between neighbours for surveillance of plaintiff's yard, but dismissed for lack of evidence, including that police officers confirmed placement of camera did not engage other property).

expect the level of privacy in their information or themselves that would meet the high threshold required for this tort of "private affairs". Even where conduct might seem to engage privacy or private affairs, where information is known to others this factor seems to also undermine the "highly offensive" qualifier such that there is no tort. As the subsequent chapters will argue though, this general interpretation of the tort is neither a necessary one, nor is it necessarily an appropriate one based on the court's own jurisprudence and based on the underlying theories of tort law and privacy.

Intrusion Upon Seclusion in Other Provincial Jurisdictions

Plaintiffs in some other provinces have filed claims for intrusion upon seclusion, in some cases, successfully. However, to date only courts in Ontario and Nova Scotia have actually recognized and applied the tort of intrusion upon seclusion to a plaintiff's claim. Courts in BC and Saskatchewan are potentially open to the possibility too, notwithstanding their existing statutory torts. This leaves individuals in most of the Atlantic provinces and northern territories without recognized tort recourse in the common law Canadian system. Though it is certainly possible and arguably, likely, some form of privacy tort could be recognized in a new claim based on the precedent from these other provinces, as has happened with respect to other Prosser torts as well.[315]

New Brunswick

The New Brunswick courts have to date declined opportunities to recognize the common law tort of intrusion in the province.[316] The most recent case asking the court to recognize the

[315] E.g., Alberta has recently recognized the tort of disclosure of a private fact, drawing on the precedent from other provinces, particularly Ontario: *ES v Shillington*, 2021 ABQB 73. Also notably, I have only reviewed published decisions from across the common law provinces. Due to practicality constraints, I am not able to review all unpublished decisions from all common law jurisdictions, so it is possible that I have not included every relevant decision in this analysis. I am confident that a judgement recognizing a new tort would likely be published, or at least be newsworthy (and therefore more readily discoverable online).
[316] See e.g., *Avery v Attorney General of Canada et al.*, 2013 NBQB 152 at para 54.

intrusion tort was *Rancourt-Cairns v. Saint Croix Printing and Publishing Company Ltd.*[317] The plaintiff who was on medical stress leave had posted on Facebook that she would be selling candy baskets at an Easter market. Having seen the post (it is not clear from the facts whether this was a public post, or whether someone from the company was 'friends' with the plaintiff on Facebook and accessed it that way), the company she worked for her sent her an email concluding that she had resigned. She sued for, among other things, intrusion upon seclusion. In summarily dismissing her claim, the court held that even if the tort of invasion of privacy exists in the province (which the court did not decide upon), the plaintiff would fail to make out the elements (presumptively drawn from *Jones*) because there was no intrusion – she could not reasonably expect privacy in a publicly visible post.[318] There was no further contextual analysis (e.g. considering the dynamics of being monitored while on medical-leave from work, *etc*). Accordingly, based on the sparse state of the current jurisprudence, a plaintiff in New Brunswick may face an uphill battle in an intrusion upon seclusion claim for any privacy conflict in public or publicly visible space in the sense that they have no prior precedent on which to rely to counter some of the trends seen in other provinces, which may be persuasive in the New Brunswick courts.

Nova Scotia

Courts in Nova Scotia have confirmed that, on the right set of facts, there can be a damage award for intrusion upon seclusion in the province.[319] In *Capital District Health Authority v Murray*, the court certified a class proceeding for, among other things, an intrusion upon seclusion action against

---

[317] *Rancourt-Cairns v Saint Croix Printing and Publishing Company Ltd*, 2018 NBQB 19 [*Rancourt-Cairns*].
[318] *Rancourt-Cairns, ibid* at para 64.
[319] *Trout Point Lodge Ltd. v Handshoe*, 2012 NSSC 245 (however, this case was resolved under the tort of defamation). In *Doucette v Nova Scotia*, 2016 NSSC 25 at para 175 the court emphasized that where the same facts can lead to an award for defamation, it is not appropriate to also render an award for invasion of privacy, however, the court did not negate that such an award could otherwise be available in the province (upheld in *Marson (nee Doucette) v Nova Scotia*, 2017 NSCA 17 at para 29). In *Candelora v Feser*, 2020 NSSC 177 the court appears to interpret *Doucette* as confirming the recognition of the tort in the province.

a hospital for strip searching patients. The court held that it was not plain and obvious that there is no tort of intrusion upon seclusion in Nova Scotia.[320] The claim has since settled out of court so there was no final court decision on the substance of the class action.[321]

Further, in a family law divorce dispute decision, *VonMaltzahn v Koppernaes*, the court seemingly recognized the tort of intrusion upon seclusion as set out in *Jones*.[322] The respondent in that case had entered into the applicant's home, took pictures and items, and changed the locks. The applicant claimed, among other things, that this amounted to an intrusion on seclusion. The court referred to excerpts from *Jones*, and in a brief paragraph applied a reasonable person standard to find that the respondent's actions here were highly offensive. The decision does not explicitly consider the other elements of the tort. MacDonald J. awarded damages on the basis that: "Ms. Koppernaes' actions caused Mr. VonMaltzahn great distress, annoyance and worry. Her removal of possessions from his property was planned and deliberate. Her return of those objects was delayed and without genuine apology."[323] Reading this decision and *Murray* together suggests that the tort of intrusion upon seclusion has been recognized in *Nova Scotia*, and that the tort will be structured similarly to that set out in *Jones*. Accordingly, strengths and weaknesses in the application of the Ontario jurisprudence to interpersonal privacy conflicts in public space will be relevant here too.

Nova Scotia has also adopted a statutory cause of action for non-consensual distribution of intimate images ("NCDII").[324] Similar to other provinces with NCDII statutes, the statutory provisions in Nova Scotia seek to remedy harm from the subsequent use and distribution of intimate images, regardless of whether the individual depicted in the image originally consented to the taking of the image or sharing it with the defendant. The statute also deals with cyberbullying.

---

[320] *Capital District Health Authority v Murray*, 2017 NSCA 28.
[321] "Class action over forensic hospital strip searches reaches proposed settlement" (Feb 5, 2020) CBC News, online: <https://www.cbc.ca/news/canada/nova-scotia/class-action-suit-strip-searches-1.5452653>.
[322] *VonMaltzahn v Koppernaes*, 2018 NSSC 192.
[323] *VonMaltzahn v Koppernaes, ibid* at para 66. Ms. Koppernaes must pay Mr. VonMaltzahn $7,000.00.
[324] *Intimate Images and Cyber-protection Act*, SNS 2017, c 7.

Only one decision has been rendered under the statute so far, finding in favour of a plaintiff suing for damages for cyberbullying.[325]

Federal Court

Claims under a common law tort of invasion of privacy have also been brought before the federal court.[326] Only one, to date, has involved conduct occurring in public space. In *Sauve v Canada*, the plaintiff alleged that he was under RCMP surveillance and brought an action for the tort of intrusion upon seclusion.[327] While the court did not accept that there was surveillance, Martineau J held that even if there had been, he would have dismissed the claim. The alleged surveillance was "never done inside private areas and was always limited to the street, parking lots or to stores."[328] The court concedes that,

> Though I agree with the plaintiff that he has a privacy interest in his day to day activities and that surveillance conducted only from public settings can constitute an invasion of the private affairs of an individual, the surveillance in this case does not meet the criteria of intrusion upon seclusion.[329]

Because there was no allegation that the plaintiff was actually videotaped or photographed (except on one potential occasion), and because the plaintiff was under investigation for criminal harassment, the court concluded that a reasonable person would not find the surveillance offensive in this case.[330] Federal court claims will not typically be relevant to interpersonal privacy claims (claims would be brought to the federal court only against government or other entities that fall within its specific jurisdiction). But decisions from the federal courts could be persuasive in the common law context, and are worth noting.

---

[325] *Candelora v Feser*, 2019 NSSC 370; and *Candelora v Feser*, 2020 NSSC 177 (addressing damages).
[326] See e.g., *Condon v Canada*, 2018 FC 522 (settlement reached and approved, for the loss of sensitive student loan information).
[327] *Sauve v Canada*, 2015 FC 739 [*Suave*].
[328] *Suave, ibid* at para 50.
[329] *Suave, ibid* at para 51.
[330] *Suave, ibid* at para 51.

Ultimately, outside of Ontario, there has been very little judicial consideration of the intrusion tort, and nearly no analysis of the torts in public spaces. Generally, courts have been quick to emphasize that being in or accessible to the public undermines the argument that the defendant is engaging the plaintiff's private affairs, or where there may be some form of intrusion, that it could be highly offensive. When an occurrence arises in public space, courts tend to engage in very little or no further contextual analysis beyond the accessibility of the information.

Ontario – Public Disclosure of Private Facts

As noted, Ontario courts have now recognized all four distinct Prosser privacy torts. The public disclosure of private facts tort can also be relevant to the scenarios imagined in this thesis, particularly because the technology mediating a dispute can create a permanent record, which if subsequently shared may further engage the plaintiff's privacy interests. Notably, the two key decisions setting out this tort in Ontario involve non-consensual disclosure of intimate images (hereinafter "NCDII"), and so provide similar protections in Ontario to the provinces that have addressed NCDII through statute. Also notable is the fact that because this tort is applicable but not limited to NCDII, it has broader application to subsequent use of information/images, compared to the NCDII-specific legislation adopted elsewhere.

Not long after *Jones* was decided, the Superior Court recognized the privacy tort of public disclosure of private facts in *Jane Doe 464533 v ND*.[331] The defendant, ND, posted an intimate video of the plaintiff, his ex-partner, online. The court recognized the new tort and held that:

> [one] who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the

[331] *Jane Doe 464533 v ND,* 2016 ONSC 541 [*ND*].

> matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[332]

The plaintiff was awarded $50,000 in general damages, and an additional $50,000 for aggravated and punitive damages. Stinson J did not adopt a cap on damages as Sharpe JA had in *Jones*, explaining that the non-pecuniary toll that the sharing of private information could take on a plaintiff can go beyond $20,000 in compensation and so there should be no limit. However, because the defendant did not appear before the court or argue a defence, Stinson J's default judgment recognizing the tort was later set aside.[333]

Two years later in a similar case also involving the non-consensual disclosure of intimate videos on the internet, *Jane Doe 72511 v NM,*[334] the court re-affirmed the recognition of a tort of public disclosure of private facts, drawing on *Jones* and *ND* to support this finding. This decision was also a default judgment, though this one was not subsequently set aside. The elements of the cause of action, as set out in *NM* are as follows:

> (a) the defendant publicized an aspect of the plaintiff's private life;
>
> (b) the plaintiff did not consent to the publication;
>
> (c) the matter publicized or its publication would be highly offensive to a reasonable person; and
>
> (d) the publication was not of legitimate concern to the public.[335]

---

[332] *ND, ibid* at para 46.
[333] *Doe v ND*, 2016 ONSC 4920.
[334] *Jane Doe 72511 v NM*, 2018 ONBSC 6697, per Gomery, J [*NM*].
[335] *NM, ibid* at para 99.

These largely track the US framing of this same tort, with one distinction where Gomery J explained that "it need not be the matter itself that is highly offensive to a reasonable person: it is enough if the fact of its publication is offensive."[336]

Gomery J also spent several paragraphs in the judgment justifying the recognition of the new tort, on bases similar to *Jones*. For instance, the federal government had recently made the non-consensual sharing of intimate images a criminal offence.[337] The criminalization of this conduct signifies that it is highly offensive and harmful, which also justifies that there should be a civil remedy available.[338] Gomery J also explains that the recognition of this tort would be consistent with the *Charter* value of privacy, and that a "cause of action for public disclosure of private facts represents a constructive, incremental modification of existing law to address a challenge posed by new technology."[339] The egregious facts and obvious harm in this case, like in *Jones*, called out for a remedy.[340] *Doe* was awarded $75,000 for the publication, and $25,000 in punitive damages.

In each of these decisions, it did not matter that the plaintiff had consented to the original taking or sharing of the photograph. The courts' analyses were nuanced in considering the ways that consent to one form of sharing or observation does not amount to a blanket consent/dismissal of privacy expectations over every subsequent use.

---

[336] *ND, supra* note 331 at para. 46, *NM, supra* note 334 at paras. 81, 98-99. In a subsequent decision, *Yenovkian v Gulian,* 2019 ONSC 7279 at para 169, the court reaffirms this modification to the description of the tort "because it is important to emphasize that a sexually explicit videotape is not in itself necessarily "highly offensive". There is nothing inherently wrong about taking intimate photos of an adult or filming consensual sex between adults, or agreeing to participate in such photos or recordings. What is wrong is the non-consensual publication or sharing of a photo or recording of someone who did not want to share it with anyone else."

[337] *NM, ibid* at para 84: "Where misconduct is identified as wrong, harmful and antithetical to an orderly society such that it attracts a criminal sanction, it makes sense that the same misconduct should give rise to a civil remedy." Continuing at para 84: "For example, in the case at bar, [NM] was convicted for his criminal assault of Jane [Doe] in March 2014, and she has a civil remedy (battery) against him for this same conduct. The criminal charge is based on the collective interest in deterring and sanctioning violent and anti-social behaviour. The civil remedy allows the victim to recover damages for their injury."

[338] *NM, ibid* at paras 85-86.

[339] *NM, ibid* at para 93.

[340] *NM, ibid* at para 95.

It is not yet clear if the Ontario courts would recognize that information collected from public space can meet the requirement that its publication be "highly offensive." The case law arising under the BC *Privacy Act* suggests that a plaintiff may have an uphill battle in arguing that they meet this element. However, absent any interpretation from the courts yet, this remains open to argument. Ultimately though, this tort also only applies to *publication*. Its scope does not address all potential subsequent use of information. While it may, for instance, be available to a plaintiff whose image has been shared on a neighbourhood app, the tort does not clearly apply to the subsequent personal-use application of, for instance, facial recognition or another means of analysis that does not involve sharing or making the information public. Such a claim would have to be made under the intrusion upon seclusion tort, overcoming its limits regarding public information. While this second Prosser tort may be applicable to interpersonal privacy conflicts arising from public space, it is limited by its scope in addressing the range of potential harms associated with subsequent use or processing of information and images.

Nova Scotia – Public Disclosure of Private Facts

In February 2021, Justice Coughlan for the Nova Scotia Superior Court recognized the tort of publication of a private fact for the first time in that province in *Racki v Racki*.[341] The defendant had published details about the plaintiff's life that she did not want shared, including about her struggles with addiction and mental health. The court drew explicitly from *Jones* (but not *Jane Doe v NM*) and the US restatement of tort in deciding to recognize the tort in Nova Scotia.[342] In particular the court relied directly on the US Restatement to understand the meaning of bringing "publicity" to a private fact. The Restatement calls for "a communication that reaches, or is sure to reach, the

[341] *Racki v Racki*, 2021 NSSC 46 [*Racki*].
[342] *Racki, ibid* at paras 18-20.

public."[343] In other words, the publication/disclosure cannot be just to one or a few others but needs to be a communication more widely to the public, and become public knowledge.

The court identified the elements as follows, which are notably somewhat different than the elements required in Ontario:

> (a) There must be publicity of the facts communicated to the public at large to become a matter of public knowledge;
>
> (b) The facts are those to which there is a reasonable expectation of privacy; and
>
> (c) The publicity given to those private facts must be considered, viewed objectively, as highly offensive to a reasonable person causing distress, humiliation or anguish.[344]

The second element here is not specifically required in Ontario, and Ontario explicitly requires that the disclosure be non-consensual. Nova Scotia's test considers whether the impugned facts that give rise to a reasonable expectation of privacy, which for the reasons discussed above could rule out facts collected from public spaces on the courts' current conceptualization of privacy in public space.

The defendant in *Racki* argued that his right to publish details about his wife was protected by freedom of expression. While not going so far as to recognize a defence to the tort, Coughlan J does appreciate that privacy interests are not absolute and must be balanced against competing interests, including free expression. Coughlan J considers whether the publication in this case was in the public interest, drawing on the defamation case *Grant v Torstar*. The SCC in *Grant* considered the same issue in developing a defence to the defamation tort when press publish untrue statements in an investigative piece.[345] Considering that the defendant's book dealt with entrepreneurship, details

---

[343] *Racki, ibid* at para 20.
[344] *Racki, ibid* at para 26.
[345] *Racki, ibid* at paras 37-39.

about the plaintiff's personal life were not in the public interest in relation to his publication. However, one might imagine a situation in which information collected, for instance from a home security system, is shared with neighbours in relation to local crime, where the defendant might argue that the disclosure was in the public interest. Subsequent courts will need to clarify how and where the public interest arises in relation to this tort.

Finally, the court in *Racki* relies on the same guidance for awarding damages provided in *Jones* (even though *NM* subsequently specifically did not rely on that guidance) to assess damages here.[346] This suggests that damages will be modest and potentially capped in Nova Scotia as well.

Alberta – Public Disclosure of Private Facts

In September 2021, Justice Inglis of the Alberta Court of Queen's Bench recognized the common law tort of public disclosure of private facts for the first time in Alberta in *ES v Shillington*.[347] The defendant had engaged in non-consensual distribution of images of the plaintiff, as well as other harmful conduct toward the plaintiff. The court drew explicitly on *Jane Doe v NM* and *Jones v Tsige* to support recognizing the tort, with almost the same elements as in Ontario. The key modification in Alberta was to the third element of the tort – "the matter publicized or its publication would be highly offensive to a reasonable person in the position of the plaintiff" – more explicitly noting that the plaintiff's perspective on the impact of publication is important.[348] While Alberta has a statutory civil action to address the non-consensual disclosure of intimate images, the court here notes that a common law tort would also protect information beyond intimate images,

[346] *Racki, ibid* at paras 47-52. The court awarded $18,000 in general damages and $10,000 in aggravated damages as the motive appeared to be malicious.
[347] *Shillington*, *supra* note 315.
[348] In Ontario the element is phrased as: "the matter publicized or its publication would be highly offensive to a reasonable person." The ABQB draws on British precedent here to make explicit this nuance to the element: *Shillington, supra* note 315 at paras 68-70.

which was an existing legal gap.[349] As this case did not engage information that was already publicly accessible or taken from a public space, similarly to the publication cases in other provinces, the observations noted above about the potential limits of this tort, particularly in regard to the similar Ontario tort, apply here as well. The court looked to the precedents from Ontario and one case from BC to consider damages. The court, as in the NCDII cases in Ontario, did not feel bound by the damages limit set in *Jones*, and awarded $80,000 in general damages and $50,000 in punitive damages, citing the even more blameworthy nature of the defendant's conduct compared to *NM*. Further, the court found this defendant was motivated by malice and awarded $25,000 in aggravated damages.[350] The court cited the particularly harmful impact of sexually-based wrongdoing.[351]

Ontario - False Light

In *Yenovkian v. Gulian*, Kristjanson J of the Ontario Superior Court recognized the remaining Prosser tort of publicity placing a person in a false light in Ontario (referred to as "false light" for short).[352] In fact, Kristjanson J directly adopted the US Restatement of the tort:

> Publicity Placing Person in False Light
>
> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
>
> (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
>
> (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[353]

---

[349] *Protecting Victims of Non-consensual Distribution of Intimate Images Act*, RSA 2017, c P-26.9.
[350] *Shillington, supra* note 315 at paras 87-102.
[351] *Shillington, supra* note 315 at para 90.
[352] *Yenovkian v Gulian*, 2019 ONSC 7279.
[353] *Yenovkian, ibid* at para 170.

Yenovkian arose out of a family dispute in which a father engaged in years of cyberbullying his ex-partner and her parents, as well as editing and posting videos and photographs of his children online along with demeaning commentary. The court found that the tort had been met through Mr. Yenovkian's extreme and flagrant online attacks of Ms. Gulian including false claims that she abused her children. This is notably the third tort in Ontario recognized as a result of domestic privacy invasions – *Jones* involved intrusions by a partner of the plaintiff's ex-partner, and the various cases grounding the disclosure of a private fact tort involve distribution of intimate images initially shared in a relationship context. While the courts have not made any specific reference to this fact, it suggests that courts *may* be attuned to the particular privacy dynamics of intimate relationships. This foundation to the torts has not generated considerable nuance within the subsequent case law, however.

Within the scope of investigation in this thesis, the seemingly most likely application of false light would be in the context of sharing information, for example through a neighbourhood sharing app, or posting information online, for instance like the drone vigilante. The tort is of somewhat limited application, given that the sharing of information must convey a falsehood about the plaintiff (where sharing of video might be found to simply covey the facts of an occurrence), and that the false light into which the plaintiff is put must be "highly offensive." But this tort could be relevant in particular in contexts where sharing is also influenced by norms of neighbourhood exclusion or other negative judgment – for instance, sharing video and portraying a plaintiff as suspicious or threatening, or insinuating other falsehoods about someone based on the information collected from public space. Such a set of facts may also engage defamation considerations which, while pertinent, are beyond the scope of this thesis. This tort in particular seeks to address *publicity* considerations, thus would require that the defendant sought to draw attention to the false information about the plaintiff, which is certainly imaginable through a network like Ring and Neighbors.

Conclusions on Common Law Torts

The elements of the common law privacy torts, like the statutory torts, do not inherently rule out the possibility of compensation for privacy harm in public spaces, or in a technology-mediated privacy conflict. However, the courts have to date interpreted at least the intrusion upon seclusion tort to be of limited application in public space/information. It is quite possible publicity of a private fact would be interpreted this way as well. In the common law, as in the statutory provisions, the use or disclosure of information has received more nuanced judicial consideration than the intrusion or collection of information. But there have been so few cases (if any) dealing with facts that might be analogous to the scenarios envisioned in this thesis that the application of these torts does remain an open question.

In the common law provinces, an individual who seeks vindication for alleged privacy-violating conduct in public space faces several hurdles. Ultimately the greatest likely barrier to the application of the common law torts to mediate the sorts of conflicts envisioned in this thesis is the salient fact that a conflict arose in *public space*. This spatial dynamic is relevant to the question of whether the plaintiff could expect privacy in the circumstances; whether the defendant's conduct is significant or highly offensive enough to meet the requirements of the privacy torts; whether the defendant wilfully invaded a plaintiff's privacy; whether the defendant has a claim of right for their conduct; whether shared information is considered a "private" fact; and likely, whether the public interest in free expression might be engaged in the court's analysis. Ultimately, many of these issues come back to how the courts have understood public space – as a space of inherent publicity/visibility, and as a space where privacy is not a relevant, or at least legally legitimate, concern for a plaintiff.

However, it remains worth noting that the earliest Canadian torts were developed to deal with the kinds of technology-mediated privacy concerns envisioned in this thesis, and that there is

nothing explicit in the torts that should exclude their application from public space. This narrower application has arisen from judicial interpretation. The next chapter examines where this judicial conceptualization of public space, and privacy in public, formed and how it arose in the Canadian jurisprudence. The subsequent chapters contend that this conceptualization is neither inevitable, nor appropriate, on a theoretical and doctrinal basis. Accordingly, Chapter 6 calls for a rethinking of the judicial mindset around the privacy torts, and reform of their interpretation that acknowledges the importance of privacy to public spaces, and to the public interest in these spaces.

Chapter 4 – The Public Space Critique of the Privacy Torts

The previous chapter identified whether and how the privacy torts might address interpersonal conflicts in public spaces, particularly where these conflicts are mediated by remotely-operated technologies. Notably, the location of such a conflict in public space often contributes to the exclusion of the application and relevance of the privacy torts, regardless of the broader circumstances of the interaction. Numerous academic commentators have raised concerns with the judicial exclusion of the privacy torts from public spaces. This chapter considers these critiques of the Canadian torts, which provide helpful guidance in considering how tort law may respond to the challenges posed by increasing inter-personal surveillance. Many critiques suggest reform that would extend the court's current privacy analysis to include public spaces by reducing or eliminating the weight given by courts to the location of an impugned intrusion in the analysis. In other words, the fact something happens in public space should only be one of many considerations in determining whether a plaintiff's privacy was violated, or is perhaps not relevant to the analysis at all.

Building upon these critiques, this chapter ultimately suggests that if the privacy torts are to truly address some of the privacy challenges raised by personal-use remote surveillance technologies, courts must go beyond just extending the current jurisprudence into public spaces. Courts will need to acknowledge and contend with the historical treatment of public space that has carried forward into the jurisprudence today. Otherwise, I suggest, the privacy torts will only be narrowly useful in public space, confined to occasions when an intrusion can replicate aspects of a private-property intrusion or violations of one's secrecy. Such torts would be of little use to mediating the kinds of privacy conflicts noted in this thesis, which would then leave those experiencing these kinds of collections/uses/disclosures of information without privacy recourse. This chapter and those that follow propose that public space location is in fact quite important to the privacy analysis. Courts need to better conceptualize the social value of public space, and the harms that flow from public

space surveillance, in the privacy tort analysis. Specifically, courts should place greater value on public space experience, and how this is shaped by (among other things) privacy and surveillance.

Academic Critiques of Canada's Privacy Torts

As noted, there are a range of academic critiques of the privacy torts in Canada. In particular, numerous authors have emphasized that it is problematic that the torts do not recognize privacy in public spaces. Many of these critiques focus on the ONCA decision in *Jones*. For instance, Professor Chris Hunt has written extensively about the common law intrusion upon seclusion tort, both before and after it was recognized.[354] In a critique of *Jones v Tsige*, he highlights three concerns with the tort as it was framed in the decision.[355] Overall, he is concerned that the ONCA uncritically adopted the US intrusion upon seclusion tort without dealing with some of its problems and weaknesses. First, he argues that the reliance on a requirement of "seclusion" in the application of the tort is problematic.[356] The requirement for "seclusion" assumes that people waive their right to privacy simply by leaving their secluded spaces (*e.g.*, by walking into public). As noted above, this reflects an all-or-nothing approach to privacy without considering other contextual factors at issue in a privacy dispute. This approach also fails to recognize any principled distinction between solely being seen by another person in public, and the technology-mediated production of a permanent record like a photograph or video of that which is seen in a public space.[357] Hunt is essentially arguing that the tort is too (arbitrarily or needlessly) narrow because it excludes privacy in public.

---

[354] See e.g., Chris DL Hunt "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37 Queen's LJ 167-219 (sets out some considerations for the development of the tort, including different theoretical definitions of privacy, and different philosophical approaches to justifying privacy protection).

[355] Chris DL Hunt "Privacy in the Common Law: A Critical Appraisal of the Ontario Court of Appeal's Decision in Jones v Tsige" (2011) 37 Queen's LJ 665-695 [Hunt, "Privacy in the Common Law"].

[356] Hunt, "Privacy in the Common Law", *ibid* at 673-674.

[357] Hunt, "Privacy in the Common Law", *ibid* at 675. Furthermore, this approach fails to consider how difficult it is to define when something is public, or private (or secluded), see e.g., Woodrow Hartzog, "The Public Information Fallacy" (2019) 98 Boston University Law Review 459 [Hartzog, "Public Information Fallacy"].

Hunt also highlights problems with the requirement that the intrusion must be into a plaintiff's "private affairs and concerns." He emphasizes that there is not a clear dividing line between "private affairs" and public affairs.[358] Courts should really be concerned with the normative, and not just the descriptive, status of the information. The underlying values of dignity, autonomy, and control of personal information identified by Sharpe JA would be better reflected through a normative approach.[359] A normative approach to the privacy assessment would consider what kind of privacy a plaintiff *should* be able to expect in their lives, not just what privacy they factually expect based on the kinds of surveillance they are subjected to in their daily lives. Courts should further avoid a categorical approach that pre-emptively lists which things and spaces are considered private, as this fails to reflect reality. What is private to one person might not be considered private to another.[360] He argues that seclusion or location should reflect only one non-exclusive consideration in a broader assessment of a plaintiff's reasonable expectation of privacy (REP).[361] This argument seeks to decenter the public/private binary in the application of the tort.

Hunt's third concern is with the "highly offensive" qualifier. He argues that this qualifier obscures the fact that the privacy interest is dignitary; in other words, the inclusion of the "highly offensive" requirement in the third element of the intrusion tort fails to recognize the invasion of privacy as a wrong in and of itself.[362] Instead, he suggests courts should treat offensiveness as one

---

[358] See also, Nicholas Blomely "Flowers in the Bathtub: Boundary Crossings at the Public-Private Divide" (2005) 36 Geoforum 281-296; Hartzog, "Public Information Fallacy", *ibid*.

[359] Hunt, "Privacy in the Common Law", *supra* note 355 at 681-684. On the falsity of a clear boundary between private and public see also Woodrow Hartzog, "The Public Information Fallacy" (2019) 99 Boston University Law Review 459-522; Nicholas Blomley, "Flowers in the Bathtub: Boundary Crossings at the Public-Private Divide" (2005) 36 Geoforum 281-296; Elizabeth Paton-Simpson, "Private Circles and Public Squares: Invasion of Privacy by the Publication of 'Private Facts'" (1998) 61(3) Modern Law Review 318.

[360] Hunt, "Privacy in the Common Law", *supra* note 355 at 684-685. See also NA Moreham, "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 Law Quarterly Review 628.

[361] This is similar to Professor Stuart Hargrave's concern as well, discussed below.

[362] Hunt, "Privacy in the Common Law", *supra* note 355 at 689-691. Hunt draws upon Moreham's work here, as she has also argued that this requirement puts the tort out of step with the other dignity-based torts like trespass to the person: NA Moreham, "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in J Finn & S Todd (eds), Law, Liberty and Legislation (Wellington, NZ: Lexis Nexis, 2008).

factor in the overall analysis, and not an independent requirement or element of the legal test. In other words, the court can still assess whether the invasion passes a seriousness threshold, but the impugned conduct does not necessarily need to cause distress as required by the "highly offensive" element - the tort is supposed to be actionable *per se*.[363] This argument targets concerns that courts might perceive impugned invasions as too small or insignificant to merit application of the tort, though cumulatively they may amount to a significant impact on privacy.

Hunt gives some broad suggestions for reform that are useful to the discussion of technology-mediated surveillance. Notably, he suggests that courts should adopt a more subjective-objective approach to assessing a plaintiff's expectation of privacy, similar to the approach taken by English courts.[364] Hunt argues that a better test would be to evaluate reasonableness from the plaintiff's perspective, and recognize the subjective nature of privacy, though with an objective element so that the tort does not become overly broad.[365] The English Test for Invasion of Privacy Tort is set out in *Murray v. Express Newspapers* where Lord Justice Clarke M.R. explains the test as follows:

> The first question is whether there is a reasonable expectation of privacy. This is of course an objective question . . . [But] the reasonable expectation [is] that of the person who is affected by the publicity . . . "The question is what a reasonable person of ordinary sensibilities would feel if she was placed in the same position as the claimant and faced with the same publicity". As we see it, the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include [1] the attributes of the claimant, [2] the nature of the activity in which the claimant was engaged, [3] the place at which it was happening, [4] the nature and purpose of the intrusion, [5] the absence of consent and whether it was known or could be inferred, [6] the effect on the claimant and [7] the circumstances in which

[363] Hunt, "Privacy in the Common Law", *supra* note 355 at 691.
[364] Others have suggested this too, see e.g., Sarit Mizrahi, "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?" (2018) 8 Western Journal of Legal Studies 3; but/and see Samuel Beswick and William Fotherby, "The Divergent Paths of Commonwealth Privacy Torts" (2018) 84 Supreme Court Law Review 225.
[365] Hunt, "Privacy in the Common Law," *supra* note 355 at 686. In fact, he suggests that Canadian courts would be better to follow England's developments rather than the US.

> and [8] the purposes for which the information came into the hands of the publisher.[366]

The more subjective approach has some important benefits, including directing decision-makers to consider how privacy can be experienced differently based on one's social location, and the dynamics between the parties in the dispute.[367] I argue below that Canada's own jurisprudence supports adopting such an approach within the scope of all of the privacy torts, not just intrusion upon seclusion.

Professor Stuart Hargreaves has also critiqued the US approach to invasion of privacy as too narrow, in particular due to the exclusion of matters that might be public or 'non-secret.'[368] He focuses on how the tort overly relies on a 'boundary' surrounding a private (protected) sphere. Distinguishing this from a public (unprotected) sphere narrows the tort such that it fails to address many invasions of privacy that occur outside a private, protected sphere.[369] He draws on feminist writing on autonomy, and particularly professor Jennifer Nedelsky's work on relationality, to argue for a 'relational' approach to privacy, emphasizing the important social dimensions of privacy, including that it enhances social relations.[370] He explains that under such an approach,

---

[366] *Murray v. Express Newspapers* [2008] EWCA Civ 446, [2009] Ch 481 at para 36 (involving an action in privacy after photographs were covertly taken of JK Rowling's toddlers while out on a public street).
[367] See also Thomasen & Dunn, "Reasonable Expectations of Privacy", *supra* note 154. Hunt also argues that the courts should not treat disclosure of private facts and intrusion as separate torts, they should be treated as one given the fluidity between the physical and informational aspects of privacy: "Privacy in the Common Law", *supra* note 355 at 668-69. However, while there is good reasoning behind this argument, there is also a compelling reason to recognize the difference between an *intrusion* of privacy, which may or may not include the collection of the information, and the subsequent use and *disclosure* of that information. Each event can have an impact (perhaps a different impact) on the targeted individual, which might vary in severity and scope depending on the circumstances. There may be greater appeasement for the global harm by recognizing each of these separate injurious actions by the defendant.
[368] Stuart Hargreaves, "'Relational Privacy' & Tort" (2017) 23(3) William & Mary Journal of Women & the Law 433 [Hargreaves, "Relational Privacy"].
[369] Hargreaves, "Relational Privacy", *ibid* at 436-444 (referring specifically to Canada's torts, in particular intrusion upon seclusion in Ontario and the provincial statutory torts at 441-553).
[370] Hargreaves, "Relational Privacy", *ibid* at 456-59, referring to Jennifer Nedelsky, *Law's Relations: A Relational Theory of Self, Autonomy, and Law* (Oxford University Press, New York: 2011), challenging the notion that one experiences a solitary form of autonomy, and instead recognizing the social and relational nature of autonomy, and one's reliance on others to become their own self. See also for example Waldman, *Privacy as Trust*, *supra* note 43 on the relational and social dimensions of privacy interests.

> a privacy loss would be understood as an unwanted reduction in the ability of an individual to negotiate their 'distance' between themselves and other social actors … a legally actionable privacy loss would be one that is so significant that it harms an individual's capacity for autonomy, understood from the relational perspective.[371]

In other words, privacy harm is that which damages one's autonomy in relations and/or ability to relate to others; a type of harm that can certainly be engaged in public space or publicly available information.

Hargreaves uses this approach to call for a move away from a location-based analysis to one that focuses on the harm to the plaintiff – location could be a factor in the analysis, but should not be exhaustive.[372] While I actually suggest in the next chapter that courts need to better recognize the importance of public space in the analysis, Hargreaves's call for an increased focus on the harm to, and the effect of a violation of privacy on, individual autonomy is helpful. The idea that privacy promotes social cohesion, relationality, and community involvement through autonomy actually signals something especially important for public spaces. The ability to operate free from pervasive scrutiny and surveillance in public spaces can also contribute to the experience of these important social values. Public spaces may offer a physical location where the value of privacy can be experienced when engaging with others. I elaborate on this idea of public space coinciding with important social and relational values in the next chapter.[373]

The intrusion upon seclusion tort is also narrowed by the cap on the amount of non-pecuniary damages a plaintiff can seek. Omar Ha-Redeye has argued that the court's indication that

---

[371] Hargreaves, "Relational Privacy", *supra* note 368 at 463.
[372] Hargreaves, "Relational Privacy", *ibid* at 464.
[373] Hargreaves has also noted the limited application of the privacy torts, particularly intrusion upon seclusion under *Jones*, in the context of commercial street surveillance, like Google Street View. Stuart Hargreaves, "'Jones-ing' for a Solution: Commercial Street Surveillance and Privacy Torts in Canada" (2014) 3(3) *Laws* 388-409. See also Hargraeves' chapter, "'I'm a Creep, I'm a Weirdo': Street Photography in the Service of the Male Gaze" in Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops (eds) *Surveillance, Privacy, and Public Space* (Routledge Studies in Surveillance Book Series: 2018) in which he emphasizes that collection and sharing of sexual images taken from public spaces goes beyond just individual privacy invasions, engaging gendered harms that are systemic and thus need a more systemic or norm-shifting solution. In this thesis, I view tort law reform as but one area in which social norms may be shifted.

damages for the tort of intrusion would be modest raises concerns about the tort's practical significance in litigation.[374] Though he suggests that the subsequent use of this tort in class actions has "put this concern to rest," since the aggregation of awards makes pursuit of a claim more financially feasible.[375] The potential for class actions aside, though, his concerns remain pertinent with respect to the practical application of the tort in contexts where there might not be a class or where a class action is not practical. Furthermore, while a class action can have a significant impact on a defendant ordered to pay a large sum in damages, each individual plaintiff remains capped in their non-pecuniary damages, so the individual concerns about the impact of the cap remain.

Sarit Mizrahi has also argued that the intrusion tort set out in *Jones*, as well as the common law tort of publication of a private fact, may both be too narrow to address emerging challenges from new technology.[376] She focuses specifically on digital information collection and 'dataveillance,' particularly by companies, and as engaged by hackers that take advantage of security weaknesses in technological systems. In regard to the common law torts, she argues that the "highly offensive" requirement needs to be clarified and, like Hunt, suggests reference to the English approach to assessing expectations of privacy, which includes greater recognition of the subjective perspectives of the plaintiff.[377]

These critiques align with numerous critiques of the US torts (on which Canada's common law torts are based, and which have at least influenced the interpretation of the statutory torts) for

---

374 Omar Ha-Redeye, "Class Action Intrusions: A Development in Privacy Rights or an Indeterminate Liability" (2015) 6(1) Western Journal of Legal Studies 1 [Ha-Redeye, "Class Action Intrusions"].
375 Ha-Redeye, "Class Action Intrusions" at 1-2.
376 Sarit K Mizrahi, "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?" (2018) 8 Western Journal of Legal Studies 3 carries out a doctrinal application of the two Ontario torts to 'internet of things' technologies. Mizrahi argues that some privacy intrusions based on IoT may not be caught due to requirements of the torts, but recognizes the courts could extend the scope of the tort to address some of these issues.
377 Emily Laidlaw also argues that the current privacy torts in Canada are insufficient to address a range of technology-mediated privacy abuses, and thus calls for a technology-mindful judicial analysis of expectations of privacy under the tort. Emily Laidlaw, "Technological Mindfulness and the Future of the Tort of Privacy" (draft on file with author) forthcoming.

being too narrow. For example, with regard to the application of intrusion upon seclusion in public space, Professor Andrew Jay McClurg has argued for a right of "public privacy" that would allow recovery for highly offensive instances of public intrusion.[378] The US intrusion tort in almost all cases does not protect people in places that are accessible to other members of the public.[379] He argues that this interpretation does not necessarily arise because of the elements of the intrusion upon seclusion tort, but rather because the courts have uncritically accepted Prosser's commentary about the tort. Prosser provides commentary in the US Restatement of Tort, that "on the public street, or in any other public place, the plaintiff has no right to be alone, and it is no intrusion of his privacy to do no more than follow him about [or take his photograph]."[380]

Based on the elements of the intrusion tort alone, without Prosser's commentary, intrusion into "private affairs or concerns" could be construed to include public space intrusions.[381] McClurg proposes a redefinition of the tort that omits reference to "solitude or seclusion" (which aligns with Hunt's critiques of the Ontario tort as well), and makes clear that an intrusion can occur in public.[382] McClurg is not arguing for a complete rethinking of the tort, but rather an expansion of its interpretation to explicitly include public space. Professor Danielle Citron has also emphasized the ways in which Prosser narrowed the interpretation of privacy within his characterization and commentary on the tort, suggesting that an approach that turns back to the "right to be left alone"

---

[378] Andrew Jay McClurg "Bringing Privacy Law Out of the Closet: A Tort Theory for Intrusions in Public Places" (1995) 73 North Carolina Law Review 9 [McClurg, "Intrusions in Public Places"].
[379] McClurg, "Intrusions in Public Places", *ibid* at 991.
[380] McClurg, "Intrusions in Public Places", *ibid* at 1025 citing Prosser, "Privacy", *supra* note 163 at 391-92.
[381] McClurg, "Intrusions in Public Places", *ibid* at 1055.
[382] McClurg, "Intrusions in Public Places", *ibid* at 1058-59: He suggests seven factors for evaluating when a defendant's conduct is highly offensive to the reasonable person (drawing factors from the public disclosure of private facts tort): the defendant's motive; magnitude of the intrusion; whether the plaintiff could reasonably expect to be free from such conduct under the habits and customs of the location where it occurred (i.e. location here is relevant, but not determinative); whether the defendant sought the plaintiff's consent; actions by the plaintiff that a reasonable person would take to manifest a desire for the defendant not to engage in the intrusive conduct; whether the defendant disseminated the images/information obtained from the intrusion; whether the images/information involve a matter of legitimate public interest.

would allow for a broader interpretation and application of the torts, more in line with modern technologies and norms.[383]

Ultimately these critiques all highlight an important observation about the current interpretation of the privacy torts, that it is not inevitable that the torts be interpreted in such a way as to exclude interactions in public space. These authors emphasize that such an interpretation leads to an unhelpful and unnecessary narrowing of the application of the privacy torts. These critiques offer useful avenues for reform of the torts so that they might better respond to people's real experiences, including in public, particularly in reaction to increasingly pervasive technological surveillance. They propose different approaches to incorporate public space into the scope of the tort, including minimizing the importance of space in the legal analysis (*e.g.*, make it one of many variables and not a determinative variable), and/or to adopt more flexible theoretical approaches to understanding privacy (*e.g.*, as an interactive, relational concept rather than an all-or-nothing concept premised on seclusion from society). In other words, many of the academic critiques note ways to extend the existing tort protections into public space through greater nuancing of the judicial assessment of whether the plaintiff could reasonably expect privacy in their circumstances, while minimizing the negative impact of the plaintiff's public space location on the analysis.

In the sections that follow, I seek to contribute a further consideration into this literature. While these critiques aim to extend the torts into public spaces, they often do so while still accepting (or without explicitly challenging) the legal treatment of a plaintiff's public space location as a "negative" in the reasonable expectation of privacy analysis. Generally, these critiques accept that being in public might lower one's privacy expectations, but argue this should not eliminate privacy all together. Based on the examinations that follow, I propose a rethinking of the way in which a

[383] Danielle Keats Citron, "Mainstreaming Privacy Torts" (2010) 98 California Law Review 1805-1852 [Citron, "Privacy Torts"].

plaintiff's public space location affects the legal analysis. Instead of inherently counting as a negative (i.e., lowering one's expectation of privacy) courts ought to recognize the important *value* of being in public spaces within the tort analysis. In other words, one's public space location could actually raise important favourable considerations for the expectation of privacy analysis. Furthermore, privacy engaging conduct in public spaces can raise important public interest considerations in the value of public and shared spaces, and the ways in which privacy can enhance such value.

This treatment of public space location as a "negative" in the court's privacy analysis stems from a historical trajectory within the US privacy torts that has been imported into the Canadian doctrine without, as Hunt highlights, sufficient thoughtfulness. Academic work examined below shows that this trajectory grows out of substantive inequalities embedded in property, which conflict with various Canadian *Charter* and social values. The next section explains this historical trajectory through reference to cases and academic writing. Chapters 5 and 6 examine how this doctrinal trajectory can shift within the Canadian privacy torts. By considering theoretical grounding for an understanding of the *value* of public space in the privacy analysis, and by examining the jurisprudential reasons Canadian tort law can and should evolve away from the negative assumptions about public space location, the remaining Chapters argue for reform that could render the privacy torts more relevant to technology-mediated public space privacy conflicts.

Tort Protection of the Notion of 'Home as a Man's Castle'

The absence of legal protection for privacy in public spaces has historically existed as a counter-point to the significant legal protection afforded to privacy in private or secluded spaces.[384] The association of privacy with the private sphere of home and family life, away from or separate from

[384] E.g., Joel Reidenberg, "Privacy in Public" (2014) 69 U Miami Law Review 141 [Reidenberg, "Privacy in Public"].

the public, stems back to ancient Greek and Roman influence.[385] Early understandings of privacy reflect a conceptual mutually-exclusive division between the spheres of one's life – one's private life is archetypically defined by the home and protected from the public sphere, which by contrast is where one engages in society, politics, *etc*, sometimes physically understood as public space.[386] The subsequent consideration of privacy in public space is not meant to undermine the protection of one's private life against incursions by the state or public realm. Instead, the discussion supporting public space privacy here seeks to bring aspects of public space experience *up to* the level of legal importance assigned to the private home. The subsequent discussion is also not challenging this distinction between private and public life *per se*[387] – there is social and legal relevance in understanding these as different aspects of one's life. Rather the below discussion challenges the notion that privacy rights cannot be found in public life, or that being in public disallows privacy rights and compensation for their violation.

The more contemporary understanding of this distinction between public and private is reflected in tort law, in particular emerging through the legal maxim that a home is a "man's castle." This maxim understands home as a protected space where one can escape from the chaos, threats, and pressures of public life. The development of this maxim, particularly in its earlier iterations, emphasizes the importance of legal protection of the home *against* the prying eyes of the public. It

---

[385] Arendt, Hannah *The Human Condition* (Chicago: Univ. of Chicago Press, 1958) Chapter II "The Public and the Private Realm" pp. 22-78; for its understanding in the French Old Regime and revolution see: Dena Goodman, "Public Sphere and Private Life: Toward a Synthesis of Current Historiographical Approaches to the Old Regime" (1992) 31 History and Theory 1.

[386] See Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, translated by Thomas Burger & Frederick Lawrence (Cambridge: MIT Press 1989).

[387] Notably though, the distinction between these spheres of life is not clear cut and may shift depending on the circumstances. See for example: Hartzog, "Public Information Fallacy", supra note 357; Nicholas Blomely, "Flowers in the Bathtub: Boundary Crossings at the Public-Private Divide" (2005) 36 Geoforum 281-296.

reinforces a spatial and value-based binary wherein the home is a safe space away from the dangers of the public space; where public visibility is the negative, to the positive of the home's seclusion.[388]

Early History of the 'Home as a Castle' Maxim

The judicial notion that a man's home is his "castle" is typically attributed at its earliest to the seventeenth century English common law decision in *Semayne's Case*.[389] Sir Edward Coke wrote in the decision that: "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose."[390] This decision grounded subsequent case law in England, and extending to the US and Canada, on warrant requirements for state entry into someone's private home. The concept and phrasing of a 'man's castle' evolved through various iterations in 17th and 18th century English law. This includes for example being famously spoken by William Pitt, 1st Earl of Chatham in English Parliament:

> The poorest man may, in his cottage, bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; but all his force dares not cross the threshold of the ruined tenement.[391]

It also grounded the foundational English warrant (and privacy) case *Entick v Carrington*.[392] The court in *Entick* forbade warrantless entry into one's home, which was adopted favourably in the US as well including in relation to constitutional privacy protections.[393] The notion of a home as a 'man's castle' is so common now as to be considered a common law maxim.[394] The

---

388 Reidenberg, "Privacy in Public", *supra* note 384; Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale Law Journal 421.
389 *Semayne's Case* (January 1, 1604) 5 Coke Rep. 91. Adopted explicitly in Canada, for example *Colet v The Queen*, 1981 CanLII 11 (SCC), [1981] 1 SCR 2.
390 77 Eng. Rep. 195. In this case a sheriff sought to enter a debtor's house, and the court determined that before an officer can enter there must be a warning.
391 William Pitt, March 1763, Speech in Response to *Cider Bill*, 1763.
392 *Entick v Carrington*, [1765] EWHC KB J98.
393 E.g., G. Robert Blakey, "The Rule of Announcement and Unlawful Entry: Miller v. United States and Ker v. California" (1964) 112 University of Pennsylvania Law Review 499.
394 H. Broom & R.H. Kersley, *Broom's Legal Maxims,* 10th ed (London: Sweet & Maxwell, 1929) at 281.

quote from Pitt, above, emphasizes another important aspect about the doctrine – it was meant to be 'equitable.' Equitable in that context was limited by the social dynamics of the times, such that only certain members of society had access to the ownership and control of a home and could benefit from such legal protection, or could experience repose within the home. Nevertheless, it is worth noting that in its earliest formulation, the notion of strong legal protection of one's "repose" and freedom from "violence" was meant to be available to all.[395]

Adoption of the Maxim in Tort and Other Areas of Law

Since its early inception, the 'man's castle' has become one of the most deeply rooted legal maxims in Anglo-American jurisprudence as well.[396] It grounds, among other things, Fourth Amendment jurisprudence in the US, as well as the privacy tort doctrine. Warren and Brandeis' influential article "The Right to Privacy" reasserts that "the common law has always recognized a man's house as his castle" in an argument that tort law needs to better protect those privacy interests of the home, lest courts "open wide the back door to idle or prurient curiosity."[397] Their concern was with media access to the ongoings of the home. This article, followed by Prosser's compiling of privacy tort cases emerging over the years in between, laid the foundation for the US privacy torts, which have since influenced the Canadian torts.

It is also no coincidence that the maxim refers to "man's" castle. The conceptualization of the home and how it is protected in law has always been circumstantial. Professor Jonathan Hafetz has examined the US history of the maxim and demonstrated through various examples how the "interplay of social factors such as gender, class, and race have helped shape legal doctrines affecting

---

[395] *Semayne's Case*, *supra* note 389.
[396] Jonathan L Hafetz, ""A Man's Home is his Castle?": Reflections on Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries" (2002) 8:2 William & Mary Journal of Women and the Law 175 at 175 [Hafetz, "Castle"].
[397] Warren & Brandeis, "Right to Privacy", *supra* note 288.

the home and influenced the home's treatment by courts, legislatures, public officials, and private agencies."[398] He examines the US legal treatment of the home from the 1870s through the 1920s. Through examples contrasting the strong protection of the home for middle/upper class property owners, where the law aimed to protect the *privacy* of the home over the interests of predominantly women and children who might experience domestic abuse and violence within the home, with the state's willingness and legal power to intrude into homes of single mothers receiving social assistance, in cases of child removal from the family, and in shared boarding houses, Hafetz underscores how the court's willingness to protect the home is not absolute and is always contextual. Race, gender, and class play intersecting roles in this context, wherein immigrant and racialized poor families and mothers more commonly experienced intrusive warrantless entries, benefiting far less from the maxim than white middle- and upper-class families do.[399] Ultimately, it is not the home as a physical structure that is protected in law and through this maxim, but certain interests associated with the home that might be more readily asserted by those with more privilege.

Hafetz further draws out the connection between the home and the judicial conceptualization of privacy specifically. Judicial decisions like *Entick v Carrington* and *Wilkes v Wood* from England, and the *Boston Writs of Assistance Case* in the US "not only solidified the link between the home and common law trespass, but also tied the home to domestic privacy and harmony."[400] This early US idea of the home as a tranquil safe place of freedom and privacy - for some - is reflected for example by John Adams:

> Every English[man] ... takes a Pride and he glories justly in that strong Protection, that sweet Security, that delightful tranquility which the Laws have thus secured to him in his own House ... [and to deprive him of this

[398] Hafetz, "Castle", *supra* note 396 at 177.
[399] See also Eden Osucha's discussion of the racial dynamics underlying the development of the appropriation tort: "The Whiteness of Privacy: Race, Media, Law" (2009) 24 Camera Obscura 1-70.
[400] Hafetz, "Castle", *supra* note 396 at 183.

> would be to treat him] not like an Englishman, not like a Freeman but like a slave.[401]

Hafetz explains how the legal protection of the home developed to respond to men's Victorian era concerns around reputation and status, as reflected in the early development of the privacy torts.[402] As Hafetz explains,

> In creating a new protective sphere around the privacy of domestic relations, courts, while speaking in formal, neutral terms, acted to shield middle- and upper-class men from risking the *evils of publicity* merely for the inevitable "frailties of [their] nature" and "the mysteries of [human] passion."[403]

Home is the castle which protects privileged people from publicity and the public sphere – pitting the home against the public in the judicial mindset.

As introduced above, these concerns regarding publicity, reputation, and the home's protection are echoed throughout Warren and Brandeis' influential piece, and their notion of the "right to be left alone." Professor Anita Allen and co-author Erin Mack explain how this historical protection of not the home *per se*, but rather the interests in seclusion, modesty, and reputation that came with shelter within the home translate to the early courts' reluctance to recognize privacy in public spaces in tort. Through an examination of early developments of the US privacy torts, as well as Samuel Warren and Louis Brandeis' famous paper "The Right to Privacy",[404] Allen and Mack identify "outmoded normative assumptions about female modesty and seclusion" at the heart of the tort's

---

401 Hafetz, "Castle", *ibid* at 183 – quoting John Adams' notes for his argument in the 1774 case *King v. Stewart*, in 1 Legal Papers of John Adams 137 (L Kinvin Wroth & Hiller B. Zobel eds, 1965).

402 "This fear of public shame and harm to reputation resonates with social concerns about manners, status, and the proper code of behavior for a gentleman. Similar concerns about protecting against a loss of privacy at the hands of the emerging mass media of newspapers would eventually lead to the development of an independent privacy tort." Hafetz, "Castle", *supra* note 396 at 188.

403 Hafetz, "Castle", *ibid* at 188, emphasis added.

404 Warren & Brandeis, "Right to Privacy", *supra* note 288; "Warren and Brandeis were not critical of the ways in which homelife […] and norms of female modesty contributed to women's lacking autonomous decision making and meaningful forms of individual privacy." Anita Allen & Erin Mack "How privacy Got its Gender" (1991) 10 Northern Illinois University Law Review 441 at 477 [Allen & Mack, "How Privacy got its Gender"].

emergence as legal protection against unwanted publicity.[405] Early privacy torts reflect a requirement for a "strict adherence to a social standard of female seclusion and modesty."[406] Allen and Mack point out,

> Middle-class white women often had a great deal of privacy, in the sense of socially imposed isolation within a private household. However, across races and classes, women were seldom heads of households, had little time to themselves, and had little of the legal autonomy concerning sexuality, marriage, and the family that sometimes is called "decisional privacy" today.

Women continued to lack access to a range of privacy interests that are not predicated on seclusion within a private residence - decisional autonomy, particularly over marriage, reproduction and sex, (which were traditionally seen as part of "family life", over which men had decision-making authority), as well as the ability to seek replenishing solitude outside the confines of the home.[407] The public realm, as Allen elsewhere describes, can be a place of private tasks, where people, especially anyone who lacks access to privacy within a private residence, can alleviate or escape the stresses of home or employment.[408]

Yet privacy intrusions that occur in public spaces are often unacknowledged or unprotected in law because of this seclusion and modesty-based understanding of privacy. Allen cites the example of street harassment that can "break the flow of thought and distract a woman's attention, utterly without purpose, from her own concerns."[409] Private tasks and repose are replaced with

---

[405] For instance, Warren and Brandeis cite a line of privacy cases in which fathers and husbands were recognized as having rights of recovery against male seducers of their daughters and wives as a reflection of the principle of non-interference with a man's family relations. "Typical judges were likely to be strongly influenced by pervasive notions of a need to take special care to preserve women's modesty as among their chief virtues." Allen and Mack "How Privacy Got its Gender", *ibid* at 442, 462-464, 458.

[406] Allen and Mack, "How Privacy Got its Gender", *supra* note 404 at 454.

[407] "Seclusion, achieved through physical distancing, and anonymity, achieved through limited attention paid, are the forms of inaccessibility that significantly constitute privacy in public" Anita Allen *Uneasy Access: Privacy for Women in a Free Society* (Totawa, New Jersey: Rowan & Littlefield 1988) at 123-24 [Allen, *Uneasy Access*].

[408] Allen defined "privacy in public" as the "inaccessibility of persons, their mental states, and information about them to the senses and surveillance devices of others." *Uneasy Access, ibid* at 123.

[409] Allen, *Uneasy Access, ibid* at 128.

experiences of leering, insulting, prying and offensive touching.[410] These unwanted intrusions have the effect (if not the intention) of silencing, intimidating, and objectifying people who experience harassment when they enter public space, often with little legal or normative recourse.[411] Viewed individually, these privacy invasions can sometimes seem *de minimis*, and perhaps for this reason receive little or no legal protection.[412] But when their frequency is considered, the impact of this privacy invasion has a cumulative effect.[413] Personal use surveillance technologies not only threaten to increase the quantity of such invasions, but also to potentially streamline the amalgamation of small instances, and/or the sharing of information across neighbourhoods and other communities. The early jurisprudence did not recognize any such privacy interests in public space, unless they could be framed within the scope of modesty and seclusion, which was difficult to do once a woman exposed herself to the public sphere.[414] The tort was not developed to address the concerns of people who might seek privacy in public space, either because they lack privacy in private, or because they lack access to private space all together.

Home as a Man's Castle in Canada

The notion that a home is a man's castle is present as a colonial narrative in Canadian legal doctrine, too, similarly encompassing the notion of the home as keeping the public/others out and keeping those within the home safe. For example, Professors Gina Starblanket and Dallas Hunt have unpacked the narratives upholding the notion of the home as a castle in the context of the trial

---

[410] Allen, *Uneasy Access, ibid* at 128. This does not include such encounters as striking up a conversation or flirtation: "The privacy-diminishing intrusions that are to be condemned as morally disrespectful and harmful have little to do with genuine personal interest in the women who are victimized" Allen, *Uneasy Access* at 133.
[411] Allen, *Uneasy Access, supra* note 407 at 131: Women do not enjoy the same privacy in public as men do.
[412] Allen, *Uneasy Access, ibid*; Cynthia Grant Bowman, "Street Harassment and the Informal Ghettoization of Women" (1993) 106 Harvard Law Review 517.
[413] Allen, *Uneasy Access*; see also Jena McGill and Ian Kerr, "Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" in *Digital Enlightenment Yearbook* (IOS Press, 2012) on the problem of reviewing a series of small privacy invasions independently, rather than as a whole.
[414] Allen and Mack, "How Privacy Got its Gender", *supra* note 404 at 453.

of Gerald Stanley for the shooting and killing of Colten Boushie. They examine the colonial legacies in Canada of "settler entitlement to property, to space, to a life free of the 'terror' occasioned by Indigenous presence."[415] Stanley was charged with murder and manslaughter after he shot and killed Colten Boushie, a 22-year-old Indigenous man from the Cree Red Pheasant Nation, at Stanley's farm in Saskatchewan. While defence of property was not raised at trial (Canada does not have a formal 'castle doctrine' in criminal law that allows for defence of property with lethal force), the defence arguments repeatedly invoked the notion of the home/farm as a castle, as an explanation for Stanley's state of mind. For instance, Stanley's lawyer Scott Spencer, argued:

> This is really not a murder case at all. This is a case about what can go terribly wrong when you create a situation which is really in the nature of a home invasion. For farm people, your **yard is your castle**. And that's part of the story here.[416]

Starblanket and Hunt explain, "What should not be lost here is how castles (and now farms) have served as sites of capitalist accumulation and protectionism, as romanticized spaces wherein heroic kings protect against incursion from hostile outside forces."[417] The trial defence evoked this notion that home as castle is as much about protecting what's inside as it is about keeping the public (perceived as dangerous) away. As they further explain,

> Castles evoke mental portraits of fortresses besieged, of hordes of enemies attempting to crash the gates of the wealthy, aristocratic, and ultimately armed gentry defending themselves against blood-thirsty intruders outside their walls and beyond their moats. These, no doubt, are the images and representations [Stanley's defence lawyer] Spencer hoped to cultivate in the

[415] Starblanket & Hunt, *Storying Violence, supra* note 138 at 15. See also: Rinaldo Walcott, *On Property* (Biblioasis, Windsor, ON: 2021) [Walcott, *On Property*]; Brenna Bhandar, *Colonial Lives of Property*: Law, Land, and Racial Regimes of Ownership (Duke University Press, Durham NC: 2018) on the ways in which colonial appropriation of Indigenous lands draws on European notions of white supremacy and associations between property and a civilized life, which are very much echoed in the home as a man's castle metaphor; Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, Durham NC: 2015) in which Browne demonstrates (among other things) how modern surveillance technologies and practices are informed by the policing of Black life and Blackness under slavery in the US.
[416] Starblanket and Hunt, *Storying Violence, ibid* at 84, citing *R v Stanley*, 2018, 607, emphasis added.
[417] Starblanket and Hunt, *Storying Violence, ibid* at 86.

> minds of those sympathetic to or willing to entertain the idea of Stanley's innocence.[418]

In other words, it was conveyed as acceptable that Stanley was in a frenzied state of mind when he shot Mr. Boushie because of the fear he felt at his property being intruded upon. The defence arguments were accepted by the all-white jury who acquitted Stanley. The maxim persists in the Canadian legal system too, where it intersects with the ongoing history of colonialism in Canada. The maxim of home as a man's castle has also been accepted elsewhere in criminal law.[419]

While Canadian tort law does not explicitly rely on the maxim in its contemporary legal tests, as the concept grounded the US doctrine which in turn has grounded the development of the Canadian privacy torts, its legacy – pitting private against public – remains. For instance, in *Zeliony v Dunn* (the Manitoba case where the plaintiff claimed a privacy violation in response to her neighbour's use of an Amazon Ring device), the camera was installed to protect personal property, and observed the shared hallway (not 'public space' as I define in this thesis, but a relevant approximate for this point). It is clear from the judgment that there was tension between the parties that escalated over a period of time. Nevertheless, while the plaintiff expressed such discomfort with the filming that, according to the brief facts, she moved away from her home so as to avoid that shared space, the court held that because the hallway was shared space and because the defendant was protecting his property, this was not an invasion of her privacy. This is despite the impact that daily surveillance might have on one's experience of coming and going from their home. In this case, the perpetual presence of the surveillance camera (made possible because of its remote

---

[418] Starblanket and Hunt, *Storying Violence, supra* note 138 at 87.
[419] See e.g., *R v Colet*, [1981] 1 SCR 2 (owner refusing entry of police onto his property); see also, e.g., Beverly Balos, "A Man's Home is his Castle: How the Law Shelters Domestic Violence and Sexual Harassment" (2004) 23 St. Louis University Public Law Review 77.

operation) rendered it seemingly impossible for the plaintiff to freely use the shared entryway to her home.

To be clear, I am not proposing that every instance of interpersonal surveillance should be actionable in tort, or even that the occurrence in *Zeliony* must have been actionable (though I discuss this decision at greater length in Chapter 6). Rather, what I am suggesting is that the courts are approaching the analysis of the plaintiff's claim through the wrong legal lens. The courts are continuing to operate from a "man's castle" perspective on public space privacy claims, wherein there is no privacy in public; and the home (or another secluded place over which the plaintiff has some control) is *the* place for protection from publicity and repose, which can also be protected from the public sphere. These themes emerge from *Zeliony* in regard to home surveillance systems, and the diminished relevance of the current privacy torts in response to most drone filming in public spaces, given the lack of privacy recognized in public spaces.[420] In the chapters that follow, I suggest that courts need to adopt a different way of understanding privacy in public within the scope of the privacy torts. Courts should not simply extend the modesty or seclusion values of privacy into some circumstances in public space.[421] Rather, the legal analysis should start from the foundation that public space is socially valuable, and that privacy in public allows for and supports human experiences in public space. A privacy violation in public space might involve conduct (collection, use, disclosure of information or an intrusion) that undermines one's ability to access this public

[420] Thomasen, "Beyond Airspace Safety", *supra* note 4.

[421] As has been the case with, for example, "upskirting" where someone uses a camera on a shoe or otherwise low to the ground to photograph up someone's skirt. This is a clear violation of privacy. But basing the analysis for why this is a violation on a theory of seclusion (e.g., despite being in a public space, the photograph reveals what is meant to be covered up), would leave individuals without remedy for similarly abusive photography of parts of their bodies that are not covered up. This is exemplified in the ONCA decision in *Jarvis* where the court held that because students' chests were not covered, their teacher did not violate their privacy when taking covert sexual photographs of them. The reason public space upskirting should be seen as a violation of privacy is because it amounts to an attack on the equal right to exist in public space free from harassment and technology-facilitated surveillance. Upskirting dissuades people, especially women, away from existing in public space and forces them to change their behaviour when entering shared space, which compromises their experience of being in a social space, and which compromises the integrity of public space as an open and accessible space. See Chapters 5 and 6 for elaboration of this discussion.

space. In such a framing, the plaintiff would not have to prove to the court that they were secluded despite being in public. The plaintiff could be fully visible and depending on the circumstances still have a legitimate claim to privacy because the surveillance they are facing undermines the values of that space – not unlike how a violation of seclusion or unwanted publicity undermine the values of private space as discussed above. I explain this idea of public space privacy further in the next Chapter.

Chapter 5 – Law, Technology, and Space: Public Space Privacy Harms

Tort law compensates for legally recognized harm. Harm under the privacy torts has been understood as a violation of one's privacy in the statutes, or as an intrusion upon seclusion, publication of a private fact, or putting a plaintiff in a false light in the common law in some provinces. Under each privacy tort, the court has developed an analytical framework for assessing when something is "private," such that its violation or revelation amounts to a compensable harm. This analytical framework considers whether the plaintiff could have a "reasonable expectation" that the thing or conduct at issue was "private." Through Chapters 3 and 4 I have sought to understand how the courts approach this analysis, and have identified that a key variable for the courts when deciding if something is "private" is whether it was concealed within private space/property. In other words, the courts have so far determined that a person cannot experience compensable privacy harm if they are in public space. However, as noted in Chapter 3, there is no explicit requirement in the statutes or in the elements of the common law torts that inherently excludes public space from the scope of the privacy torts.[422] This exclusion has largely been the result of judicial interpretation, which arose from a trajectory of jurisprudence dating back to the early US foundations of the torts.

In the chapters that follow, I propose a reimagining of this "reasonable expectation of privacy" analysis that not only includes, but values, conduct and social interactions in public spaces. The following chapters make practical proposals for reform on the basis of existing jurisprudence, which I argue has been overlooked by the courts. But first, this chapter provides a theoretical grounding for the proposed reforms.

[422] See also Danielle Citron, "Privacy Torts" *supra* note 383.

In this chapter, I draw on privacy scholarship that seeks to understand the notion of privacy harm, and particularly, public space privacy harm. Read together, the theory examined below supports a recognition of a socio-spatial privacy harm that arises from a loss of public space as a result of intentional surveillance. I suggest that this conceptual loss of public space through a privacy violation can amount to a privacy harm that comes within the scope of the torts, and provide a grounding for courts when assessing whether a plaintiff may have a "reasonable expectation of privacy" even when entirely visible in a public space.

First, I outline theoretical work that has been done to conceptualize privacy as a social value – in particular, as a value that supports and underscores social relations. This theoretical work supports the notion that privacy is important to public space, as a space of necessary and sometimes unavoidable social interaction. Next, I draw upon the writing of scholars who have sought to articulate spatial privacy harms that occur in public space, in particular Julie Cohen and Hille Koskela, to make a case for a public space privacy harm that should be recognized in tort law. I draw on some of Cohen's articulation that there can be such a thing as a spatial privacy harm. I also build on this with Koskela's explanation for how technology is specifically relevant to this spatial harm (something that Cohen has also argued). I return to Cohen's work, as well as that of Ryan Calo and other privacy scholars to explain the dimensions of that harm and why it can occur even without a defendant present at the time of an intrusion. Finally, I connect this theoretical grounding back to the social dimensions of privacy, and draw upon scholarship from Law & Geography to explain why legal recognition of privacy in public space is important and necessary to support any notion of public space as an open and equitable social space. The next chapter then considers why such a harm can and ought to be recognized in the Canadian privacy torts. The conclusion identifies several reforms to the privacy torts that would allow for such a recognition.

Privacy as a Social Value

Much of the 19th and early 20th century philosophical and legal thinking about privacy was focused on its individual value – promoting personal autonomy, seclusion, isolation from others, a right to be left alone.[423] Through the late 20th and into the 21st century, scholars have challenged this liberal individualistic notion of privacy and laid theoretical groundings for recognizing privacy's social importance.[424] The privacy torts emerged in the earlier individual-focused context. I will argue through the remaining chapters that in the context of social, technical, and jurisprudential change that has occurred since that time, the torts require reform that reflects the theoretical grounding that privacy is also a social value – supporting social relations, and benefiting society as a whole.[425]

Referring to privacy as a 'social value' can have two different and interrelated meanings.[426] Privacy is a social value in that its recognition and protection at an individual-level also benefits society more generally.[427] Priscilla Reagan for instance has highlighted at least three ways in which privacy's value can be understood as a common good, and not as a strictly individual-benefit. Privacy is a common value, in the sense that people (at least within the US/North American western context she writes in) generally agree that there is some concept of privacy and it is important, even if they have different understandings of the boundaries of privacy. Privacy is also a public value in the sense that it is important to public and political processes – for instance she argues it preserves the democratic process by limiting the use of personal information for direct political advertising, which

---

[423] See the comprehensive literature review in Waldman, *Privacy as Trust, supra* note 43; Priscilla Reagan, "Privacy and the Common Good: Revisited" in Social Dimensions of Privacy, Beate Roessler and Dorota Mokrosinska (eds) (Cambridge: Cambridge University Press, 2015) at 50 [Reagan, "Common Good"]; Priscilla Reagan, Legislating Privacy: Technology, Social Values, and Public Policy (Chapel Hill: University of North Carolina Press, 1995) [Reagan, *Legislating Privacy*]

[424] See e.g., Reagan, *Legislating Privacy, ibid*; Robert C. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 California Law Review 957, specifically in regard to tort law.

[425] Reagan, "Common Good," *supra* note 423.

[426] Kristy Hughes, "The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse" in Social Dimensions of Privacy, Beate Roessler and Dorota Mokrosinska (eds) (Cambridge: Cambridge University Press, 2015) at 225 [Hughes, "Social Value of Privacy"].

[427] Reagan, *Legislating Privacy*; Allen, *Uneasy Access, supra* note 407.

would fragment the body politic and undermine the integrity of the political process. Privacy in this sense may also be seen as important to permitting the creation of the public and communities within public space. Privacy allows space within which relationships can occur absent the fragmentation caused by surveillance that singles people out (the discussion of Cohen's work below builds on this point). Finally, Reagan suggests that privacy is a collective value in the sense that the market cannot provide an optimal supply of privacy, and thus society requires public regulation and governance to ensure access to sufficient levels of privacy.

Privacy as a social value can also refer to the manner in which privacy supports social connection and interaction, building on Reagan's second point above. The role of privacy in social relations is necessarily relevant to life in public spaces. When one enters into public space, they are likely to encounter and have various interactions with others, especially in an urban and/or residential setting.[428] Professor Valerie Steeves for instance, building on Reagan's work, examines the role of privacy in social context as importantly permitting intersubjective (i.e., between two or more people) management and negotiation of personal boundaries. Privacy allows someone to manage their boundaries in relationship with others, in their preferred manner depending on the social context. Privacy is thus socially constructed within the situation in which one finds themselves. The ability to manage one's relationships with others is important to individual interactions, and is valuable to society. Notions of privacy as necessary to relational boundary management are also reflected in recent foundational privacy scholarship, including understanding privacy as contextual

[428] Valerie Steeves, "Reclaiming the Social Value of Privacy" in Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, Ian Kerr, Valerie Steeves, Carole Lucock (eds) (New York: Oxford University Press, 2009) at 191 [Steeves, "Reclaiming Social Value of Privacy"]; see also e.g., Charles D. Raab, "Privacy, Social Values and the Public Interest" in A. Busch and J. Hofmann (eds), *Politik und die Regulierung von Information* (Politische Vierteljahresschrift, Sonderheft 46, 2012) at 1 [Raab, "Social Values and Public Interest], drawing upon literature examining privacy's individual value and public value, determining that the theoretical building blocks for a social value approach to privacy are available, which could challenge the individual vs collective interest approach to weighing of competing interests.

integrity,[429] privacy as trust,[430] and privacy as obscurity.[431] Much of this scholarship has emerged in response to changing socio-technical conditions in North America, noting the significant impact that a range of technologies, including automated technologies, have on personal privacy outside the confines of seclusion.

The vital point here is that privacy protection cannot be separated from an understanding of the social context in which a privacy conflict arises. And, where privacy facilitates social dynamics (which are crucial to public space – where one inevitably encounters others), courts need to recognize the relational and social nature of privacy expectations in law.[432] Privacy allows for freedom in associating with others.[433] Privacy law that recognizes context and boundary management better reflects the reality of existing in public and shared spaces.

There is good policy reasoning for the judicial recognition of privacy in public space where that recognition facilitates social interaction and is beneficial to society. The remainder of this chapter elaborates on theoretical grounding for the recognition of privacy harm in public space, which builds on these theories of privacy as a social value that is intersubjective and relational. The contribution this chapter makes to the literature on various approaches to understanding "reasonable expectations of privacy" is to propose a particular understanding that is shaped by privacy's social

---

[429] Proposing that one manages their conduct and interactions based on social context, and a violation can occur through the stripping of that context and use of information in a different context than where it was shared: Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009).

[430] One manages their sharing and intimacy with others based on their trust in their interlocutors, privacy is violated when that trust is undermined: Waldman, *Privacy as Trust, supra* note 43; and Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Harvard University Press: 2018).

[431] One can expect privacy from others through expectations that others will not go to the effort to track or identify them, and privacy is lost, for example, when technology can overcome the discouraging level of effort needed to surveil: E.g., Selinger and Hartzog, "Obscurity", *supra* note 155; Selinger and Hartzog, "Inconsentability", *supra* note 155. See also, on the relational nature of privacy: Jennifer Nedelski, *Law's Relations: A Relational Theory of Self, Autonomy, and Law* (New York, Oxford University Press: 2011); and specifically in regard to automated technology: Ian Kerr, "Schrödinger's Robot: Privacy in Uncertain States" (2019) 20 Theoretical Inquiries in Law 123.

[432] See discussion below in Chapter 6 for ways in which courts have begun to do exactly this.

[433] E.g., Ben Goold, "Surveillance and the Political Value of Privacy" (2009) 1 Amsterdam Law Forum 3-6; Ferdinand David Schoeman Privacy and Social Freedom (Cambridge: Cambridge University Press, 1992) arguing privacy allows for freedom in association with others.

function, as discussed above, in conjunction with the particular spatial context of conduct arising in shared public spaces.

Reagan and Hughes also offer a note of caution on how courts approach striking a balance between privacy and other competing interests. For example, free expression and privacy are sometimes in tension in a privacy claim, such as when a journalist collects private information about a public figure, or even more routinely, when an amateur photographer photographs a public space full of people. A defendant in such a case might respond to the plaintiff's privacy claim with an appeal to the broad social values associated with free expression. In these cases, if an exclusively individualistic understanding of the value of privacy is measured against the social and collective benefits of free expression and/or journalistic freedom, privacy will often lose.[434] One person's individual interest in concealing their behaviour, for instance, may be little match for the social good of free expression. But where the collective and social value of privacy is instead measured against the collective value of free expression, a more nuanced weighing of these interests can be engaged.[435] Chapter 6 discusses practical options for courts in dealing with such balancing. The main point here is that understanding the social value of privacy is pertinent not only to understanding the interaction between the plaintiff and defendant, but also to the policy reasoning that often drives the development of tort doctrine in Canada.[436]

Relatedly, while this Chapter considers the *social* value of privacy, I note there are some peculiarities to tort law and thus to the analysis in this thesis. Tort law, as it is framed currently, addresses only *individual* harms – a plaintiff must show how their individual rights were violated or how they specifically were injured in order to recover in tort. Generally speaking, tort law does not

[434] Steeves, "Reclaiming Social Value of Privacy", *supra* note 428; and Reagan, *Legislating Privacy, supra* note 423.
[435] E.g., as the Supreme Court of Canada has engaged under the Quebec *Charter of Rights and Freedoms*. See: *Aubry, supra* note 50 at paras 52-59, 62-64.
[436] Reagan, "Common Good", *supra* note 423; Hughes, "Social Value of Privacy", *supra* note 426.

address systemic or collective harms in a direct way, with some narrow exceptions.[437] Thus, this thesis does focus on the notion of individual privacy at the core of the privacy torts. But, as developed in the below subsections and the next chapter, it calls for a notion of this individual right that reflects collective interests and is responsive to systemic harms and inequities, and moves away from privacy's historical and ongoing intersections with private property. The proposals in this thesis are nevertheless positioned as but one component in an approach to privacy that values public, shared, and social spaces.

The scholarship on the social value of privacy introduced here emphasizes the importance of considering the social value of privacy in social interaction, and the importance of recognizing the collective benefit of such privacy when balancing potentially competing social interests or policies. The next section builds upon this notion of the social value of privacy to explicitly consider the value of privacy in public spaces, and to articulate an understanding of a public space privacy harm.

Public Space Privacy Harm ~ Generally

This sub-section considers whether it is possible to conceptualize privacy harm in public space. In particular, this section examines literature suggesting it is possible to conceptualize such harm, not just through a limited expansion of the traditional privacy theory of seclusion, but more fulsomely on the basis that plaintiffs expect privacy in public space because it is a component of a public space experience. The rest of this Chapter argues that to enjoy a public, open, accessible, shared space, privacy is necessary and therefore can be reasonably expected, and when that expectation is violated, a plaintiff could experience a privacy harm. I consider below if a reasonable expectation of privacy exists in public *by virtue* of the public and social nature of the space.

[437] Public nuisance claims for example can address a collective problem.

A common vision of public space considers space to be a communal site for interaction, expression, and sharing—a physical location of the public sphere.[438] Public spaces are where diverse members of the public can co-exist; where individuals of distinct backgrounds and views can come together.[439] Public space is where individuals encounter difference, and it accordingly must be structured in a way that permits such difference to be expressed.[440] This view of public space calls for access to (and use of) space by any and all members of the public, even where the differences between individuals might create discomfort.[441] In fact, such discomfort from the exposure to difference is one of the core values of public space according to this view.[442] As Professor Nicholas Blomley explains, "the potential of public space can only be realized if it allows for spontaneous and unprogrammed encounters with others."[443]

However, in some instances for a space to serve its communal public purpose, it requires some carefully tailored law and regulation to ensure that the space is available to all members of the public. Generally, some rules will dictate permissible (or impermissible) conduct, things, and interactions in that space. I suggest in the pages that follow that this may include a legal mechanism for addressing and vindicating intentional privacy harms occasioned in public spaces. However, one

---

[438] This vision of public space is many ways driven by Habermasian ideals. Habermas' view of the public sphere as a discursive space/community was not tied to specific property. However, the ideals underlying the discursive public sphere have since been echoed in visions of public space and have informed judicial and academic perspectives on what public spaces are meant to be like. See Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, translated by Thomas Burger & Frederick Lawrence (Cambridge: MIT Press 1989).

[439] This view reflects an idea that public spaces are public not simply because they are "publicly owned". Rather, they are spaces within which the "public sphere" is formed, policed, and contested. See e.g., Evelyn S Ruppert, "Rights to Public Space: Regulatory Reconfigurations of Liberty" (2006) 27:3 Urban Geography 271 at 273.

[440] Ruppert, "Rights to Public Space" *ibid* at 280. "If public space is where difference is encountered then it must be structured in a manner that enables difference to be expressed and where particular conducts and uses are not privileged above and beyond those of others." Public space is a site where strangers can come together and encounter other people, meanings, and ideas crucial to politics: see also Nicholas Blomley, "Begging to Differ: Panhandling, Public Space, and Municipal Property" in Eric Tucker, James Muir & Bruce Ziff, eds, *Property On Trial: Canadian Cases in Context* (Toronto: Irwin Law for the Osgoode Society of Legal History, 2012) 393 at 407 [Blomley, "Begging to Differ"].

[441] See e.g., Don Mitchell, *The Right to the City: Social Justice and the Fight for Public Space*, (New York: Guilford Press, 2003); Jeremy Waldron, "Homelessness and Community" (2000) 50(4) UTLJ 371.

[442] Waldron argues that encountering realities and lived experiences that make the comfortable uncomfortable is what public space is all about. He argues it is a social good to be challenged in our comfortable preconceptions. *Ibid* at 380.

[443] Nicholas Blomley, "Public Space: Introduction" in Nicholas Blomley, David Delaney & Richard T Ford (eds) *The Legal Geographies Reader: Law, Power, and Space* (Oxford: Blackwell Publishers, 2001) 3 at 4.

of the underlying goals or policy drivers in such an approach should also be to preserve to the extent possible the public nature of that space. The privacy analysis should both consider and be shaped by the space in which it arises.

Spatial privacy harm refers to the harm(s) that can be caused to one's experience of a space as a result of surveillance or privacy engaging conduct (*e.g.*, collection, use, disclosure of information or a physical intrusion).[444] For example, a spatial analysis in public space might consider the ways surveillance alters one's experiences of public space, perhaps rendering that space less public, open, or accessible; or more exclusive.[445] This section expands on what this means, and how it can be understood, drawing first on professor Julie Cohen's writing, where she has articulated a concept of spatial privacy harm, through reference to a range of sociological and critical literatures.[446]

Cohen explains how many privacy scholars have reacted negatively to the notion of a "spatial metaphorization of privacy expectations and interests," and thus have not carefully considered the roles that space and spatial metaphors play in privacy discourse.[447] Reasons for resisting a spatial emphasis in privacy discourse include: not wanting to reinforce doctrinal links between privacy and private property (for fear that this would undermine claims to privacy in public and in spaces owned or controlled by third parties); not wanting to reinforce the social and economic relations of inequality arising in the links between privacy and property; some assert that spatial metaphors are too imprecise (e.g., do not define the shape or dimensions of a relevant space and what it contains); many argue spatial metaphors are unhelpful in the networked information

---

[444] Julie Cohen identifies "a harm that is distinctively spatial: that flows from the ways in which surveillance, whether visual or data-based, *alters the spaces and places of everyday life*." Julie Cohen, *Networked Self, supra* note 51 at 121, emphasis added.
[445] *Ibid.*
[446] Cohen, *Networked Self, supra* note 51.
[447] Cohen, *Networked Self, ibid* at 120: "the metaphoric structuring of privacy discourse affects our understanding of privacy and privacy harms." At the same time, privacy doctrine relies on visual metaphors – privacy as being unseen; invasions as becoming visible – that have gone unnoticed and/or under-analyzed.

society "because the greatest threats to privacy arise from the pervasive collection and sharing of information" not from lived experiences in different public or private spaces.[448]

Yet, privacy doctrine already uses spatial understandings and metaphors. Cohen explains, "whether surveillance invades a legally recognized interest in spatial privacy depends in the first instance on background rules of property ownership."[449] To date this has meant that generally speaking, surveillance in public or in spaces owned by third parties does not violate any expectation of privacy. In other words, the courts already rely on spatial guidelines for assessing someone's reasonable expectation of privacy.[450] Courts also use spatial metaphors like "zones" and "spheres" of privacy to facilitate the privacy analysis; in Canada this has been particularly notable in the constitutional jurisprudence.[451]

Cohen identifies two conceptions of privacy harm that pertain to public space, one of which is specifically a spatial privacy harm, which she calls "exposure". The concept of exposure builds on the other harm that she articulates – "transparency" – which is particularly applicable to the subsequent use and analysis of information that is collected from public space. Cohen writes about these harms in response to an increasing focus by privacy scholars and courts on informational

---

[448] Cohen, *Networked Self, ibid* at 122.
[449] Cohen, *Networked Self, ibid* at 121.
[450] Cohen, *Networked Self, ibid* at 121. She notes that in the US jurisprudence "the interesting thing about the reasonable expectations test is that it is fundamentally concerned not with expectations about the nature of particular *spaces*, but rather with expectations about the accessibility of *information* about activities taking place in those spaces." The courts protect our privacy in private properties when we do not expect information to be collected from those spaces; if we can expect information to be collected from a private property, then our privacy in that property might not actually be protected, despite our presence in private property. For example, the US Supreme Court decision in *Kyllo* was concerned with technology not in general public use – not expected. In contrast, the court held that it was permissible for the police to collect information from one's private backyard, even when fenced in, by flying a plane over the backyard because one cannot expect that information not to be collected. The Canadian privacy doctrine has followed a different line of reasoning with regard to private space. In Canada, information on the outside of the home that can be seen or accessed (in one's garbage, or on the surface of the home) was not considered private (though as I discuss in the next chapter, this case law is also changing in Canada). Information inside the home has been considered private, with a constitutional case in Canada dealing with parallel facts to *Kyllo* deciding the case in a different way – such that whatever takes place within the home is subject to a reasonable expectation of privacy regardless of whether technology can make information about that activity "visible." Accordingly, in Canada there has seemingly been a greater understanding of a spatial harm but one that has to-date only been predicated on valuing *private* spaces.
[451] See e.g., *R v Tessling*, [2004] 3 SCR 432.

privacy, which she argues is insufficiently addressing some of the deeper, *embodied* spatial harms associated with information technologies and surveillance. Germane to the discussion in this thesis is how Cohen articulates a way to understand the embodied harm that can follow specifically from public space surveillance, in a way that I later suggest could be (at least in part) addressed by tort law.

Cohen explains **exposure**, her conceptualization of a spatial privacy harm, as a particular kind of privacy harm that has to do with the way spaces are designed or modified in order to subject people in those spaces to a "condition of exposure" - a design that "constrains the range of available behaviors and norms."[452] Cohen emphasizes that this understanding of privacy is not just informational, it has a *spatial dimension*. She explains:

> The spatial dimension of the privacy interest, which I characterize as an interest in avoiding or selectively limiting exposure, concerns the structure of experienced space. It is not negated by the fact that people in public spaces expect to be visible to others present in those spaces, and it encompasses both the arrangement of physical spaces and the design of networked communications technologies.[453]

There is an embodied, situated experience that supports a spatial privacy interest, and is harmed by exposure, which again goes beyond just being visible to others:

> Surveillance infrastructures alter the experience of places in ways that do not depend entirely on whether anyone is actually watching. Governments know this well; that is part of the point of deploying surveillance infrastructures within public spaces. It seems sounder to conclude that the information-based frameworks are incomplete. Conceptualizing the privacy interest as having an independently significant spatial dimension explains aspects of surveillance that neither visibility nor informational transparency can explain.[454]

---

[452] Julie Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 75 The University of Chicago Law Review 181 at 190 [Cohen, "Privacy, Visibility"].
[453] Cohen, "Privacy, Visibility", *ibid* at 181.
[454] Cohen, "Privacy, Visibility", *ibid* at 192.

Direct visual surveillance affects the experience of space and place, causing privacy harm in at least two ways, she argues. First, it can promote a kind of passivity when operating in that space which she describes as a "ceding of power over space."[455] A sense of passivity arises because individuals under such surveillance lack agency to do anything about the surveillance.[456] Cohen elaborates:

> the targets of surveillance cannot entirely avoid the gaze (except by avoiding the place) and also cannot identify the watchers. We can say, therefore, that surveillance alters the balance of powers and disabilities that obtains in public places. It instills an expectation of being surveilled, and contrary to the conventional legal wisdom, this reasonable expectation and the passivity that it instills are precisely the problem.[457]

Surveillance can alter the ways in which places evolve and change in dynamic and relational ways.[458] In particular, Cohen characterizes the spatial dimension of the privacy interest here as an "interest in avoiding or selectively controlling the conditions of exposure."[459] The harm to one's spatial experience comes from the ways surveillance undermines one's ability to engage in public space; some places become non-places for those who seek or need to avoid that surveillance. *Zeliony v Dunn* for instance signals such harm, where the plaintiff felt she could not use her shared hallway any longer, due to the defendant's use of Ring to monitor the hall. Drawing on a range of literature, Cohen explains the idea of "non-places" as places where, for instance, some residents of a neighbourhood might be welcome, but that place is not accessible or welcoming to those whose entry incites automatic suspicion and surveillance.[460] This is the exact impact that critics of the Ring

---

[455] Cohen, "Privacy, Visibility…", *ibid* at 192.
[456] At least, lack agency to do anything immediate and/or legal, as reflected for instance in the example of the drone at a beach that opened this dissertation. See also: Thomasen, "Beyond Airspace Safety", *supra* note 4; Calo, "Drone as Privacy Catalyst," *supra* note 94.
[457] Cohen, "Privacy, Visibility…", *supra* note 453 at 193.
[458] "Like identities, places are dynamic and relational; they are constructed over time through everyday practice. Surveillance alters important parameters of both processes." Cohen, "Privacy, Visibility…", *ibid* at 193.
[459] Cohen, "Privacy, Visibility…", *ibid* at 194.
[460] She draws on the work of Marc Augé and others for this idea of non-places – e.g., "wealthy residential enclaves may be non-places to those whose entry incites automatic suspicion." Cohen, "Privacy, Visibility…", *ibid* at 193.

system warn about – that while the cameras might collect images of every passerby, the threat (of bringing in law enforcement, of interpersonal policing, of online gossip or shaming) is really directed at some but not all people who pass by the camera.[461]

Surveillance of a place and the creation of conditions of exposure, Cohen explains, "makes places more like non-places. Spaces exposed by surveillance function differently than spaces that are not so exposed."[462] Surveillance in public spaces alters the balance of power, where the space becomes more predictable for the watchers, and less so for the observed public – changing the dynamic and performance of identity, community, and place within that space.[463] In other words, it undermines the public nature of the space.[464] Privacy therefore, "encompasses an interest in the *structure of experienced space*, and this interest is threatened under conditions of visual or informational exposure."[465] There is a privacy harm or loss associated with the ways in which surveillance, or the perception of surveillance, affects the use of or exclusion from a space. Cohen's theory is backed by qualitative evidence. For instance, studies have shown that surveillance technologies can cause a person to alter or self-censor their behaviors if they believe they are being watched.[466]

The notion of exposure as Cohen has explained it – as a privacy interest in a spatial experience, or access to particular spaces – is not well understood, if at all, in the Canadian legal system's application of privacy torts outside of private property/seclusion. As the discussion in Chapter 3 suggests, courts have remained fairly steadfast within tort law in finding that being in public

---

461 E.g., Gilliard, "Caught in the Spotlight," *supra* note 122.
462 Cohen, "Privacy, Visibility…", *supra* note 453 at 193-94.
463 Cohen, "Privacy, Visibility…", *ibid* at 194. Cohen draws on the feminist scholarship of Hille Koskela throughout this analysis. "Koskela observes that surveillance makes public spaces less predictable for the watched. The relation is reciprocal: surveillance also attempts to make those spaces more predictable for the watchers. By altering the balance of powers and disabilities, exposure changes the parameters that shape the ongoing performance of identity, community, and place."
464 Thomasen, "Robots and Public Space," *supra* note 88.
465 Cohen, "Privacy, Visibility…", *supra* note 453 at 201. Emphasis added
466 See e.g., the studies reviewed in I. Manokha, "Surveillance, Panopticism, and Self-Discipline in the Digital Age" (2018) 16(2) Surveillance and Society 219-237. See also Jon Penney's work on the chilling effects of surveillance on public online activity, e.g., Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31 Berkeley Technology Law Journal 117.

undermines one's expectation of privacy, when Cohen has suggested that one might in fact expect or need privacy specifically in order to engage in public space.[467] Cohen's discussion of exposure emphasizes the ways in which surveillance can cause harm through a loss of access to the benefits of public space, including community, interaction, rest and respite, and freedom and autonomy of movement and identity. In the next chapter, I explain why the privacy torts should recognize these harms.

Layering onto the notion of exposure (a spatial harm that can be experienced whether or not information is actually collected), is Cohen's second concept of **transparency**. Transparency is conceptualized as a harm that can arise from the collection of information, including from public spaces. It can be a second dimension to an exposure harm. While the question of whether one is visible to others, or not, has long been employed in the tort doctrine as a basis for determining whether a plaintiff could expect privacy, transparency calls for a deeper and more nuanced analysis than this. The notion of transparency distinguishes simple observation from knowledge. The issue in assessing whether there has been a privacy harm is not just whether someone might be subject to mere observation by others. Cohen explains how visibility, while sometimes an important consideration in assessing privacy harm, cannot be the exclusive focus.[468] Focus on someone's visibility alone (i.e. the fact something/someone can be seen) "diminishes the salience and obscures the operation of nonvisual mechanisms designed to render individual identity, behavior, and preferences transparent to third parties."[469] Focusing only on visibility makes surveillance seem like it is just "passive observation rather than the active production of categories, narratives, and norms."[470]

---

[467] Neil Richards has written about the ways in which privacy enhances freedom of thought and expression: *Intellectual Privacy: Rethinking Privacy in a Digital Age* (Oxford University Press, Oxford: 2015).
[468] Julie Cohen, "Privacy, Visibility …", *supra* note 453.
[469] Cohen, "Privacy, Visibility", *ibid* at 181.
[470] Cohen, "Privacy, Visibility", *ibid* at 181.

In other words, Cohen argues that transparency addresses a deeper kind of harm than the concept of visibility would allow. When considering the potential expansion of tort remedies into public spaces, the courts need to balance a plaintiff's interest in privacy against the legitimate interests of defendants. People, including those who might be defendants, need to be able to participate in public space freely – an overly constraining privacy tort that makes mere observation actionable sets too low a threshold for the tort, and would undermine the very values the tort purports to protect (freedom, autonomy, dignity, *etc*). It would undermine the experience of public space for those who come to be in the position of defendants. However, *transparency* allows the courts to move beyond the superficial question of whether a plaintiff was visible (which rightly might not be actionable), to question whether surveillance has been used to rendered them *transparent* to a defendant.

Transparency, or being known, happens not just from mere observation but from what is then done with the observed or visible information. Put differently, the privacy analysis for transparency would go beyond just asking whether the defendant observed the plaintiff, to include an assessment of what information they might have collected and *how* any collected information was then used or processed. Currently the privacy torts for use and disclosure of a private fact seem inapplicable to information collected in public (because it is not a "private" fact). If courts were to instead consider a notion of transparency, they would engage a deeper analysis than just assessing if information was collected from public. Under a transparency analysis, courts are less concerned about whether a plaintiff could simply be seen by others, and are instead concerned with the use of a surveillance technology to record, analyze, identify, and/or share observable information about that person. For instance, such an approach would nuance the analysis in *Silber* where the plaintiff was filmed on his publicly visible parking lot. The plaintiff's claim was dismissed because he could be seen by others, without deeper consideration of the impact of the *filming* on the plaintiff and his privacy expectation.

A focus on transparency might draw the court's attention more directly to the significance of filming in his claim.

Transparency allows courts to distinguish between, for example, being seen by a neighbour who is sitting on their porch and being recorded and technologically or publicly scrutinized through the Ring security system and network or being seen by others at a park, and being followed or filmed by an anonymous remotely-located drone operator. This concept also captures the privacy harm that might be experienced from a system of surveillance – for instance, while a Ring camera on one home might only capture a moment in a person's day (which the court might deem *de minimus,* if even private), when that information is shared and compiled with other footage through the Neighbors network, it becomes possible for observers (home owners, police, *etc*) to draw more detailed inferences, create narratives, and categorize the people caught on film (e.g., this person belongs here, or is a stranger, and/or is threatening, *etc*). This goes to Cohen's notion of transparency – gaining knowledge of a person (not just simply looking at them). It allows courts to strike a balance within the privacy/private information assessment between society's interests in being able to function in public without widely incurring tort liability, and a plaintiff's legitimate interest in their privacy and the need for privacy in public.

A transparency harm can also arise at the collective or group level, with individual and group impacts. As Cohen explains, "The privacy interest against transparency encompasses not only the individualized information that surveillance collects, but also the informational frameworks that it imposes."[471] On this concept of the deeper transparency harm in informational accessibility and processing, Cohen explains:

> … threats to privacy from visual surveillance become most acute when visual surveillance and data based surveillance are integrated, enabling both real-time identification of visual surveillance subjects and subsequent

[471] Cohen, "Privacy, Visibility", *ibid* at 201.

> searches of stored visual and databased surveillance records. And, for the most part, informational accessibility does not result from a conscious decision to target particular individuals. Rather, accessibility is embedded in the design of social and technical institutions.[472]

This is not to say that unwanted visibility or observation never amount to privacy harm of some form, but that the analysis needs to go beyond just whether someone was visible to others, to also consider how techniques are used to gain knowledge about a person, or to impose frameworks or categories on a person, that are in themselves harmful or lead to harm. Transparency allows those with knowledge of others to assert power over them, not simply because they can be seen but because they can be "known" and therefore controlled.[473] An example of this might be seen in insurance cases like *Milner*, where the insurance company is seeking to categorize the claimant as truthful/fraudulent through surveillance. This categorization (and its underlying stereotypes about disability claims and claimants[474]) is a part of the privacy harm articulated by the plaintiff.

Cohen's concepts articulate some of the concerns or potential harms that can be experienced as a result of surveillance in public spaces. Law professor Ryan Calo has also explained privacy harm in a different way that can be helpful not just for understanding the range of privacy harms that can occur in public or in private spaces, but also as another way of conceptually approaching some of the concerns that Cohen identifies in the concepts of exposure and transparency within tort law framing.[475] Calo identifies two kinds of privacy harm - **subjective harms** (an internal sense of, or

---

[472] Cohen, "Privacy, Visibility", *ibid* at 184.
[473] Cohen, "Privacy, Visibility", *supra* note 453 at 185, emphasis added. "Claims of privacy invasion are claims about *unwanted subjection to the knowledge or power of others*. Within this metaphoric framework, it makes sense for such claims to be conceptualized in terms of seeing and being seen. Yet this way of understanding privacy carries significant intellectual and political costs. If it makes sense to conceptualize privacy problems in terms of visibility, it also makes sense to conclude that problems that cannot be so conceptualized are not privacy problems. […] But knowledge, power, and sight are not the same. If *"privacy" really is meant to denote an effective barrier to knowledge or the exercise of power by others, equating privacy invasion with visibility assumes what ought to be carefully considered."*
[474] Deirdre Heenan, "Challenging Stereotypes Surrounding Disability and Promoting Anti-oppressive Practice: Some Reflections on Teaching Social Work Students in Northern Ireland" (2005) 24(5) Social Work Education 495 [Heenan, "Challenging Stereotypes"] (identifying and challenging social stereotypes associated with the making of disability insurance claims).
[475] Ryan Calo, "The Boundaries of Privacy Harm" (2011) 86 Indiana Law Journal 1131 [Calo, "Privacy Harm"].

anticipation of, privacy loss – like the anticipatory/psychological concept of assault in tort law) and **objective harms** (externally imposed consequences of privacy loss – like the consequential/physical concept of battery in tort law).[476]

Calo defines a subjective privacy harm as: "the perception of unwanted observation. This category describes unwelcome mental states—anxiety, for instance, or embarrassment—that accompany the *belief* that one is or will be watched or monitored."[477] He gives the examples of the unease caused by a data breach, and concerns associated with generalized government or other surveillance, as subjective privacy harms. A subjective harm from "observation" could come from being watched directly, but could also come from someone reading information about a person, making inferences about them, or "systematic use of personal data systems."[478] The harm here is the discomfort, apprehension, or feeling of vulnerability that people experience as a result of feeling observed. The scope of what can prompt subjective harm in Calo's examples is broad and not all of these subjective harms will ground legal claims. But connecting the notion that privacy harms can arise from subjective experience (like the tort of assault) to the concepts of transparency and exposure, which can help to limit the scope of the tort, can allow for a nuanced analysis of one's experience of privacy harm without becoming overbroad. In other words – Calo's concept helps to further explain what is happening to a plaintiff who, for instance, experiences exposure harm through the loss of public space without any definable monetary loss that they could claim in court. The privacy torts in Canada are already equipped to recognize non-pecuniary damages.

---

[476] Calo's concepts of privacy harm build on the notion of privacy as "the loss of control over information about oneself or one's attributes." While not the exact definition I use in this thesis, his understanding of privacy closely aligns with the Prosser torts and the way Canadian courts have approached privacy in tort to date: Calo, "Privacy Harm", *ibid* at 1134. Calo argues that "privacy harm is unique in that it is a harm tied broadly to observation": at 1133. Of course, connecting this with Cohen's discussion of harm above, we can consider that there might be additional or deeper harms beyond just visibility/observation that arise from transparency or exposure (Calo does not specifically discuss Cohen's two framings).

[477] Calo, "Privacy Harm", *ibid* at 1133, emphasis added.

[478] Calo, "Privacy Harm" at 1144; the latter quote is drawn from Roger Clarke, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance," (1993) 4 Journal of Law & Information Science at 4032.

This concept of subjective harm is especially helpful for understanding the ways in which exposure and transparency might intersect. For instance, when someone sees a drone or home surveillance system and senses exposure, adjusting their behaviour or leaving a space, without ever knowing whether the camera is actually filming, the notion of subjective privacy harm can reflect the loss of public space that occurs here even if no information was actually collected or used.[479] It is the subjective mental state of the individual that has been affected, resulting in a spatial harm.

Subjective harm is what happens inside the mind of the person being harmed; this is in contrast to an objective harm which is an external harm that can include for example, a negative opinion subjectively held by *someone else* - external to the harmed person.[480] An objective privacy harm entails: "the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information."[481] Calo analogizes this harm to the battery tort, where law is concerned with what happens to us (whether we realize it at the time or not).

For example, Calo explains that an objective harm could occur when a company sells a user's contact information without authorization resulting in unwanted spam (not unlike the harm alleged in *Broutzas*), or when classified information is leaked revealing an undercover agent. As an example of a coerced use, Calo refers to occasions where a drunk-driver's blood is drawn without consent and used as evidence against him. This objective harm does not have to be carried out by a person – machines are capable of it as well.[482]

---

[479] Calo, "Privacy Harm" at 1146. Calo also refers to the fact people need "episodic solitude" from subjective privacy harm for their comfort, curiosity, self-development, mental health. This escape from observation could very well only be possible in public space for some people. Anita Allen, for example, explains why for a long time for many women, public space has been an escape or respite from the privacy invasiveness of the home.
[480] Calo, "Privacy Harm", *supra* note 476 at 1145.
[481] Calo, "Privacy Harm", *ibid* at 1133.
[482] Calo, "Privacy Harm", *ibid* at 1151. Also referring to Danielle Keats Citron, "Technological Due Process" (2008) 85 Washington University Law Review 1249.

The notion of objective harm connects well with Cohen's idea of transparency, for instance when observations are used to draw conclusions or "knowledge" about someone and then used against that person. Importantly for this discussion, objective harm can occur even if the plaintiff was not aware that the privacy violation was happening, as with the sharing of one's image on a neighbourhood app for example. While the sharing in and of itself, if not known, might not affect an individual's experience of public space in the moment (e.g., may not amount to subjective harm), it can still have a spatial effect, should the individual learn of it later and thus feel unable to enter the same space again, or especially, should the surveillance lead to further policing of that individual, and even an accompanying a loss of liberty or other externally imposed harms.[483]

Calo also seeks to "debunk[] the widely held view – that privacy harm can only occur when one human being observes another."[484] He emphasizes that "privacy harm can and does occur in the absence of a human perpetrator," or in the absence of a direct human observer.[485] This is significant in the context of technology-based surveillance.[486] It emphasizes that privacy harm could occur even when a drone does not have a camera payload but an individual believes they are being watched

---

[483] Calo pre-emptively addresses some potential critiques of his framework, one in particular that is significant to considerations in public space because it deals with social and collective issues. He refers to the argument that privacy harm is not merely individual but can be structural or "architectural," as Daniel Solove has called it. He explains the potential critique as: "The absence of privacy creates and reinforces unhealthy power imbalances and interferes with citizen self-actualization. These harms go to the very architecture or structure of our society." See: Calo, "Privacy Harm", *supra* note 476 at 1158. While these harms are important, Calo contends that they are not privacy harms – they are perhaps better characterized as societal cohesion and trust harms that happen to be composed of privacy harms though not necessarily or exclusively: at 1158. Lack of privacy might just be one component contributing to a larger societal/structural/architectural harm. Calo gives the example of police surveillance as individual privacy harms that add up to a different harm – the erosion of community trust. This community-level harm results from privacy harms in addition to other things but is itself not a privacy harm, he argues: at 1158. Drawing on the range of literature explored in this chapter and the *Charter* values discussion in the next Chapter, I disagree that the aggregate cannot be understood as a privacy harm at least within the Canadian tort law context, rather (in a tort law framework) I think the practical difficulty with the aggregate harm is in appropriately identifying against whom liability ought to lie. In this thesis, I am focused on intentional intrusions into privacy, thus am not specifically as focused on the aggregate of many incidental (unintentional) intrusions. Though I do believe reform in addressing individual privacy rights could provide some legal mechanisms toward addressing aggregate harms, as noted in the concluding chapter below, I also think that the social power dynamics and oppression embedded in some of the examples of aggregate harms are not optimally resolved or mediated through the individual-rights and monetary framing of tort law.

[484] Calo, "Privacy Harm", *ibid* at 1134.

[485] Calo, "Privacy Harm", *ibid* at 1134.

[486] See for example, Kerr, "Schrödinger's Robot," *supra* note 432.

(subjective harm; exposure); or where a home surveillance system captures and stores footage, or even more deeply processes the information to make an identification of the people in the footage, yet no human is directly involved in overseeing these processes.[487] Neither Calo nor Cohen limit their concepts to direct human observation, intentionally responding to the ways technology can be engaged in information collection and processing, and the psychological experience associated with being surveilled.[488] Cohen sets out a map for extending the privacy torts to more explicitly recognize and uplift the importance of privacy to public space; Calo provides further nuance and understanding for the various ways in which interpersonal surveillance in public space can cause privacy harm within the scope of tort.

Additionally, Professors Daniel Solove and Danielle Citron recently set out a typology of privacy harms. None specifically reflect the kind of embodied spatial harm discussed throughout this chapter. They do however flag an issue that is pertinent here, related to individually small but aggregate harms. These could occur, for instance, where an individual Ring camera only captures one moment of a person's day, but over the course of walking through a neighbourhood that person encounters many cameras and experiences a cumulative privacy harm.[489] To pursue an action for the cumulation of privacy harm, a plaintiff would have to name a large number of individual defendants. This presents practical challenges, in that it would increase costs and complexity of litigation, likely discouraging most potential litigants who have suffered exclusively non-pecuniary damages.

---

[487] Someone of course initiated the process by introducing the technology into that space, though they may be at a distance from its operations that impact the plaintiff, and/or may delegate the processing of collected information to the system and not be directly involved in or aware of that process.

[488] See also Ian Kerr's examination of the ways in which robot observation engages reasonable expectations of privacy even in the total absence of a human observer: Kerr, "Schrödinger's Robot," *supra* note 432.

[489] Danielle Citron and Daniel Solove state that "these types of injuries do not fit well into judicial conceptions of harm, which have an individualistic focus and heavily favor tangible physical and financial injuries that occur immediately.": "Privacy Harms" (2022) 102 Boston University Law Review (forthcoming) at 4 [Citron and Solove, "Privacy Harms"]. Notably, their work is focused on US jurisprudence. The Canadian privacy torts all explicitly allow for a claim to succeed even in the absence of tangible financial or physical injury. Nevertheless, this point raises an additional consideration for the Canadian torts - that of the cumulative harm arising from many individually less significant harms. See the discussion of aggregate harms above in footnote 484.

Additionally, each individual defendant in such a case is not morally culpable for the cumulative harm. Rather, the concern here is with the infrastructure that has been created through, for instance, a Ring system. The construction of a surveillance infrastructure from which individuals have no meaningful opportunity to disengage is a systemic issue and not an individual one, so individual harm-based torts will not adequately address or remedy these harms. Nevertheless, the privacy torts may serve as an important building block toward other legal mechanisms that *can* seek liability against some institutional actors, like vicarious liability or collective actions.[490] For either of these mechanisms to be successful, a litigant must first prove they have experienced harm. To do that in this context, the courts would need to recognize privacy harm in public spaces. While acknowledging the limits in the scope of the privacy torts for addressing systemic or infrastructural issues, I nevertheless suggest that the judicial conceptual shift to recognizing privacy harm in public spaces could contribute to broader reform efforts as well.[491]

Technology is Relevant to the Analysis of Spatial Privacy Harm

Calo emphasizes that privacy harm can occur even when a human is not directly involved in the invasive conduct. Cohen's notion of exposure relates specifically to the ways in which technology and/or architectures of spaces create conditions of exposure that either lead to people changing their behaviour in that space (loss of autonomy) or avoiding that space all together (loss of access/freedom of movement). Technology, particularly remotely-operated surveillance technology, plays an important role in the analysis of one's embodied experience of public space. Ultimately, the

[490] Negligence can also be useful but only where there is provable "damage."
[491] "Privacy harms often involve the aggregation of many small harms to each individual, which is compounded by the aggregation of all these harms to many individuals. The result makes privacy violations large-scale problems that cause a significant societal impact, but that do not fit readily into the traditional way the law looks at harm." Citron and Solove, "Privacy Harms", *supra* note 490 at 44.

use of remotely-operated technology can not only lead to a privacy harm, but might even deepen the spatial harm that is experienced by individuals under the gaze of the technology.

Professor Hille Koskela has argued that surveillance changes the nature of public urban spaces, producing new kinds of space and spatial experiences. For instance, she considers remotely-operated and monitored security and CCTV cameras that are put in place for the purpose of bringing safety to a space. She suggests that cameras change the physical/architectural nature of a space in ways that alter one's experience of and social interactions in that space. She proposes that "surveillance actually *makes* space a container" and objectifies those who live and operate within it, for the benefit of those behind the camera[492]:

> The alienated who look from behind the camera see the space under surveillance through the monitor (simplified to two dimensions) and they look at people as if they were objects. The very absence of direct personal contact and the fact that the overseers are not themselves in the monitored space make them see the space from the outside.[493]

Public space can be shaped into a passive space, where the watched objects simply exist.[494] Drawing from Foucault's writing on how architecture and space can be used to institute and facilitate the exercise of power, Koskela refers to this kind of space as "impregnated with disciplinary practices."[495] The presence of cameras, that are then associated with monitoring a space to mitigate, police, and punish unwanted behaviour, turns the space into one of power imbalance; one which she notes has inequitable impacts on individuals in that space depending on their relative social power.[496] Technology-mediated surveillance will affect people differently, both subjectively and objectively, and this could factor into whether a plaintiff experiences a privacy harm (e.g., one

---

[492] Hille Koskela, "'The Gaze Without Eyes': Video-Surveillance and the Changing Nature of Urban Space" (2000) 24(2) Progress in Human Geography 243 at 250 [Koskela, "Gaze without Eyes"]. See also, Anne Uteck, "Reconceptualizing Spatial Privacy for the Internet of Everything" (PhD Thesis, University of Ottawa Faculty of Law, 2013).
[493] Koskela, "Gaze without Eyes", *ibid* at 250.
[494] Koskela, "Gaze without Eyes", *ibid* at 251.
[495] Koskela, "Gaze without Eyes", *ibid* at 251.
[496] Koskela, "Gaze without Eyes", *ibid* at 254-55.

person might be more harmed by exposure than another in the way that surveillance deters someone from a space; or by transparency in the ways that identity factors can make some members of the public hypervisible to surveillance).

Finally, Koskela draws attention to the ways in which a remotely monitored space shapes the personal experiences and feelings of those being watched. She argues that the power dynamics of a space are fundamentally intertwined with emotion.[497] Surveillance can draw up a range of sometimes paradoxical emotions – such as feeling both safer because there is a camera, and simultaneously unsafe/vulnerable because of the loss of control over how and by whom one is watched.[498] This emotional paradox is poignant specifically because of the remote nature of the technology:

> Even though people under surveillance are well aware of the fact that the camera itself cannot see (and thus they do not trust the camera [for example, to intervene should their physical safety be at risk]), they are at the same time aware that someone sees, or might see, through it.[499]

Remote personal-use technologies shape and change experiences, and even the nature of the public spaces, where they are used or operated. Remote technologies like the drone that can operate in otherwise hard to use spaces, like low airspace, can create possibilities for spatial privacy harm where it becomes difficult to avoid the technology (a non-space) and so one is forced to change behaviour in light of the technology's presence, and its remoteness that makes it difficult to take remedial steps (loss of autonomy). In other words, the presence of remotely-operated surveillance technology would be pertinent to a privacy analysis that incorporates or recognizes exposure and transparency and the ways in which the harms of each can be experienced either subjectively or objectively. The presence of such technology changes the experience of a space, and changes the

[497] Koskela, "Gaze without Eyes", *ibid* at 257.
[498] Koskela, "Gaze without Eyes", *ibid* at 259.
[499] Koskela, "Gaze without Eyes", *ibid* at 259-60.

ways in which one experiences observation (from visibility to transparency).[500] The absence of laws that recognize and address this embodied experience in public spaces might further conceptually contribute to the public space harm that is experienced through interpersonal surveillance, as I explain in the next section.

Technology Does Not Emerge in a Vacuum

Another way to understand the public space impact of interpersonal surveillance, and of the current legal exclusion of the privacy torts from public space, can be found in academic thinking from the field of law & geography. The interdisciplinary field of law & geography explores the reciprocal relationships between law, space, and society, guided by a central proposition that law co-creates space, and space co-creates law.[501] Specifically helpful to this analysis of technology and privacy rights in public space, the field has examined how the notion of public space is produced through law and regulation, and how the public nature of space influences law.[502] In particular, law & geography scholars have emphasized that simply designating a space as 'public' in law does not on its own render that space public for everyone, or in some cases for anyone.[503] For a space to be

---

[500] This portion of a spatial analysis – that recognizes the particular impact of technology - could also overlap well with a contextual integrity understanding of privacy as proposed by Helen Nissenbaum in *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009); see also Jason Patton, "Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places" (2000) 2(3) Ethics and Information Technology 181. The taking of information from one place and then using it elsewhere or combining it with other information changes or affects the context in which the subject of observation was operating – their expectations of privacy might be guided by the space where they are, but they actually experience a loss of privacy through this decontextualizing of collected information. This chapter is specifically interested in the ways in which public space could be relevant to the privacy tort analysis; that could be extended into a broader discussion of a contextual integrity approach to privacy analyses as well.

[501] Law and property scholar Antonia Layard's personal website provides clear explanations of some central concepts: <http://antonialayard.com/what-is-legal-geography/>. See also the below citations in this sub-section for further academic writing.

[502] Parts of this discussion of Law and Geography draw from an earlier paper of mine, see: Kristen Thomasen, "Flying between the Lines: Drone Laws and the (Re)Production of Public Spaces" in Eric Hilgendorf and Uwe Seidel (eds) *Robotics, Autonomics, and the Law* (Germany: Nomos, 2017). See also e.g., Nicholas Blomley, "Law, Property and the Spaces of Violence: The Frontier, the Survey, and the Grid" (2003) 93 Annals, Association of American Geographers 121; David Delaney, "Beyond the Word: Law as a Thing of this World" in Jane Holder and Carolyn Harrison (eds), *Law and Geography* (Oxford: Oxford University Press, 2003) 67.

[503] Some public-owned government buildings, for example, are entirely off limits to members of the public.

public, members of the public must be able to identify it as such, and must be able to access and use the space.[504] The architecture of the space, including surveillance architectures, are relevant to whether it is really a public space. Similarly, the physical qualities of a space, such as being physically open and accessible to members of the public, do not alone determine whether a space is a 'public' space. A shopping centre could feel public to those seeking to enter, but it is legally designated as private property and its owners have a private property-based right to exclude.[505] To actually be a *public* space, the space also requires a legal status that permits public use, and the protections that flow from that.[506]

Beyond the legal status of a space though, as either public or private for instance, the regulatory regimes that apply *within* that space can also determine or affect the public nature of the space.[507] Regulations that exclude some people from the space, prohibit certain conduct or activities within the space, permit certain designs of space or objects within that space, or permit forms of policing and surveillance,[508] can all have the effect of rendering a public space *less* public to the

---

[504] Antonia Layard, "Freedom of Expression and Spatial (Imaginations of) Justice" in Dimitry Kochenov, Grianne de Burca, Andrew Williams (eds), *Europe's Justice Deficit?* (Oxford: Hart Publishing, 2015) at 7. The status of a space as public can be derived through reference to different qualities of the space: the features of the space, social norms associated with the space, etc. For more see e.g., Henri Lefebvre, *The Production of Space,* translated by Donald Nicholson-Smith (Oxford: Blackwell Publishers, 2000); S. Ruddick, "Constructing Difference in Public Spaces" (1996) 17 Urban Geography 132; Don Mitchell, *The Right to the City: Social Justice and the Fight for Public Space* (New York: Guilford Press, 2003); Evelyn Ruppert, "Rights to Public Space: Regulatory Reconfigurations of Liberty" (2006) 27 Urban Geography 271.

[505] Such spaces can be regulated at least largely if not fully by the private owner. See Layard, "Freedom of Expression", *supra,* note 505 at 5; see also *Harrison v Carswell* [1976] 2 SCR 200; Evelyn S. Ruppert, "Rights to Public Space: Regulatory Reconfigurations of Liberty" (2006) 27 Urban Geography 271-292; Bert-Jaap Koops and Galič discuss the growing privatization and securitization of public space in "Conceptualizing Space and Place: Lessons from Geography for the Debate on Public Privacy" in Tjerk Timan, Bryce Newell, & Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Edward Elgar Publishing, 2017) 19-46; Anne Bottomley, "A Trip to the Mall: Revisiting the Public/Private Divide" in *Feminist Perspectives on Land Law,* Hilary Lim (ed) (Cavendish: Routledge, 2007) 65-96.

[506] Layard, *supra* note 505 at 6. See also Antonia Layard, "Public Space: Property, Lines, Interruptions" (2016) 2(1) Journal of Law, Property and Society 1. Drawing from Layard's compelling arguments in the latter piece, I am mindful that legal status alone does not make space 'public' and often might just serve to determine who has the authority over the space, including the authority to regulate and to exclude.

[507] Mitchell, *The Right to the City*, *supra* note 442.

[508] Hille Koskela, "'The gaze without eyes': video-surveillance and the changing nature of urban space" (2000) 24 Progress in Human Geography 243.

extent that it is not as accessible or open to all members of a community in the same way.[509] This can mean that different individuals experience the same space as either public or private/exclusionary, despite a common legal designation of the space as 'public.'

For this very reason, Professor Evelyn Ruppert argues that what is really at issue when considering the public nature of a space are the "regulatory practices that configure liberty – that is, rights to public space and who and what belong as part of the public."[510] In order to understand public space as a collective space, she adds, "we must examine how it is constituted by regulatory practices."[511] Accordingly, the absence of a legal recognition of privacy rights between private individuals in public spaces, which could permit the use of remote technologies for surveillance and interpersonal policing, can actually undermine the publicness of public space. Said otherwise, tort law's current understanding of public space (driven by historical patriarchal and colonial norms) might actually undermine the nature and values of public spaces.[512]

While this last point – that the absence of law can itself affect public space experience – may not be directly pertinent to the judicial analysis of an individual plaintiff's reasonable expectation of privacy (e.g., it may risk circularity in the privacy analysis), it is worth noting more generally in light of the discussion in this thesis until this point. Namely, it is relevant to people's lived experiences in public space that there is a seemingly sweeping exclusion of public space from the privacy torts' scope. This absence of recognition of the value of privacy in public has emerged from traditional

---

[509] Evelyn Ruppert, "Rights to Public Space: Regulatory Reconfigurations of Liberty" (2006) 27 Urban Geography 271. Nicholas Blomley, "Public Space: Introduction" in Blomley et al, *Legal Geographies Reader* at 3.
[510] Ruppert, "Rights to Public Space", *ibid* at 271.
[511] Ruppert, "Rights to Public Space", *ibid* at 272-273. "While many social and political activities that make up public life occur in public spaces, these are enabled and constrained by a variety of practices (laws, regulations, urban design, surveillance, and policing). Collectively these constitute a regulatory regime. […] in order to understand public space as a collective good we must examine how it is constituted by regulatory practices." Ruppert in fact defines public space as "that object which is constituted not by ownership but by a regime made up of regulatory practices" at 273.
[512] Public space can lose its configuration as a space for the public though regimes with a limited view of who constitutes the 'public', or of who and what (including various technological systems) belong in that space. Ruppert, "Rights to Public Space", *ibid* at 273: "What is at issue in assertions about the decline of public space is that this regulatory regime is reconfiguring liberty – that is, rights to public space – through a change in the conception of the public, of who and what belong as part of that public."

(though ongoing) oppressive social norms about the private home and about public space. The absence of any legal recognition of interpersonal privacy rights in public enables the establishment of interpersonal surveillance infrastructure. Put bluntly, tort law's treatment of public space is bad for public space, and for those subjected to surveillance within it. While this observation may not contribute to the privacy analysis directly (as the other observations above are suggested to do), I suggest it does further support a case for some form of tort reform that recognizes the value of privacy in public specifically because it is good for the lived experience of public space. This is especially the case given that the literature examined through this Chapter outlines *how* people can experience privacy harms in public space. The next chapter builds from this point to make a practical doctrinal argument for *why* tort must recognize the value of privacy in public, and must vindicate a range of public space privacy harms.

Chapter 6 – *Charter* Values as a Groundwork for Privacy Tort Reform

This thesis has examined the relevance of the privacy torts in addressing technology-facilitated interpersonal surveillance in public space, and vindicating public space privacy harms. The torts are currently interpreted to be of little application to such conduct. However, the reason for this stems largely from the outdated and oppressive historical trajectory of the torts. This chapter builds upon the preceding discussions of the historical trajectory of the privacy torts, the value of privacy in public spaces, and the conceptualization of public space privacy harms to argue for extending the scope of the Canadian privacy torts. As noted in Chapter 4, various scholars have previously argued for privacy tort reform, including in relation to the limited application of the torts in public space. This chapter contributes to that discussion by proposing a legal basis on which to approach such reform, recognizing the ways in which being in public space can actually heighten the social importance of a plaintiff's expectations of privacy in different circumstances. This chapter argues that courts must explicitly reject the historical prioritization of particular interests in the privacy analysis particularly as centered around the 'home as a man's castle' doctrine, and adopt a theory of privacy in public that truly values public space.

I approach this argument through the lens of *Charter* values. Notions of privacy, (in)equality in the application and meaningfulness of the law, and community experiences in public space evoke a number of values embodied in the *Canadian Charter of Rights and Freedoms*, including privacy, substantive equality, and expressive freedom. The *Charter* does not apply directly to private law disputes, like privacy-based tort law disputes, and parties cannot rely on *Charter* rights in a strictly interpersonal claim like those under consideration here.[513] However, the common law is meant to

[513] If, however, collected images are subsequently shared with law enforcement or another state agency, a plaintiff/claimant may also be able to draw directly upon the *Charter* in an action involving the state.

evolve in line with *Charter* values.[514] And to some extent, the privacy torts have purportedly been interpreted in line with *Charter* privacy values, particularly in Ontario and in the interpretation of BC's *Privacy Act*. I argue below though that these decisions have not reflected the contemporary *Charter* value of privacy. Furthermore, there is no reason to limit the *Charter* values analysis to privacy alone – other important *Charter* values like equality and expressive freedom support the evolution of privacy tort law toward recognizing privacy rights and harms in public spaces, too. Judicial recognition of such is all the more pressing in the context of increasing interpersonal, technology-facilitated surveillance.

This chapter begins by explaining the significance of *Charter* values to the privacy torts. The next section explains how the current interpretation of the privacy torts, in particular as excluding occurrences arising in public spaces, failing to distinguish the privacy implications of being seen from being recorded, and failing to consider the relational and contextual factors at play between the parties to a dispute, no longer accords with the *Charter* value of privacy. Finally, this chapter proposes a broader understanding of the pertinent *Charter* values to also include, at least, substantive equality and expressive freedom. This broader approach would necessitate a recognition of privacy harms in public space, and in particular, explicit denunciation of the historical trajectory that has tightly associated the privacy torts with property and secrecy/seclusion. Such a step would create space for the development of privacy torts that can better respond to interpersonal surveillance, particularly where mediated by remotely-operated and automated technologies. Similarly, as noted at the end of Chapter 5, such a step could help create a socio-legal environment where technology design should have to consider and account for interpersonal privacy rights in public spaces. More specifically, by addressing the interpersonal surveillance gap in the law, developers of technical systems would no longer benefit to the same extent from designing interpersonal surveillance tools.

---

[514] *RWDSU v Dolphin Delivery Ltd*, [1986] 2 SCR 573 [*Dolphin Delivery*].

Quasi-Constitutionality of Privacy Protection and of the Privacy Torts Specifically

Before examining the pertinence of *Charter* values to the interpretation of the privacy torts, it is worth noting the special attention courts have paid to privacy protections throughout the Canadian legal system. In particular, the Supreme Court of Canada (SCC) has emphasized that privacy protecting laws are "quasi-constitutional" and should thus be interpreted in broad and nuanced ways, even within private law.[515] By virtue of this quasi-constitutional status, it is even more arguable that the privacy torts should be interpreted in line with contemporary *Charter* values. Most recently, the majority and concurring opinions of the Supreme Court of Canada's decision in *Douez v Facebook* emphasized that the BC *Privacy Act* has a quasi-constitutional status.[516]

In *Douez*, Facebook sought to have Ms. Douez's class action for violation of the BC *Privacy Act* (for the alleged non-consensual use of images of Facebook users to advertise products to others) stayed because of a forum selection clause in Facebook's user agreement, which requires disputes to be resolved in California. The chambers judge declined to enforce the clause, permitting the claim to go forward in BC courts. This decision was appealed to the SCC. In affirming the chambers judge's decision, the Court emphasized that the privacy interests protected by the BC *Privacy Act* are quasi-constitutional in their nature.[517] The SCC explained that because of this quasi-constitutional status,

---

[515] E.g., *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, [2013] 3 SCR 733 [*Alberta Privacy Commissioner*]; *Lavigne v Canada (Office of the Commissioner of Official Languages)*, [2002] 2 SCR 773, at para 24 [*Lavigne*]; *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403, at paras 65-66 [*Dagg*]; *H.J. Heinz Co. of Canada Ltd. v Canada (Attorney General)*, [2006] 1 SCR 441, at para 28 [*Heinz*].

[516] *Douez v Facebook*, 2017 SCC 33 at paras 4, 52, 58-62, 105 [*Douez*].

[517] See also: *Alberta Privacy Commissioner, supra* note 516 at para 20: "As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society." The court also said in regard to privacy in public at para 27 (in the context of data protection legislation): "It goes without saying that by appearing in public, an individual does not automatically forfeit his or her interest in retaining control over the personal information which is thereby exposed. This is especially true given the developments in technology that make it possible for personal information to be recorded with ease, distributed to an almost infinite audience, and stored indefinitely. Nevertheless, *PIPA*'s restrictions operate in the context of a case like this one to impede the formulation and expression of views on matters of significant public interest and importance."

local courts have an important interest in hearing claims under the *Privacy Act*, as "these rights play an essential role in a free and democratic society and embody key Canadian values."[518]

Douez dealt specifically with British Columbia's privacy statute. However, the court's analysis should logically also apply to, at least, the other provincial privacy statutes as well, given their similar origins, scope, intention, and even wording. It is also arguable that the *Douez* reasoning should apply to the common law privacy torts. The Supreme Court has recognized other common law private law causes of action to be quasi-constitutional in the past. For instance, the common law tort of defamation is also considered quasi-constitutional.[519] Defamation and privacy are closely connected in their underlying purpose of protecting dignity and autonomy.[520] Further, the common law torts strive toward a similar recognition of privacy harm as the statutory torts, as noted in Chapters 3 and 4. While these torts have come about through different legal processes, the purpose they are meant to serve is similar. Given that the Supreme Court has consistently recognized other privacy protections as quasi-constitutional, the quasi-constitutional status of the BC *Privacy Act* protections should extend to the other provincial privacy torts as well.

The quasi-constitutionality of private law remains a somewhat ambiguous legal designation. Private laws that are quasi-constitutional can be seen as reflecting the fundamental rights set out in the *Charter*, which ought to influence how these protections are interpreted.[521] Courts are meant to give quasi-constitutional laws a "broad and generous" interpretation.[522] The quasi-constitutional designation may also afford greater weight to these legal rights when they must be balanced with

---

[518] *Douez, supra* note 517 at para 58.
[519] *Éditions Écosociété Inc. v Banro Corp.*, 2012 SCC 18 at para 57 [*Banro*], affirming that *Hill v Church of Scientology* held that the reputational interests protected by defamation have quasi-constitutional status (though that language was not used in *Hill*). Cory J considered privacy to be a *Charter* value that informed the judicial interpretation of the scope of the defamation tort: *Hill v Church of Scientology*, [1995] 2 SCR 1130 at para 121 [*Hill*].
[520] *Jones, supra* note 27 citing *Hill, ibid* at para 43.
[521] Vanessa MacDonnell, "A Theory of Quasi-Constitutional Legislation" (2016) 53 Osgoode Hall Law Journal 508-539 at 522 [MacDonnell, "Quasi-Constitutional"]. *Dolphin Delivery*, *supra* note 515.
[522] MacDonnell, "Quasi-Constitutional", *ibid* at 510.

other potentially competing interests.[523] The quasi-constitutionality of privacy protection calls for a generous interpretation of that protection, which I will argue below must now include recognizing privacy harm in public spaces.

Charter Values and the Evolution of the Common Law

As noted, the *Charter* itself does not apply to interpersonal private law conflicts. Nevertheless, courts are meant to be mindful of the values reflected in the *Charter* when developing and evolving the common law, especially where that law is considered quasi-constitutional.[524] *Charter* values have already purportedly played a role in the development of the privacy torts in Canada. For instance, *Charter* values guided the ONCA's recognition of the common law tort of intrusion upon seclusion in *Jones*; and have aided the courts in the interpretation of the BC *Privacy Act*.[525] The next section examines the role that *Charter* values are meant to play in the interpretation and development of the law generally. The subsequent sections consider what this means for the current interpretation of the privacy torts, and particularly, for the application of these torts to technology-mediated privacy conflicts arising in public space.

---

[523] See e.g., *Banro, supra* note 520 at para 57 and *Douez, supra* note 517 although see *Alberta Privacy Commissioner, supra* note 516: SCC striking balance between privacy and expression.

[524] "Where, however, private party "A" sues private party "B" relying on the common law and where no act of government is relied upon to support the action, the *Charter* will not apply. I should make it clear, however, that this is a distinct issue from the question whether the judiciary ought to apply and develop the principles of the common law in a manner consistent with the fundamental values enshrined in the Constitution. The answer to this question must be in the affirmative. In this sense, then, the *Charter* is far from irrelevant to private litigants whose disputes fall to be decided at common law" Justice McIntyre at para 39 of *Dolphin Delivery, supra* note 515; see also *Jones, supra* note 27 at paras 45-46; *Hill, supra* note 520 and *Grant v Torstar Corp.,* [2009] 3 SCR 640 [*Grant v Torstar*] (both regarding defamation – another reputational tort).

[525] *Jones, supra* note 27; *TeBaerts v Penta Builders Group Inc,* 2015 BCSC 2008 (affirming that *Charter* jurisprudence can be used to aid the interpretation and application of the BC *Privacy Act*).

What Are Charter Values?

Charter values refer to the values embodied in the *Canadian Charter of Rights and Freedoms*. These values can inform non-*Charter* statutory interpretation and the development of the common law, including the recognition of new private law causes of action.[526] The methodology for how courts and other decision-makers (e.g., administrative bodies) ought to draw on *Charter* values when making a decision is not always clear. However, generally speaking the courts should not develop the common law or interpret statutes in ways that directly undermine the values embodied in the *Charter*. The question of *how* courts should rely on *Charter* values to develop the law, including private law, has been the subject of academic analysis.

For instance, professor Peter Hogg has said that "the concept of "*Charter* values" has been invented by the Supreme Court of Canada to mitigate the fact that the *Charter of Rights* applies only to governmental action."[527] He explains that,

> While the *Charter* does not directly apply to the common law, the common law should respect *Charter* values and will in appropriate cases be amended so that it does respect *Charter* values. And, in reliance on this doctrine, a number of common law rules have in fact been modified, so that in practice there is not a great deal of difference between the direct application of the *Charter* to statute law and the indirect application of the *Charter* to the common law.[528]

Hogg's impression is that every *Charter* right is likely a *Charter* value. However, the concept of *Charter* values also extends beyond the specifically enumerated rights. For instance, *Charter* values include privacy, even though privacy is not an explicitly enumerated right within the *Charter*.

---

[526] Peter Hogg, "Equality as a Charter Value in Constitutional Interpretation" (2003) 20 Supreme Court Law Review 113-133 at 116-17 [Hogg, "Equality as a Charter Value"]; Hogg cites to *Hill, supra* note 520 at paras 97-98.
[527] Hogg, "Equality as a Charter Value", *supra* note 527 at 116.
[528] Hogg, "Equality as a Charter Value", *ibid* at 116.

Lorne Sossin and Mark Friedman have identified at least eight *Charter* values explicitly named and discussed in SCC jurisprudence.[529] These are: liberty, human dignity, substantive equality, autonomy, fairness, expressive freedom, religious freedom, and privacy. The courts also allude to mobility, the promotion of multiculturalism and diversity, and democracy as possible additional standalone values, or perhaps as nuances to other recognized *Charter* values.

Like Hogg, Sossin and Friedman conclude that there is ambiguity in the jurisprudence as to the source and application of *Charter* values. For example, they say that the *Charter* value of expressive freedom clearly connects with the *Charter* right to freedom of expression. Dignity and privacy, by contrast, have been consistently identified as *Charter* values, even though neither exists as a standalone right in the *Charter*. Privacy has emerged especially through the s. 8 right to be free from unreasonable search and seizure, but also is embodied in other *Charter* rights, along with dignity. Some *Charter* values like minority rights might arise from unwritten constitutional principles.[530] There is some uncertainty in how the courts can identify *Charter* values, other than by looking to prior SCC jurisprudence. Sossin and Friedman suggest, "that there may well be multiple sources for *Charter* values — as the *Charter* both extended and reflected Canada's constitutional commitments."[531]

In terms of evolving the common law, a *Charter* value may be cited as a reason justifying, for instance, the adoption of a new legal test or a break from prior precedent, as was the case in *Jones v Tsige*[532]; or a *Charter* value may support the recognition of a new defence to an action, as was the case in *Grant v Torstar*.[533] Or, the court might face competing *Charter* values and have to strike a balance

---

[529] Lorne Sossin and Mark Friedman, "Charter Values and Administrative Justice" (2014) 67 Supreme Court Law Review (2d) 391-430 [Sossin and Friedman, "Charter Values"], see history of *Charter* values starting at 403.
[530] Sossin and Friedman, "Charter Values", *ibid* at 408
[531] Sossin and Friedman, "Charter Values", *ibid* at 408
[532] *Jones*, supra note 27 at para 31.
[533] *Grant v Torstar*, *supra* note 525 at e.g., paras 44-45.

between them.[534] But the particular methodology that courts should use to develop the common law in line with *Charter* values remains somewhat unclear. The Supreme Court, for instance, has not explained explicitly how *Charter* values should influence the evolution of the law, other than that the law should evolve in accordance with, and with respect for, those values.[535] Where the common law is "out of step" with *Charter* values, the SCC has said that courts should change the common law rule to bring it into consistency with *Charter* values, where possible.[536] This would seem to require a more active role for courts than simply not contradicting *Charter* values.

Charter values also serve as a principle of statutory interpretation, which is pertinent with respect to the statutory privacy torts.[537] However, lawyers Mark C. Power and Darius Bossé show how muddled the concept is as a statutory interpretation tool. While the SCC has said that statutes must be interpreted in line with *Charter* values in order to maintain internal consistency in the law,[538] the courts have expressed varying views on the extent to which *Charter* values are a guiding principle of statutory interpretation, or simply a secondary principle that arises when a genuine ambiguity in a statute cannot otherwise be resolved.[539] The authors essentially conclude that the endeavour of

---

[534] See Sossin and Friedman, "Charter Values", *supra* note 530 at 423-424; also see Angela Cameron and Paul Daly, "Furthering Substantive Equality Through Administrative Law: Charter Values in Education" (2013) 63 Supreme Court Law Review (2d) 169-204 [Cameron and Daly, "Furthering Substantive Equality"], addressing purportedly conflicting values in the administrative setting.

[535] *Hill, supra* note 520 at para 97: "When the common law is in conflict with *Charter* values, how should the competing principles be balanced? In my view, … the balancing must be more flexible than the traditional s. 1 analysis undertaken in cases involving governmental action cases. *Charter* values, framed in general terms, should be weighed against the principles which underlie the common law. The *Charter* values will then provide the guidelines for any modification to the common law which the court feels is necessary."

[536] *R v Salituro*, [1991] 3 SCR 654, at 675 [*Salituro*]; *Aubry, supra* note 50 at para 16.

[537] *Charter* values also gained notable traction in administrative law, particularly following the SCC decision in *Doré*, see also *Vavilov*. I do not focus specifically on how it is to be used as a concept in administrative decision making, because that is beyond the scope of the current investigation.

[538] E.g., *R v Sharpe* at para 33. See: Mark C Power and Darius Bossé, "Une tentative de clarification de la présomption de respect des valeur de la Charte canadienne des droits et libertés" (2014) 55 Les Cahiers de Droit 775-807 [Power & Bossé, "Clarification"].

[539] E.g., This issue was live in a recent privacy decision, *R v Jarvis*, 2019 SCC 10, [2019] 1 SCR 488 [*Jarvis*] in which the majority of the Court held that *Charter* conceptualizations of privacy formed a relevant part of the legislative context that should be considered when interpreting the impugned *Criminal Code* provision, given that Parliament specifically referred to the concept of a "reasonable expectation of privacy". The minority opinion in *Jarvis* rejected this approach though. The majority decision penned by Wagner CJ states: "the s. 8 case law represents a rich body of judicial thought on the meaning of privacy in our society. Far from being unmoored from our ordinary perceptions of when privacy can be

interpreting statutes in line with *Charter* values requires greater clarity. But they also assert that in the case of quasi-constitutional legislation (like the privacy tort statutes), the standard rules of interpretation call for a consideration of the context of legislative drafting, which should include *Charter* values. In other words, *Charter* values should not be used only as a secondary rule of interpretation (i.e., only turned to in cases of genuine ambiguity), but as a primary part of understanding the context in which the statute was drafted.[540] Notably though, the provincial *Privacy Acts* were largely drafted before the *Charter* came into force, thus it cannot be said that the *Charter* was a part of the legislative drafting context. Nevertheless, given their quasi-constitutional status as confirmed by the SCC, per *Douez*, *Charter* values may remain significant to the interpretation of the various provincial *Privacy Acts*.[541]

For the purposes of the analysis in this thesis, in particular the argument that the interpretation of the provincial *Acts* needs to evolve away from the historical trajectory that the courts have read into them, I argue that *Charter* values are pertinent to the interpretation of the *Acts*.

---

expected, judgments about privacy expectations in the s. 8 context are informed by our fundamental shared ideals about privacy as well as our everyday experiences." The minority decision penned by Rowe J disagreed with this interpretation, for reasons stemming from the different context of a *Charter* protection and a criminal prohibition. Accordingly, future cases could also raise disagreement in the court. In a recent Federal Court Reference decision pertaining to the interpretation of PIPEDA (which has been said to be quasi-constitutional), the Federal Court declined to defer a decision until it could hear a *Charter* values argument to narrow the scope of a PIPEDA protection by expanding the interpretation of an exclusion to the *Act*, as it was "not necessary to resort to Charter values unless there is "genuine ambiguity" in interpretation of a statute" (at para 94). The Court did not expressly address the quasi-constitutional nature of *PIPEDA*, but did nevertheless explain why it was not ambiguous. The Court held that the impugned exclusion (which narrows the application of the Act) should not be broadly interpreted based on plain meaning of the language in the Act. The Court does not explicitly denounce the relevance of *Charter* values but proceeds without that argument, suggesting *Charter* values are only necessary in cases of genuine ambiguity. See: *Reference re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723.

[540] Power & Bossé, "Clarification", *supra* note 539. But see also *Reference re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723.

[541] Professors Angela Cameron and Paul Daly have also argued that where a decision-maker's decision touches upon the life, liberty, and security of vulnerable persons, the decision maker's discretion (in their example, an administrative decision maker), should be especially sensitive to the values underlying the *Charter*. They argue that the value of substantive equality looms especially large in such a context. "An individual's life, liberty, and security of the person may not be threatened to such an extent that section 7 is itself engaged, but where administrative decisions touch upon these aspects of vulnerable people's lives, discretion should be exercised in an appropriately sensitive manner. More broadly still, the notions of compassion and fairness, in a broader setting of constitutionalism, democracy, and the rule of law, animate the provisions of the Charter. For the vulnerable individual, these notions are full of vitality. Section 15's guarantee of substantive equality looms especially large in this decision-making picture, whether or not the formal threshold of section 15 is surpassed." Cameron and Daly "Furthering Substantive Equality", *supra* note 535 at 188.

Charter values are either directly relevant in the interpretation of a quasi-constitutional *Act*, or they are relevant in the case of a genuine ambiguity, which I suggest arises in the interpretation of a "violation of privacy" in an *Act* where privacy is not defined. Furthermore, public space is not excluded, and drafters intended to address issues like electronic surveillance which would be analogous to many of the concerns raised by increasingly automated personal-use devices, yet case law interpreting the *Act* has suggested otherwise. If this *Charter* values approach is not adopted, I nevertheless suggest that much of the reform argued for here can and should influence the future trajectory of the provincial torts, as the socio-technical environment in which they operate has shifted and tort law has long been influenced by policy considerations that account for changes in social norms and experiences.[542] And given that courts have already appealed to *Charter* jurisprudence to interpret the BC *Privacy Act*, reference to contemporary *Charter* jurisprudence could also fall within the scope of precedent driven developments of the law.[543]

It is clear that *Charter* values are perceived by both courts and academic commentators as relevant to the common law privacy torts, even if what this means for their interpretation bears some lingering uncertainty. Prior to *Jones v Tsige*, John Craig argued that a *Charter* values approach to the development of the common law should encourage the courts to recognize a new common law privacy tort, given the significance of privacy as a *Charter* value. His article was cited by the ONCA when the court elected to do exactly that in *Jones*.[544] The ONCA said:

> The explicit recognition of a right to privacy as underlying specific *Charter* rights and freedoms, and the principle that the common law should be developed in a manner consistent with *Charter* values, supports

---

[542] See e.g., recently *Caplan v Atas*, 2021 ONSC 670 (recognizing new tort of Internet Harassment given changing dynamics of social interaction on the Internet); and even *Jones, supra* note 27 recognizing the significant social changes accompanying more prolific uses of technology.
[543] E.g., *TeBaerts v Penta Builders Group Inc,* 2015 BCSC 2008.
[544] John D.R. Craig, "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997), 52 McGill LJ 355 [Craig, "Invasion of Privacy"].

> the recognition of a civil action for damages for intrusion upon the plaintiff's seclusion.[545]

Craig had, however, advocated for the Ontario courts to draw more directly from *Charter* privacy jurisprudence, including to develop a nuanced test for liability that would recognize privacy beyond territorial or private property-based interests. He included examples like surveillance, stalking, and harassment as harms that could be addressed by a privacy tort as an intrusion into a personal zone of privacy.[546] These are harms that in many cases are not currently vindicated in Canadian tort law when occurring in public spaces.[547] The ONCA did not adopt Craig's recommended approach to the tort, relying instead on the US Restatement of Torts and adopting the US tort of intrusion upon seclusion almost verbatim.

Since *Jones* was decided, lawyer Jared Mackey has also argued that consideration of an additional *Charter* value – expressive freedom – could further inform the common law tort's development, supporting the recognition of a defence for journalist information gathering.[548] Such an approach to understanding the common law privacy tort, by recognizing a broad right that is limited by defences where necessary, would echo the judicial approach to another quasi-constitutional tort - defamation. This approach would also permit, for instance, the application of the privacy tort in public spaces while tempering concerns of overreach through the recognition of defences that can balance sometimes competing interests, like expressive freedom. Additionally, this approach would reflect the general structuring of the privacy statutes, wherein the statute creates a tort for the violation of privacy, followed by exceptions to the scope of the tort that act like and reflect some common defences, like consent. Notably, in other contexts, the Supreme Court has

---

[545] *Jones* at para 46, citing Craig, "Invasion of Privacy", *ibid.*
[546] Craig "Invasion of Privacy", *ibid* at 385-86.
[547] Intentional infliction of mental suffering (IIMS), assault, or battery may address some harms with particular facts, but are not designed to protect a privacy right and will not be available to a plaintiff in many cases of surveillance, stalking, or harassment.
[548] Jared A Mackey, "Privacy and the Canadian Media: Developing the New Tort of 'Intrusion Upon Seclusion' With Charter Values" (2012) 2:1 UWO J Leg Stud 3 [Mackey, "Privacy and the Media"].

addressed the sometimes-competing interests that arise in public space between expression (particularly with regard to journalism) and privacy in public, concluding that neither right is unlimited and that depending on the context a balance can be struck between the two rights.[549] In other words, concerns for free expression need not prohibit all recognition of privacy in public, though may limit the scope of such a right in particular circumstances.

Having noted the relevance of *Charter* values to the interpretation of quasi-constitutional interests like privacy, the next sections consider what some different *Charter* values could mean for the privacy torts, starting with the *Charter* value of privacy. Ultimately the below examination shows that the current interpretation of the torts, including their inapplicability in public spaces, is contrary to at least the *Charter* values of privacy, substantive equality, and arguably expressive freedom. *Charter* values accordingly provide a basis for a re-thinking of the privacy torts, and a rejection of the lingering core philosophy that the torts emerged from, which associates privacy with the home as a man's castle. Below I refer to several potential reforms that can stem from a *Charter* values approach to interpreting and evolving the torts.

The *Charter* Value of Privacy and the Current Interpretation of the Privacy Torts

The *Charter* value that is most immediately relevant to the interpretation of the privacy torts is the *Charter* value of privacy – as has already been recognized by courts and academics alike. As the common law is meant to evolve in line with *Charter* values, it is notable that the *Charter* understanding of privacy has itself evolved over the past decade. In *Charter* claims, courts, including the SCC, increasingly recognize that people *can* reasonably expect privacy in public spaces, and these expectations must sometimes be protected by law. The below analysis examines how the *Charter*

[549] *Aubry, supra* note 50; *Alberta Privacy Commissioner, supra* note 516.

understanding of privacy has evolved over the past decade, and argues that contemporary analysis of the application of the privacy torts must incorporate this evolution in *Charter* doctrine and privacy theory.[550]

How the Courts Understand Privacy & Technology under the Charter

While Supreme Court of Canada *Charter* jurisprudence regarding privacy expectations in public or quasi-public spaces has fluctuated over time, recently it has more firmly recognized the nuanced nature of privacy expectations everywhere, including in public space, especially in light of the emergence of increasingly invasive technologies. Judicial consideration of constitutional privacy protection commonly arises under section 8 of the *Charter,* which stipulates that "everyone has the right to be secure against unreasonable searches and seizures." In order to pinpoint the values that might be reflected in s. 8 jurisprudence, I think it is helpful to briefly explain how courts approach s. 8 assessments of privacy rights.

A "search", within the meaning of s. 8, takes place when state authorities intrude upon an individual's *reasonable* expectation of privacy ("REP"). The court is meant to assess the reasonableness of an individual's expectation of privacy from the perspective of the "reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[551] In other words, this is meant to be a normative, rather than a descriptive, assessment. Courts should assess what a reasonable person should be able to expect in terms of privacy, as opposed to assessing what they might actually descriptively expect (an assessment that could be skewed by the pervasive presence of surveillance technology, for example).[552] Absent an

---

[550] See e.g., *M(A) v Ryan*, [1997] 1 SCR 157 [*M(A) v Ryan*], where the majority explicitly explains that the private law must be updated if it falls out of line with *Charter* values including privacy and substantive equality, which were engaged in that case.
[551] *R v Patrick*, 2009 SCC 17 at para 14 [*Patrick*]; *R v Spencer*, 2014 SCC 43 at para 18 [*Spencer*].
[552] *R v Tessling*, 2004 SCC 67 at para 42 [*Tessling*]; *Spencer, ibid* at para 18.

REP, the court will find that state conduct did not amount to a search, and therefore does not engage s. 8 protection. The assessment of whether an accused's expectation of privacy in something is *reasonable* with regard to the long-term social consequences of the impugned government action is therefore crucial to claiming s. 8 protection. The value the court ascribes to privacy under the *Charter* can at least in part be seen expressed through the ways in which the court understands an expectation of privacy to be *reasonable*. Given the normative approach to assessing REP, the court is essentially determining – when, where, or in what circumstances any individual should be able to expect freedom from interference, and be able to rely on the law to protect that expectation.

The line between reasonable and unreasonable expectations (or, the determination of when privacy should be valued and protected in law) can be difficult to draw.[553] So in order to determine whether an accused has a REP in the subject matter of an alleged search in a s. 8 claim, the Court considers the "totality of the circumstances" in which the state action took place.[554] Among many other things, the Court considers: where the search occurred (e.g., in a public or private area); whether the subject matter was visible to the public; and whether the accused had abandoned her property interest in the subject matter, such that it was accessible to the public.[555]

In early *Charter* jurisprudence, the Court made clear statements that location alone was not meant to determine whether an individual could or could not reasonably expect privacy.[556] Nevertheless, a substantial body of jurisprudence developed around the notion that once someone

---

553 *Tessling, ibid* at para 25.
554 *Tessling, ibid* at para 19; *Patrick, supra* note 552 at para 20.
555 See e.g., *Tessling*, *ibid* and *Patrick, supra* note 552.
556 E.g., *Hunter v Southam*, [1984] 2 SCR 145 at 159, the first SCC decision to consider s. 8 of the *Charter*, the Court adopted from the US constitutional search and seizure jurisprudence the understanding that that s. 8 "protects people, not places", in other words, that search doctrine and the REP analysis are not meant to be a property analysis, but rather protect a personal right that follows a person even when they leave a private residence. In *R v Wise*, [1992] 1 SCR 527 [*Wise*] in concurrence, LaForest J. emphasized that the important qualitative difference between the risk of being fleetingly observed by others, and the risk that an electronic device will track one's every movement. See also, *R v Wong* [1990] 3 SCR 36 where the Court held that one's REP can follow them to a hotel room, and that one's REP is not diminished by the fact they are engaging in illegal activity.

exposed themselves, or information about themselves, to the public, they could no longer expect privacy.[557] The Court's decisions in *Tessling*[558] and *Patrick*[559] in particular reflected this approach. The interpretations of the privacy torts in many ways align with this period of *Charter* jurisprudence.

However, the Supreme Court has since moved away from this line of reasoning, returning to the earlier approach which held that location is not determinative (i.e., public location is not destructive) of privacy expectations. Notably, the Court's 2014 decision in *R v Spencer*, and the early s. 8 decision it draws on in *R v Wise,* underscore how one can expect a degree of privacy in a public place.[560] *Wise* was not referred to in *Patrick,* and only briefly noted in *Tessling* as an example illustrating the diminished REP in a private car.[561] *Spencer* seems to mark the beginning of a stronger return to the Court's earlier reasoning that privacy is not (at least exclusively) tied to private property, and is not automatically lost for any person who is publicly visible. In *obiter* the Court in

---

[557] E.g., *R v Stillman*, [1997] 1 SCR 607, and Lamer CJ and McLachlin J's concurrence in *R v Wong* [1990] 3 SCR 36 at 62-63.

[558] In *R v Tessling, supra* note 553 at para 40, the Court had to assess whether an accused had a REP in heat emanating from his home. Binnie J., writing for a unanimous court, specifically noted in his decision that "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place." But see Ian Kerr and Jena McGill "Emanations, Snoop Dogs and Reasonable Expectation of Privacy" (2007) 52 Criminal Law Quarterly 392; Jena McGill and Ian Kerr, "Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" in J. Bus et al (eds), *Digital Enlightenment Yearbook* (Amsterdam: IOS Press, 2012).

[559] In *Patrick*, *supra* note 552 the Court had to determine whether an accused had an REP in garbage he set out for collection. Given how intimately revealing the information contained in a garbage bag can be, the Court accepted that individuals generally have an REP in household waste (paras 2, 32). However, Binnie J., writing for the majority of the Court, held that the reasonableness of this privacy interest is lost as soon as an accused has done "everything necessary" to designate the garbage for collection – in other words, once the accused has abandoned it to public access (*Patrick, supra* note 552 at paras 25, 55, 62). But see Justice Abella's separate concurring opinion, where she disagreed with the weight that the majority assigned to the property abandonment in this case. She distinguished between one's property interest in the objects in a waste bag, and one's privacy interest in the information revealed by those objects (para 85). In her view, while property abandonment may be one factor to consider in the REP analysis, it should not be determinative of the accused's reasonable expectations with respect to the intimately personal information that can be gleaned from household waste: see paras 80, 83, 88. When one puts his garbage out for collection, he expects it to reach the waste disposal system, "nothing more, nothing less": para 89. She draws a normative, contextually-driven distinction between expecting one's garbage to be collected, and expecting it to be searched by state agents, emphasizing that "[n]o one would reasonably expect the personal information contained in their household waste to be publicly available for random scrutiny by anyone, let alone the state, before it reaches its intended destination": at para 89.

[560] *R v Spencer*, *supra* note 552 at paras 43-44.

[561] *Tessling*, *supra* note 553 at para 22.

Spencer suggests that one can expect privacy in public spaces and information in certain contexts.[562] Subsequent cases have reaffirmed this notion and have further contextualized the REP analysis.

In *Spencer,* the Court had to assess whether associating the accused's identity with his pseudonymous but publicly observable illegal Internet activity amounted to a violation of s. 8. In determining that one's REP includes an expectation of anonymity, the Court emphasized that, "[a]nonymity permits individuals to act in public places but to preserve freedom from identification and surveillance,"[563] such that "[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights."[564] The Court opened the door for a recognition of privacy in public, which soon followed.

It is worth noting that anonymity does still rely on notions of secrecy (even in public, one expects privacy in the fact that their name or identity remains a secret from others).[565] Anonymity would not aid a plaintiff who knows their defendant, as neighbours, intimate partners, classmates, *etc.* Also, while protection of anonymity is significant in public space, it is not the only interest a plaintiff may be seeking to protect. For instance, even where the plaintiff's identity remains anonymous in the encounter, they may be concerned about other forms of transparency or exposure harm, through the collection of other information about them, or from technology-mediated physical intrusion. Nevertheless, Justice LaForest's reasons in *Wise* held that people should not be subjected to warrantless long-term technology-based monitoring, even in public space, simply because such conduct is highly invasive.[566] This reasoning suggests that some forms of surveillance

---

[562] *Spencer, supra* note 552 paras 43-44.
[563] *Spencer, ibid* at para 43.
[564] *Spencer, ibid* at para 44. Also, e.g., Selinger and Hartzog "Obscurity", *supra* note 155; Hartzog, *Privacy's Blueprint, supra* note 430.
[565] Anonymity can also (but does not inherently) engage concerns about equity and accountability. See e.g., Jesssa Lingel, "A Queer and Feminist Defence of Being Anonymous Online" (2021) Hawaii International Conference on Systems Sciences, online: https://scholarspace.manoa.hawaii.edu/handle/10125/70925; Jane Bailey, "'Sexualized Online Bullying' Through an Equality Lens: Missed Opportunity in *AB v Bragg*?" (2013) 59 McGill Law Journal 709.
[566] *R v Wise*, [1992] 1 SCR 527 at 558.

in public space should simply not be permissible without legal oversight, even if the individual is known, and even if others can see them, because it would violate and/or be detrimental for social norms. *Spencer*'s reliance on *Wise* might give weight to a stronger return to such reasoning.

The Supreme Court has also recently adopted a more contextual and relational approach to assessing expectations of privacy in *R v Marakah*.[567] The accused in this case sent text messages to his friend and accomplice about the illegal sale of firearms. When the Crown sought to use the text messages as evidence against him, Marakah argued that the text messages were obtained in violation of s. 8. The majority of the SCC held that "text messages that have been sent and received can, in some cases, attract a reasonable expectation of privacy."[568] The Court emphasized that maintaining control over information "is not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest."[569] Individuals exercise control over the information contained in a text message through the *context* in which they share that information, including with whom they choose to share that information, when, and how they disclose information.[570] According to the Court, these are factors that guide one's expectations around the implications of sharing information.

This line of reasoning is similar to the approach courts and lawmakers have taken to consent and privacy expectations in the context of non-consensual disclosure of intimate images[571] and is reflective of the elements of a breach of confidence as well, which is closely associated with tort law.[572] While *Marakah* does not engage physical public space, it does engage an analysis around

---

[567] *R v Marakah* [2017] 2 SCR 608
[568] *Marakah*, *ibid* at para 4
[569] *Marakah, ibid* at para 38
[570] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009); Waldman, *Privacy as Trust, supra* note 43.
[571] The Court had also recently held in *R v Fearon,* 2014 SCC 77, [2014] 3 SCR 621 that the contents of a phone carry a strong REP, however, the majority found that nonetheless that can be searched incident to a lawful arrest.
[572] *Lac Minerals Ltd.* v *International Corona Resources Ltd.*, [1989] 2 SCR 574: elements at para 129; discussion of *sui generis* nature of the action, with a relationship to tort law, at para 73.

expectations of privacy in information that is accessible to others. How, why, and in what conditions someone normatively ought to expect to be not just seen but rendered transparent in public space can contribute to an analysis of one's reasonable expectation of privacy. However, given the reliance on control (though a more nuanced view of control) in the decision, the analysis may be limited to contexts where one is only *selectively* visible to others (i.e., maintaining a lingering reliance on secrecy/limited control), as opposed to where one might be visible to many others as in public space.

The increasingly nuanced approach to privacy in shared or public contexts in these *Charter* decisions is further reflected in some non-*Charter* Supreme Court jurisprudence. While not *Charter* cases, in each of these decisions the Court is considering the *Charter* value of privacy, either in connection to the Quebec *Charter of Human Rights and Freedoms* or in connection with the Canadian *Charter* jurisprudence. These decisions, perhaps even more so than the s. 8 jurisprudence discussed above, give a sense of what the SCC sees as the *Charter* value of privacy.

In 1998 the Supreme Court of Canada held that a person in Québec could pursue an action against a photographer who took their photograph in a public place and subsequently published it without consent. In its decision in *Aubry v Éditions Vice-Versa*, the majority of the Court held that the right to privacy under the Quebec *Charter* included the right to control the use of one's image. This right is violated upon publication of an image that enables a person to be identified.[573] This is true even if the photograph is taken in a public space, the mere fact of being in public does not undermine one's privacy interests in controlling the use of their image. The Court also acknowledged that such a limitation on the collection and use of information from public space could impede another important value, namely, freedom of expression. In addressing this concern, the Court made reference to the *Charter* values approach to evolving the common law and to

[573] See also *Pia Grillo c Google Inc.*, 2014 QCCQ 9394.

understanding both privacy and expression interests.[574] The Court notes that neither value is absolute and the common law can reflect these sometimes conflicting values by considering the public interest in the publication of a photograph taken in a public space.[575] In this case, there was no overriding public interest in the publication, and the Court agreed that the plaintiff was entitled to compensation for the publication of her photograph.

More recently, the Court also affirmed a contextual approach to privacy expectations in public and semi-public spaces in *Jarvis*, a criminal case involving interpersonal voyeuristic surveillance.[576] The majority decision in this case drew explicitly upon *Charter* doctrine in order to understand and interpret the meaning of privacy within a statutory *Criminal Code* provision. Because Parliament employed the specific terminology of "reasonable expectation of privacy" in the phrasing of the offence, the *Charter* jurisprudence interpreting the meaning of this term was an important part of the legal context for understanding Parliament's intent, according to the majority decision.[577] The analysis therefore also signals what the majority of the Court saw as significant about the *Charter* understanding of privacy.[578] Given the facts of this case, the decision is additionally relevant to the present discussion of tort law's recognition of interpersonal surveillance in public spaces, particularly in response to technology-facilitated privacy harm.

Jarvis had surreptitiously filmed sexual images of students in the public or quasi-public areas of the high school where he worked, using a pen camera. The majority of the Court drew upon s. 8 jurisprudence to aid the assessment of whether the complainants in that case had a reasonable

---

[574] *Aubry, supra* note 50 paras 16-19.
[575] *Aubry, supra* note 50 paras 25-27.
[576] *Jarvis*, *supra* note 540.
[577] *Jarvis, ibid* at para 54.
[578] The minority decision held firm on the use of *Charter* values only as a secondary tool of statutory interpretation – and as they found no genuine ambiguity in the statute, the minority of the Court held that *Charter* values should not apply. The interaction between s. 8 jurisprudence and the Court's interpretation of the *Criminal Code* was a point of contention between the majority and concurring reasons, and with the majority's interpretation that s. 8 could influence this area, it seems possible the court would hold that this decision could also influence s. 8. I would argue that it should and can also be arguably extended to other areas of privacy law, including the privacy torts.

expectation of privacy vis-à-vis Jarvis' filming (a necessary element of the voyeurism offence). The majority decision made important statements about privacy expectations in public and semi-public spaces.

First, the decision affirmed that privacy is not an all-or-nothing concept in public spaces. The mere fact of going out into public does not on its own undermine all expectations of privacy.[579] The majority rejected the notion that once someone can be seen by others, they have lost all expectation of privacy in any circumstance. The REP analysis must instead be contextual, and one's presence in public space is but one of several contextual factors that should be considered. The majority also said the students in this case held a reasonable expectation of privacy vis-a-vis their teacher in part because of the trust relationship and social norms that exist between students and teachers generally. Further, the fact that the technology mediating the surveillance in this case created a permanent record that Jarvis could return to distinguishes the surveillance from the mere fact that the students could be observed by other students, and even by Jarvis, as they made their way around the school.

Professor Jane Bailey has highlighted that these aspects of the decision – including that privacy can normatively be expected in public (contrary to the secrecy approach noted above in earlier *Charter* cases), and the relational and contextual nature of the privacy analysis (including consideration of who the parties are, and their relationships to one another) – are implicitly feminist.[580] These factors bring the analysis closer to one that recognizes the particular ways in which privacy invasions are lived and experienced differently. For instance, violations like voyeurism are particularly targeted at women and girls,[581] and thus to exclude any expectation of privacy simply by

---

[579] *Jarvis, supra* note 540 at para 41.
[580] Jane Bailey, "Implicitly Feminist?: The Supreme Court of Canada's Decision in R v Jarvis" (2020) 32 Canadian Journal of Women and the Law 196 [Bailey, "Implicitly Feminist"].
[581] Bailey, "Implicitly Feminist", *ibid* at 198; Moira Aikenhead, "Non-Consensual Disclosure of Intimate Images as a Crime of Gender-Based Violence" (2018) 30(1) Canadian Journal of Women and the Law 117 [Aikenhead, "NCDII"].

virtue of being in a public space would disproportionately affect the privacy of women and girls in this context. Drawing on the range of circumstances shaping the context of the filming in that case, the Court essentially said the students should normatively be able to expect privacy vis-à-vis their teacher making such recordings.[582]

The *Charter* jurisprudence, and other doctrine interpreting that jurisprudence, make at least several points clear in relation to the understanding of privacy under the *Charter*. Privacy is assessed within all the circumstances of an interaction, which means that the mere fact of being in public or being publicly visible does not on its own negate a reasonable expectation of privacy. Expectations of privacy are normative, which means the courts must consider what a person *should* be able to expect in a given situation, in light of the social value of privacy, and not simply what they could descriptively expect. Privacy is contextual and relational, such that in a privacy conflict it is relevant to consider who the parties are, how they are related, and what that relationship should mean for their expectations vis-à-vis one another. These nuances of the privacy analysis are largely absent from the privacy torts. As explained in Chapter 3, one's presence in public space, or being visible to the public, have been deemed fatal to a privacy claim contrary what courts have recently said about the *Charter* understanding of privacy. In some cases, public space location has also negated any consideration of the other circumstances of a privacy dispute.

For instance, in *Milner*, the court simply relied on the fact that Ms. Milner was visible to the public to find that long-term private investigation surveillance was not a violation of her privacy.[583] Other pertinent factors exist in that case, though, which could be relevant within a more

---

[582] *Jarvis, supra* note 540 at paras 68, 73, 83. See also Lisa Kelly, "A Tale of Two Cameras: Sex and Surveillance in *R v Jarvis*" (2019) 52 Criminal Reports 126-138 [Kelly, "Tale of Two Cameras"] for consideration of the ways in which *Jarvis* continues to echo the gendered approach to privacy as being concerned protecting women's modesty and shielding women's bodies, while simultaneously legitimating the school's use of security cameras to keep students "safe." See also Jane Bailey and Jasmine Dong, "Toward Survivor-Centred Outcomes for Targets of Privacy-Invasive TFVA: Assessing the Equality-Affirming Impact of *R v Jarvis*" in CL Hunt and Robert Diab (eds) *The Last Frontier: Digital Privacy and the Charter* (Toronto, Thompson Reuters: *forthcoming*) 121 at 140-142.
[583] *Milner*, *supra* note 222.

contemporary understanding of privacy. For instance, the court did not consider the implications for Ms. Milner's privacy that a permanent recording was made of her daily life; instead, the surveillance in that case was equated with being seen by any passersby. The relationships in the case may also have been relevant to how Ms. Milner experienced the surveillance, and should be considered in a normative analysis of her REP. For instance, there was no analysis of the fact that she was under investigation because of a disability insurance claim, and how surveillance like this might affect her disability, or may normatively dissuade other individuals from making legitimate claims. There was no normative consideration of whether a reasonable person should *have* to expect pervasive surveillance as a consequence of making a disability claim. Even where there is a perceived need to detect fraudulent claims, there are alternative, more transparent and consent-based means for assessing claims including through medical oversight (while noting that this process can still be fraught for many claimants[584]). The fact that her family was also subjected to surveillance was noted by the court, but apparently did not influence the REP analysis, in particular the court did not consider the harm such family surveillance might have caused to Ms. Milner.

These factors all seem relevant to the analysis in light of the *Charter* and other jurisprudence developing around privacy. Ultimately, I suggest that a relational, contextual, and normative analysis of privacy in this case, that also recognizes the impact such surveillance would have on a person's conduct and ability to live freely in and outside their home (and elsewhere in public space), would conclude that Ms. Milner experienced a violation of privacy. In fact, drawing upon the analysis in Chapter 4, I would argue that Ms. Milner's location should have weighed in her favour in this case. Pervasive surveillance like this has an exposure effect on daily activities like letting one's children play on a front lawn. But even under the current framework for privacy, it could be argued that Ms.

[584] See for e.g., Andrew Pulrang, "Ableist Narratives that Poison Disability Policy and Disabled People's Lives" (December 27, 2019) Forbes, online: <https://www.forbes.com/sites/andrewpulrang/2019/12/27/ableist-narratives-that-poison-disability-policy-and-disabled-peoples-lives/?sh=7499be137eb6>.

Milner's location meets the exact goals of the "home as a man's castle" doctrine – protecting those in their homes or on their property from incursions from public space. The contrary outcome in that case may instead reflect what some of the authors cited in Chapter 4 emphasize about the castle doctrine. It is not actually meant to protect the *home* so much as the interests of specific types of home owners – wealthy, white, heteronormative, able-bodied men – which Ms. Milner was not.

Some of the factors identified in the *Charter* and related jurisprudence would deepen the court's analysis in a case like *Milner*. The current interpretation of the privacy torts is not in line with the current *Charter* value of privacy. A more contextual and normative analysis would be necessary to bring the torts closer in line with the *Charter* privacy value. However, the *Charter* understanding of privacy still does not *value* public space. It has mainly reduced the negative impact of being in public on one's privacy claim. Building on the theory discussed in Chapter 4, I argue below that the courts ought to in fact go deeper in their understanding of the relevance of public space to the privacy claim.

Substantive Equality and the Possibility of Recognizing Public Space Privacy Harm

Substantive Equality as a Charter Value

This sub-section explains what is meant by substantive equality and its conceptualization as a *Charter* value; the next section connects this *Charter* value with privacy. Substantive equality has been recognized by the courts and academics as a significant *Charter* value. In fact, legal academics have argued that substantive equality is a foundational constitutional principle that extends beyond the

scope and requirements of s. 15 of the *Charter*, which explicitly enumerates a right to equal protection and benefit of the law.[585]

The *Charter* s. 15 jurisprudence explicitly calls upon courts to recognize the distinction between formal equality (everyone is treated exactly the same under the law, even if this treatment has differential advantages and disadvantages) and substantive equality (where courts strive to make legal rights and protections equally accessible to everyone, and/or to ensure the law is equally meaningful, taking into account historical and contemporary discrimination and oppression).[586] *Charter* s. 15(1) sets out the right to equal treatment before and under the law, and equal protection and equal benefit of the law without discrimination based on a ground enumerated in the section or one that the court recognizes as analogous to these grounds. The enumerated grounds are race, national or ethnic origin, colour, religion, sex, age, and mental or physical disability. The Supreme Court has recognized sexual orientation, marital status[587], and citizenship as analogous grounds.[588] Section 15 includes the right to be free from discrimination, which occurs when an individual or group are treated distinctly based on a personal, unchangeable characteristic with the purpose or effect of denying a benefit or placing a burden on that individual or group.[589] The values associated with the equality provision are similar to those commonly associated with privacy protection – namely, equality, dignity, freedom, and personal autonomy.[590]

---

[585] Patricia Hughes, "Recognizing Substantive Equality as a Foundational Constitutional Principle" (1999) 22 Dal LJ 5 [Hughes, "Recognizing Substantive Equality"] emphasis added; Angela Cameron and Paul Daly, "Furthering Substantive Equality Through Administrative Law: Charter Values in Education" (2013) 63 Supreme Court Law Review (2d) 169. Kerri Froc, "Constitutional Coalescence: Substantive Equality as a Principle of Fundamental Justice" (2012) 42 Ottawa Law Review 411.

[586] *R v Kapp,* [2008] 2 SCR 483 at paragraph 15, citing *Andrews v Law Society of British Columbia*, [1989] 1 SCR 143 at 165; see also *Withler v Canada*, [2011] 1 SCR 396 at paragraph 39; *Kahkewistahaw First Nation v Taypotat*, [2015] 2 SCR 548, at paragraph 17; *Quebec (Attorney General) v Alliance du personnel professionnel et technique de la santé et des services sociaux*, [2018] 1 SCR 464, at paragraph 25; and *Fraser v Canada (Attorney General)*, 2020 SCC 28 at paragraphs 41-42.

[587] *Miron v Trudel*, [1995] 2 SCR 418.

[588] Employment status, marijuana/drug use, and membership in the military have been held not to be analogous grounds.

[589] *Canadian National Railway Co v Canada (Canadian Human Rights Commission)*, [1987] 1 SCR 1114 at para 33.

[590] *Quebec (Attorney General) v A*, 2013 SCC 5 at paras 135, 140 [*Quebec v A*].

If a law has the effect of discriminating, even if discrimination was not intended, it can be found to be in violation of s. 15.[591] Notably, the courts will recognize that seemingly neutral laws, that are written as though they apply equally to everyone, can actually be discriminatory in their application or effect. As Justice Abella recently explained in *Quebec v A* (writing for the majority on s. 15(1)), "the purpose of the s. 15 equality provision is to eliminate the exclusionary barriers faced by individuals in the enumerated or analogous groups in gaining meaningful access to what is generally available."[592] She emphasized, in synthesizing the s. 15 case law, that enumerated and analogous groups have been historically discriminated against, and s. 15 is meant to curtail such ongoing discrimination.[593] She underscored that claimants do not need to prove that specific attitudes or intentions of prejudice motivate the distinction or exclusion of a group from legal protection.[594] If the group is excluded from legal protection or benefit on the basis of on an enumerated or analogous ground, or in a way that has the effect of worsening marginalization, it should be found to be discriminatory.[595] Or as McLachlin CJ explained in her reasons, concurring with Abella J: "what constitutes discrimination requires a contextual analysis, taking into account matters such as pre-existing disadvantage of the claimant group, the degree of correspondence between the differential treatment and the claimant group's reality, the ameliorative impact or purpose of the law, and the nature of the interests affected."[596]

Drawing on s. 15 jurisprudence, professor Patricia Hughes has defined the *Charter* principle of substantive equality as:

---

[591] *Eldridge v British Columbia (Attorney General)*, [1997] 3 SCR 624 at para 60.
[592] From headnote, summarizing the synthesis of s. 15 law within the judgment.
[593] As she succinctly summarizes: "The root of s. 15 is our awareness that certain groups have been historically discriminated against, and that the perpetuation of such discrimination should be curtailed. If the state conduct widens the gap between the historically disadvantaged group and the rest of society rather than narrowing it, then it is discriminatory": *Quebec v A, supra* note 591 at para 332.
[594] *Quebec v A, ibid* at paras 327-333.
[595] *Quebec v A, ibid.*
[596] *Quebec v A, ibid* at para 418.

> a form of equality which is satisfied only if *policy or law is made meaningful for all members of society*, including those who have been racialized or systemically defined by gender, sexuality, or disability or similar kinds of characteristics, as well as intersecting identities; in contrast, formal equality is satisfied if everyone is treated as subject to the law or is subject to it in the same way.[597]

Professor Diana Majury has described substantive equality as follows:

> Substantive equality recognizes that in order to further equality, policies and practices need to respond to historically and socially based differences. Substantive equality looks to the effects of a practice or policy to determine its equality impact, recognizing that in order to be treated equally, dominant and subordinated groups may need to be treated differently.[598]

As noted above with regard to s. 8, interpreting the law through the lens of the *Charter* value of substantive equality does not necessitate the application of the *Charter* s. 15 analysis. In some ways, the courts may actually have more flexibility in applying substantive equality as a *Charter* value in the development of the private law, than in directly resolving *Charter* claims, given the complexity of the analysis in a *Charter* claim.[599]

Professors Angela Cameron and Paul Daly explain how, in an administrative context for instance, exercising decision-making discretion in accordance with the value of substantive equality would mean that the decision-maker considers the impact of their decision on historically disadvantaged groups.[600] In administrative decisions, this would mean:

> applying home statutes in ways that *take into account difference between Canadians*, within the parameters of their legislative mandate. In other

---

[597] Hughes "Recognizing Substantive Equality", *supra* note 586 at 7, also cited in Cameron and Daly "Furthering Substantive Equality", *supra* note 535.
[598] Diana Majury, "The Charter, Equality Rights, and Women: Equivocation and Celebration" (2002) 40(4) Osgoode Hall LJ 297 at 305.
[599] Observation raised by Professor Sonia Lawrence at Tackling Technology Facilitated Violence Workshop, May 25, 2021.
[600] Cameron and Daly, "Furthering Substantive Equality", supra note 535 at 191.

> words, administrative decision-makers must *consider how equality-seeking groups may be subject to their home statute in different ways depending on their social location*.[601]

Substantive equality values call on decision-makers to consider the social and legal context of the respective claimants. While a different type of decision-making process is engaged in the administrative context than in the tort law context,[602] this guidance - that the value of substantive equality prompts a decision-maker to consider the impact of their decision on historically disadvantaged groups, and whether the law protects differently based on a claimant's social location - is pertinent to considering the role of substantive equality values in a tort privacy dispute too.

Substantive equality emphasizes at least two important guidelines for courts: (1) neutrally phrased laws are not inherently equitable, and (2) courts should accordingly be mindful of differential impact and applicability for historically marginalized groups. Drawing on the discussion throughout the preceding chapters I argue that the judicial resistance to recognizing privacy in public space means that the benefits of the law (the privacy torts) do not apply equally, including on the basis of various enumerated and analogous grounds, such as race, sex, age, disability, *etc.* Accordingly, substantive equality values lend further support to reform of the current interpretation of the privacy tort, including as it applies to technology-mediated privacy conflicts in public spaces.

Substantive Equality is Relevant to Privacy

Scholars have repeatedly emphasized the significance of equality values for Canadian tort law broadly,[603] as well as for various privacy laws and protections specifically.[604] The Supreme Court of

---

601 Cameron and Daly, "Furthering Substantive Equality", *ibid* at 191, emphasis added.
602 One that has also evolved since Cameron and Daly's publication, see *Vavilov*.
603 Chamallas, "Architecture of Bias", *supra* note 34; Adjin-Tettey, "Discriminatory Impact," *supra* note 22; Ken Cooper-Stephenson, "Corrective Justice, Substantive Equality and Tort Law" in Ken Cooper-Stephenson and Elaine Gibson (eds), *Tort Theory* (North York: Captus University Publications, 1993) 48 at 49 [Cooper-Stephenson, "Corrective Justice"]: "tort law locates itself in, and is throughout influenced by, a socio-legal context which includes important norms of substantive equality," and at 58: "[Intentional] tort law is mostly useful in addressing confrontations where *ex ante* the plaintiff and defendant stood in a position of *in*equality – where there was an unequal balance of psychological or physical power." Where there is equality in power, a defence might be more likely to apply – tort is commonly useful for protection of the relatively powerless: Cooper-Stephenson "Corrective Justice" at 59.
604 See especially Jane Bailey, "Towards an Equality-Enhancing Conception of Privacy", *supra* note 31 at 295; Jane Bailey, "Missing Privacy Through Individuation: The Treatment of Privacy Law in the Canadian Case Law on Hate, Obscenity,

Canada has also previously held that the *Charter* values of privacy and equality intersect in ways that are relevant within the scope of tort law. In *M(A) v Ryan*, the Court held that the law of privilege, and requirements for disclosure of a therapeutic records about a plaintiff to a defendant in a tort action, must evolve with regard to the *Charter* values of privacy and equality.[605] The case drew on doctrine related to the *Criminal Code* "*Mills* regime"[606] that guides courts in ordering disclosure of records in cases involving sexual assault. Writing for the majority, Justice McLachlin (as she then was) said:

> …the common law must develop in a way that reflects emerging *Charter* values. … One such value is the interest affirmed by s. 8 of the *Charter* of each person in privacy. Another is the right of every person embodied in s. 15 of the *Charter* to equal treatment and benefit of the law. A rule of privilege which fails to protect confidential doctor/patient communications in the context of an action arising out of sexual assault perpetuates the disadvantage felt by victims of sexual assault, often women. The intimate nature of sexual assault heightens the privacy concerns of the victim and may increase, if automatic disclosure is the rule, the difficulty of obtaining redress for the wrong. The victim of a sexual assault is thus placed in a disadvantaged position as compared with the victim of a different wrong. The result may be that the victim of sexual assault does not obtain the equal benefit of the law to which s. 15 of the *Charter* entitles her. She is doubly victimized, initially by the sexual assault and later by the price she must pay to claim redress -- redress which in some cases may be part of her program of therapy. These are factors which may properly be considered in determining the interests served by an order for protection from disclosure of confidential patient-psychiatrist communications in sexual assault cases.[607]

---

and Child Pornography" (2008) 31(1) Dalhousie Law Journal 55 at 281; Lise Gotell, "When privacy is not enough: Sexual assault complainants, sexual history evidence and the disclosure of personal records" (2006) 43 Alberta Law Review 743 at 750; Aikenhead, "NCDII", *supra* note 582; Scott Skinner-Thompson, *Privacy at the Margins* (Cambridge: Cambridge University Press, 2021); Waldman, *Privacy as Trust, supra* note 43; Thomasen & Dunn, "Reasonable Expectations of Privacy", *supra* note 154.

[605] *M(A) v Ryan*, *supra* note 551 at para 23 on *Charter* values: "ensuring that the common law of privilege develops in accordance with "*Charter* values" requires that the existing rules be scrutinized to ensure that they reflect the values the *Charter* enshrines. This does not mean that the rules of privilege can be abrogated entirely and replaced with a new form of discretion governing disclosure. Rather, it means that the basic structure of the common law privilege analysis must remain intact, even if particular rules which are applied within that structure must be modified and updated to reflect emerging social realities."

[606] See e.g., *R v Quesnelle*, 2014 SCC 46.

[607] *M(A) v Ryan, supra* note 551 at para 30.

McLachlin J emphasized that the law must develop in such a way that it recognizes the particular impact that onerous disclosure requirements have on survivors of sexual assault, many of whom are women (the dissent also recognized that children and people with disabilities are especially impacted by the onerous requirements). A neutral approach to disclosure requirements, which does not consider such particular impact, would mean that survivors of sexual assault would not obtain equal *benefit* of the law of tort – they would suffer much greater privacy consequences as a result of a decision to pursue an action for compensation than would a plaintiff not suing for sexual assault. This distinction would occur *because* the law is applied equally to all claimants regardless of impact (reflecting formal equality).[608]

The wholescale exclusion of privacy rights in public space can also lead to discriminatory results in terms of the effectiveness and meaningfulness of the law for some plaintiffs. For instance, individuals can experience surveillance targeting differently based on their social location or identity.[609] One's race, gender, disability, or other identity factors might cause them to experience more frequent surveillance or qualitatively different surveillance, and different consequences resulting from that surveillance.[610]

---

[608] Justice L'Heureux-Dubé's dissenting opinion, while not forming the law, relied heavily on *Charter* values of privacy and equality in finding that a judge must exercise their discretion in ordering disclosure in line with *Charter* values. She explicitly noted that sexual assault predominantly affects women, children, and those with disabilities. Accordingly, the privacy interests engaged by a records production precedent that would allow disclosure of therapeutic records in such cases will disproportionately affect these groups, and so must be developed with regard to the value of equality.

[609] See for example, Anita Allen *Uneasy Access: Privacy for Women in a Free Society* (Totawa, New Jersey: Rowan & Littlefield 1988); Anita Allen, "Privacy torts: Unreliable remedies for LGBT plaintiffs" (2010) 98(6) California Law Review 1711; Anita Allen & Erin Mack "How privacy got its gender" (1991) 10 Northern Illinois University Law Review 441; Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham, North Carolina: Duke University Press, 2015); A Crosby & J Monaghan, *Policing Indigenous Movements: Dissent and the Security State* (Winnipeg: Fernwood Publishing, 2018); Davis, D. "The harm that has no name: Street harassment, embodiment, and African American Women" (1994) 4 UCLA Women's Law Journal 133-178; Tulloch, M. *Report of the independent street checks review* (Toronto: Queen's Printer for Ontario, 2018); Khiara Bridges, "The Poverty of Privacy Rights" (2011) 34 Harv J L & Gender 113; Michele Gilman, "The Class Differential in Privacy Law" (2012) 77 Brook L Rev 1389; Skinner-Thompson, *Privacy at the Margins*; Anil Kalhan, "Immigration Surveillance" (2014) 74 Maryland Law Rev 1.

[610] *Ibid.* And see, Selinger and Hartzog "Obscurity", *supra* note 155.

Furthermore, access to the kinds of private spaces that currently provide individuals with legally protected privacy is unequally distributed as a result of social and legal oppression, on the basis of many of the enumerated grounds.[611] This is particularly true for individuals who are unhoused or precariously housed, and/or for those who rely on government assistance and support.[612] While housing and/or economic status are not recognized as an enumerated or analogous ground under s. 15, statistical research overwhelmingly shows that homelessness and poverty are experienced at far greater rates in Canada at the axes of enumerated and analogous grounds.[613] An interpretation of the privacy torts that wholly excludes privacy rights in public space can be said to be substantively inequitable – it fails to be equally meaningful for everyone – on the basis of how and where people find privacy, and experience privacy harms differently. As discussed in Chapter 4, such inequality was specifically embedded in the early doctrine, upon which the current Canadian torts are premised. Equality values, like privacy values, can support the development of a more nuanced approach to understanding privacy within the scope of tort law, accompanied by the rejection of the historically inequitable basis for why public space was excluded from tort protection in the first place.[614]

---

611 E.g., Cheryl Harris, "Whiteness as Property" (1993) 106(8) Harvard Law Review 1707.

612 See the examples investigated by Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (New York: St. Martin's Press, 2017); Khiara Bridges "Privacy Rights and Public Families" (2011) 34 Harvard Journal of Law & Gender 113.

613 Natalie Rech, "Homelessness in Canada" (July 9, 2019) The Canadian Encyclopedia, online: <https://www.thecanadianencyclopedia.ca/en/article/homelessness-in-canada>.

614 The Supreme Court of Canada has rejected the notion of a standalone tort of discrimination in *Bhadauria v Seneca College*, [1981] 2 SCR 181. The Court declined to recognize a standalone tort for discrimination because the Canadian legal system offered an alternative statutory mechanism for addressing concerns of direct discrimination through Human Rights Codes. Notably, the decision was rendered before the *Charter* was in effect, and it has been critiqued both in relation to whether the alternative mechanism provides the sort of recourse the court imagined (see e.g., Larry Chartrand, "The Crumbling Wall of *Bhadauria*: If Not Today, Tomorrow" (2009) 44 Supreme Court Law Review 107-134) and whether such an action could alternatively arise in negligence (see: Rakhi Ruparelia, "'I Didn't Mean it that Way!: Racial Discrimination as Negligence" (2009) 44 Supreme Court Law Review 81). None of this ought to stand in the way of a *Charter* values interpretation of tort law, as implied for instance by the fact the Court did not hesitate to interpret the law of civil disclosure through the Charter values of privacy and equality in *M(A) v Ryan, supra* note 551. See also: Kate Sutherland, "Precedent, Principle and Pragmatism: Justice Wilson and the Expansion of Tort Law" (2008) 41 Supreme Court Law Review 131-160 at 133-137, Justice Wilson authored the ONCA decision in *Bhadauria* in which the Court initially recognized the tort of discrimination.

That said, even with a recognition of the possibility of expecting privacy in public space, Chapter 3 outlined a number of ways in which the current interpretation of the privacy torts might limit their application to technology-based interpersonal intrusions. For instance, public space surveillance might not be considered significant or offensive *enough* to a reasonable person, because of where it takes place, if it is temporally limited, or if it does not engage anything courts consider offensive or embarrassing; the use of technology could complicate the analysis of whether the defendant *wilfully* invaded a plaintiff's privacy; the defendant might argue they have a claim of right for their conduct in protecting their property from members of the public; information that has already been shared or is publicly visible might not be considered a "private" fact; *etc.* Many of these factors arose in the case law in connection with how the courts have understood public space – as a space of inherent and consensual publicity/visibility. Some of these considerations can perhaps be more fulsomely considered in the privacy tort analysis, with reform to how the courts approach an understanding of privacy in public space.

The next section considers potential reforms that could be supported through a substantive equality values approach to the privacy torts. While I consider this reform at an abstract level (i.e., not in regard to a specific individual or group), these reforms are suggested with an aim to make the interpretation of the law more substantively equitable, which should purportedly be a goal for the evolution of tort even absent specific discrimination in a particular dispute between parties. Further, these reforms seek to place value on public space, and recognize the role that privacy can play in supporting a more equitable public space.

What Substantive Equality Values Can Mean for the Privacy Torts

Interpreting the privacy torts with regard to the *Charter* value of substantive equality could mean at least three things for their relevance to technology-mediated public space privacy conflicts,

the last of which also engages considerations of expressive freedom. First, substantive equality values (in conjunction with privacy values noted above) could call upon the courts to consider social/normative privacy expectations in public space, beyond the specific interaction between the plaintiff and defendant. Integrating substantive equality and privacy values could support judicial consideration of what a plaintiff *ought* to be able to expect in the circumstances (in line with the s. 8 normative approach), but with a further view to substantively equitable access to and application of the law.[615] In other words, courts should nuance the normative approach to also consider and care about substantive equality in the effect of the law.

Second, substantive equality values can support a more nuanced assessment of a purported privacy violation, beyond strictly objective legal tests. The objective analysis of privacy expectations has to-date limited the court's assessment of the "circumstances" that are relevant to a privacy analysis. A more subjective-objective analysis would permit parties to contextualize a dispute and contribute to the court's normative assessment of whether the plaintiff ought to be able to expect privacy in the circumstances.[616]

Relatedly, and finally, I suggest that substantive equality values would support the courts recognizing the social *value* of public space location within the privacy analysis. In other words, rather than approaching the analysis asking whether the plaintiff could expect privacy *despite* being in public space, the court could consider whether the parties' presence in public space raises additional normative reasons to protect privacy. This final point also engages considerations about the *Charter* value of expressive freedom, which I suggest can be enhanced (and not just undermined, as is often assumed) through more robust recognition of privacy in public space. Notably, each of these

---

[615] For those who view tort law as driven predominantly by corrective justice concerns, this may at first blush seem counter to the corrective justice approach of focusing on the interaction specifically between the parties to a claim, but here I turn to the many instances where Canadian tort law already considers policy factors in the legal analysis (outlined in Chapter 1).

[616] See e.g., Hunt, "Privacy in the Common Law," *supra* note 355.

proposed reforms has support elsewhere in the law as well, including in the privacy jurisprudence outlined earlier in the chapter.

A Normative Understanding of Privacy: What Level of Surveillance Ought *We Accept in Public Space*

The current interpretation of the privacy torts considers privacy at the level of the individual. While courts and many academics have noted that individual privacy rights can also contribute to broader social values, like democracy,[617] most often in the tort case law addressing privacy in public spaces, this is not a consideration.[618] As discussed above, *Charter* privacy values could support a normative approach to assessing a plaintiff's privacy rights and expectations in a dispute, asking what one should be able to expect, "from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy."[619] In this section, I suggest substantive equality values can support an even deeper and more nuanced judicial analysis of a plaintiff's reasonable expectations of privacy through a normative lens. This analysis could consider what level of privacy people ought to expect in public space, given privacy's social importance as a component of accessible and equitable public and shared spaces.

Privacy and equality scholars have emphasized how individualistic approaches to privacy overlook systemic and group impacts of surveillance and privacy invading conduct, leading to (or failing to address) substantive inequality. For example, professor Jane Bailey has explained how the

---

[617] See e.g., Anita Allen, *Uneasy Access, supra* note 407; and as discussed in Chapter 5.
[618] While an individual-focused approach would align with the typical focus on individual rights in tort law and views that tort law should reflect corrective justice principles, as noted earlier, Canadian tort scholars have challenged the perception of a limited focus of corrective justice in Canada, citing the ways in which courts already consider broader social questions when resolving tort disputes.
[619] *R v Spencer*, *supra* note 552 at para 18.

atomistic individual-level view of privacy obscures the court's ability to recognize the "discriminatory social context leading to [a] situation, and … the ramifications of the particular conception of privacy for the broader equality-seeking community."[620] A strictly individual-level analysis fails to recognize and thus address the systemic forces and stereotypes that might underlie a privacy conflict, or lead to its emerging in the first place, and/or that can shape the ways in which a plaintiff experiences harm.[621] As Bailey notes,

> the historic legacy of an atomistic conception of privacy risks continuation of an analysis that pits individual against individual in a competition that reinforces the notion we are dealing with a completely individualistic and "private" realm, while ignoring the political realities which shape that realm, the imbalance of power between individuals within it and the legitimate public interest in intervening in an attempt to right the balance.[622]

Professor Lise Gotell similarly highlights that a strictly individual-level framing of privacy *prevents* the flourishing of substantive equality within the community:

> The claim to privacy is attached to the isolated individual, not the community; it has no social dimensions and thus lacks capacity to express collective interests in the struggle against gender and racial subordination. … feminist critics have emphasized how privacy reinforces the idea that the personal and private are distinct from the social and political. As Schneider writes, "[p]rivacy encourages a focus on the individual and avoidance of collective definition, systemic analysis and social responsibility."[623]

---

[620] Jane Bailey, "Towards an Equality-Enhancing Conception of Privacy" *supra* note 31 at 281.
[621] *Ibid.* "Since traditional privacy analysis focuses on the particular situation of the particular individual claiming its protections, *attention is all too often and too easily diverted from the discriminatory social context leading to that situation*, and from the ramifications of the particular conception of privacy for the broader equality-seeking community": Bailey, "Equality-Enhancing", *supra* note 31 at 295, emphasis added. See also Jane Bailey, "Missing Privacy Through Individuation: The Treatment of Privacy Law in the Canadian Case Law on Hate, Obscenity, and Child Pornography" (2008) 31(1) Dalhousie Law Journal 55 [Bailey, "Individuation"].
[622] Bailey, "Equality Enhancing", *supra* note 31 at 283.
[623] Lise Gotell, "When privacy is not enough: Sexual assault complainants, sexual history evidence and the disclosure of personal records" (2006) 43 Alberta Law Review 743 at 750.

While tort law is not designed to recognize collective rights (e.g., under which a plaintiff might sue for harm experienced at a group level rather than on an individual basis[624]), through the lens of both privacy and equality values, the privacy torts could nevertheless take a more explicit normative approach to evaluating a plaintiff's privacy expectations. As under the *Charter* privacy doctrine, courts can reflect social and collective considerations about the value and expectations we *ought* to ascribe to privacy in public spaces when assessing the level of privacy a plaintiff ought to be able to expect in a set of circumstances.

Charter privacy jurisprudence has emphasized that the "expectation of privacy is a normative rather than a descriptive standard."[625] The court is meant to consider and be concerned with "the degree of privacy needed to maintain a free and open society, not necessarily the degree of privacy expected by the individual or respected by the state in a given situation…".[626] In other words, the court is meant to consider what degree of privacy should be maintained in the interests of and benefit to society.[627]

While tort actions would continue to be resolved at an individual level (e.g., compensating the individual plaintiff(s) for their personal harm, not collective injury or loss), this analysis turns the court's attention to the question of collective interests in what the law ought to say is or is not permissible, which can have social impacts. A normative approach to the REP analysis that considers substantive equality might consider whether, for instance, members of equity-seeking groups must expect and endure certain forms of targeted or discriminatory surveillance that arise because of one's social location or identity. Referring to the *Milner* case again, we may imagine a

---

[624] The public nuisance tort might provide some foundation here, but is exceptional within tort law and requires a plaintiff to suffer special damage – damage that lasts an unreasonable amount of time, in unreasonable circumstances. Claims can also be brought by the Attorney General. See e.g., Philip H. Osborne, *The Law of Torts*, 6th ed (Toronto: Irwin Law, 2020).
[625] *R v Tessling, supra* note 553 at para 42.
[626] *R v Ward*, 2012 ONCA 660 (CanLII), 97 CR (6th) 377 at para 86.
[627] Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011) 54 Supreme Court Law Review 335.

specific judicial consideration of whether, as a society, we normatively condone that an individual making a disability claim must expect to subsequently be surveilled (in public and private spaces) to confirm the validity of their claim. On a normative level, such an outcome should be rejected when such surveillance would likely discourage other legitimate claims, undermining the role of group insurance plans and undermining the ability of the disabled community to access financial supports. Or in the alternative, it would undermine the ability of the disabled community to freely access and use public space, as individuals will be subjected to constant exposure and transparency harms. Such a decision would perpetuate discrimination in the form of ableism – a person who would not otherwise experience pervasive (or even limited) surveillance experiences this solely because of seeking financial support for disability. Such an outcome directly conflicts with substantive equality values.

In considering the social and normative impacts of such surveillance, courts can continue to engage a balancing of interests (e.g., considering the defendant's reasons for the surveillance), wherein countervailing factors (e.g., evidence providing a *reasonable* basis for suspecting a fraudulent claim) can also be considered. I argue here, though, that any counter-arguments in support of surveillance should also be understood within the broader context of substantive equality, which would mean the court should consider the impacts on the community where countervailing considerations are accepted as justifications for surveillance. I also suggest that a *Charter* values approach would justify a reconsideration and moving away from past judicial decisions where courts have simply accepted surveillance as a consequence of insurance claims, without engaging in a normative analysis of the implications of that finding for the claimant, the community, and for access to and use of public space more generally.

Another example would arise if the students in the *Jarvis* case were to bring a tort privacy action[628] for the voyeuristic privacy violation they experienced. Under the current doctrine, the court might simply ask whether the students could reasonably expect not to be seen when in the public and shared spaces of the school, as the ONCA did in the criminal proceedings. However, this approach was rejected by the SCC majority. Were the court to take a normative approach to the question of 'private affairs' and 'highly offensive' intrusions for the purposes of an intrusion upon seclusion tort, it might ask whether the plaintiffs ought to be able to expect not to be surreptitiously filmed by their teacher in the shared and public spaces of their school. These are spaces where the students must co-exist with the teacher in order to have access to an education; and spaces where they co-exist and socialize with their peers, an activity that should be socially/normatively fostered, but that could be undermined through an awareness of sexualized surveillance.[629] In fact, one of the complainants from *Jarvis* has spoken publicly about how the surveillance has affected her ability to move comfortably through public and shared spaces even years after the voyeuristic surveillance took place.[630]

Such a normative approach might lead to a result more similar to that in the SCC majority decision in *Jarvis*, where the court found that the conduct in that case engaged an REP. However, if the court were to approach the normative analysis also through a substantive equality lens, it should specifically ask whether women and girls ought to expect gender-based filming when they move

---

628 As one student has already, but engaging different legal mechanisms: Colin Butler, "Ex-teacher who filmed students with spy pen, Ontario school board named in $200K civil suit" (April 23, 2021) CBC News, available online: <https://www.cbc.ca/news/canada/london/ryan-jarvis-beal-voyeurism-civil-lawsuit-1.5996802>.

629 Notably, these spaces were also under school surveillance. Considering impact on public space experience through a normative lens, we might also imagine a challenge to this surveillance. However, through the same analysis, we can understand some of the differences between these forms of surveillance too. Nevertheless, school surveillance may differentially impact student experiences of the space, and may even be targeted at students differently in spite of a seemingly neutral appearance of filming everyone. See e.g., Kelly, "Tale of Two Cameras," *supra* note 583.

630 Amy Dodge, "This voyeurism case changed Canadian privacy laws. It also changed this victim's life" (February 12, 2020) CBC News, online: <https://www.cbc.ca/news/canada/london/this-voyeurism-case-changed-canadian-privacy-laws-it-also-changed-this-victim-s-life-1.5458776#:~:text=Canadian%20privacy%20laws.-,It%20also%20changed%20this%20victim's%20life,teacher%20secretly%20filmed%20her%20chest>.

through shared and public spaces and whether such filming should meet the 'highly offensive' threshold, given evidence that it is predominantly women and girls who experience this form of privacy intrusion, as was argued at the SCC.[631] Much like the disclosure requirements at issue in *M(A) v Ryan*, the court could recognize the specific gendered nature of the intrusion in its analysis, and specifically assess the plaintiff's claim within that context. Something that might not be considered a privacy violation under current tort doctrine can be seen as such when a normative approach is taken to the analysis. Substantive equality values could nuance the normative analysis in such a way that the tort is not only capable of appreciating the social value of privacy, but also, can recognize the interests of parties who experience privacy violations specifically due to their social location and identity.[632] Jane Bailey and Jasmine Dong found in reviewing post-*Jarvis* decisions that in fact the contextualized privacy analysis from that decision influenced a broader systemic analysis of privacy in some sexualized technology-facilitated violence criminal cases. In other words, *Jarvis* appeared to offer the possibility of grounding a more normative and intersectional understanding of privacy, at least in the context of the *Criminal Code* offences relating to sexualized violence.[633] Such an approach ought to be echoed in tort, especially given the relevance of the same *Charter* values.

Considering the REP analysis through a normative lens, i.e. focusing on what kind of privacy one *should* be able to expect in the plaintiff's circumstances (as opposed to what the plaintiff did or could expect in the circumstances), and particularly considering REP with a view to enhancing substantive equality values, could also ground an explicit judicial rejection of the historical trajectory of the torts.[634] Such a rejection would, I suggest, provide some freedom for courts to break with

---

631 Factum of the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic; Factum of the Intervener, Women's Legal Education and Action Fund Inc., *J v Jarvis* SCC Court File No: 37833; Aikenhead, "NCDII", *supra* note 582; Bailey and Dong, "Impact of *Jarvis*," *supra* note 583.
632 See also Thomasen & Dunn, "Reasonable Expectations of Privacy," *supra* note 154.
633 Bailey and Dong, "Impact of *Jarvis*", *supra* note 583 at 140-142.
634 Chapter 4 explained that the privacy torts evolved from gendered, raced and colonial norms centered around the home and private property. While these norms are no longer explicitly central to the torts, their legacy is never the less apparent in some judicial reasoning. In particular, this legacy underscores the sharp reliance on location in the US

entrenched doctrine and precedent – particularly the decisions that deny any privacy in public and shared spaces. The common law and judicial interpretation of statutes rely on consistency with past decisions to ensure fairness and predictability within the law. To diverge from prior precedent requires judicial justification. My suggestion here is that a recognition and rejection of the historical trajectory provides that crucial justification permitting re-interpretation of the torts' application and relevance to interpersonal privacy conflicts in public spaces.

Notably, this analysis is also pertinent to defendants. Where a plaintiff brings a claim against a defendant on grounds that involve stereotyping or discriminating against the defendant; or where the defendant is engaging in socially valuable surveillance (e.g., journalism in the public interest; or self-defensive uses[635]) a normative analysis of whether the plaintiff ought to be able to expect privacy in the circumstances would allow the courts to recognize these nuances and distinguish them from other claims. Defendants might also engage with expressive freedom values, which could be balanced at this stage in assessing whether the plaintiff had a reasonable expectation of privacy, and at the defences stage of the analysis in assessing whether despite *prima facie* violating privacy, the defendant had a legitimate defence for their conduct, as discussed further below.[636] The analysis in this thesis has focused primarily on whether and how courts should recognize tort privacy in public spaces, however all of the factors involved in recognizing the value of public space can also apply to considering the value of public space to defendants. The notion of a normative and substantively equitable approach to privacy should be reflected throughout the balancing of competing individual interests too. Developing the tort with an eye to substantive equality has the potential to create a more adaptable legal test than is currently employed under the privacy torts.

---

doctrine which informed Canada's torts, wherein public location decimates a plaintiff's claim regardless of any other circumstances that might be relevant to a plaintiff's experience of privacy harm.

[635] See e.g., Jennifer Chandler, "Technological Self-Help and Equality in Cyberspace" (2010) 56(1) McGill Law Journal 39.

[636] See also e.g., Mackey, "Privacy and the Media," *supra* note 549.

Subjectivity, Objectivity and a Reasonable Expectation of Public Space Privacy

The above suggestions that a normative analysis of privacy could recognize concerns around stereotyping and discrimination engage a second consideration for the development of the privacy torts – namely, recognizing the subjective lived experience and expertise of the parties as part of the relevant context for the legal analysis.[637] A central tenet reflected in *Charter* s. 15 jurisprudence is that the equality protected by s. 15 is *substantive* equality, not formal equality. While a law or legal test may apply the exact same way to everyone (formal equality), its effect might be particularly harsh, or particularly meaningless, for different people depending on their circumstances. Section 15 seeks to recognize this in particular when that differential impact is experienced on the basis of an enumerated or analogous ground. The notion of *substantive* equality could provide further guidance for the development of the privacy torts, particularly in relation to technology-mediated public space privacy conflicts. In particular, courts might take closer consideration of the plaintiff's experience of privacy harm, including especially (but not necessarily exclusive[638] to) when connected to or on the basis of an enumerated or analogous ground. This could be done through judicial openness to some subjectivity in the privacy analysis, such as by considering whether a reasonable person in the position/positionality of the plaintiff should be able to expect privacy in the circumstances.

Some privacy scholars have already argued that the torts require some consideration of subjective privacy expectations and experience within the privacy test.[639] Unlike the s. 8 *Charter* analysis, the privacy torts do not have an explicit element requiring the court's consideration of a *subjective* expectation of privacy (which, while explicit, has also received little practical weight in the *Charter* jurisprudence). The four statutory torts do explicitly call for courts to consider the

---

[637] On expertise, see e.g., Ngozi Okindegbe, "Discredited Data" (2022) 107 Cornell Law Review (*forthcoming*).
[638] One of the surprising benefits of a *Charter* values, rather than a *Charter*, analysis.
[639] See: Hunt, "Privacy in the Common Law", *supra* note 355; Thomasen & Dunn, "Reasonable Expectations of Privacy", *supra* note 154; also, Mayo Moran, *Rethinking the Reasonable Person: An Egalitarian Reconstruction of the Objective Standard* (Oxford: Oxford University Press, 2003) [Moran, *Rethinking the Reasonable Person*].

relationship between the parties, either in the context of assessing whether there was a violation of privacy, or in Manitoba, in assessing damages.[640] The intrusion upon seclusion tort calls for consideration of the relationship between the parties at the damages stage as well. Scholars have emphasized the importance for the court to recognize the subjective relational dimensions of a privacy violation under the torts – through the relationship between the parties, as well as the ways in which privacy violations can undermine social relationships.[641]

To date in the tort case law, there has been relatively little if any consideration of relationships, power-dynamics, stereotyping or discrimination, or other contextual factors in the privacy in public analysis. For instance, I have already discussed how some of these factors arose in *Milner* but were not considered in the analysis. Rejection of ableist stereotyping that assumes untrustworthiness of a claimant,[642] the impact of surveillance on a person already experiencing a disability that requires leave from work, the power dynamic of one's insurance company covertly and pervasively surveilling one's family could have factored into considering what Ms. Milner or another plaintiff in her position ought to be able to expect in the circumstances. But the decision was framed through a "neutral" objective lens asking what would *any* reasonable person expect in the circumstances. As many legal scholars have emphasized though, this fictitious objective "reasonable person" also has subjective characteristics, they are simply implied rather than explicitly considered.[643] As Jane Bailey has emphasized, the courts have *always* considered subjective context in a privacy dispute, but the analysis has only focused on *familiar* contextual factors:

> Historically … the context implicitly taken into account actually reflected the experiences and narratives of the white, cis, wealthy, males who

[640] B.C. *Privacy Act* at s. 1(3) *Saskatchewan Privacy Act* at s. 6(2), Newfoundland *Privacy Act* at s. 3(2); in Manitoba these circumstantial factors are to be considered in awarding damages – Manitoba *Privacy Act*, s. 4(2).
[641] E.g., Hargreaves, "Relational Privacy", *supra* note 368; Kerr, "Shrödinger's Robot," *supra* note 204; and Waldman, *Privacy as Trust, supra* note 43.
[642] E.g., Heenan, "Challenging Stereotypes," *supra* note 475.
[643] Moran, *Rethinking the Reasonable Person, supra* note 640; Bailey, "Equality Enhancing", *supra* note 31; Hadley Friedland, "Making Space for the Cree Reasonable Person in the Canadian Justice System" (2016) 67 UNB Law Journal 269.

> dominated judicial ranks. The degree of commonality in their experiences was sufficiently uniform that it came to be thought of as just the way things are, rather than as a contextualized perspective born of living in a particularly privileged social location.[644]

By virtue of not considering the disability dimensions of that interaction, the court is implicitly enacting a "reasonable person" who is able-bodied. If the reasonable person were a person who, like over 22% of the Canadian population,[645] experiences a disability, these factors would be pertinent to that analysis.

Even in *Jones v Tsige*, the foundational privacy tort case in Ontario, the parties involved were engaged in a complex inter-personal relationship, which was noted in the facts but is never considered in the privacy analysis. The court focused on the secret nature of Ms. Jones' banking record, but did not further consider the privacy impact on Ms. Jones of her ex-partner monitoring her accounts through his new partner. When considering what a "reasonable person" ought to expect in these circumstances, the court could consider the power dynamics of inter-partner surveillance to emphasize that aside from the specific nature of what was being monitored, individuals in Ms. Jones' position should be able to expect not to be monitored by former romantic partners. In fact, the courts have yet to note the overarching factor that all of the significant privacy tort cases in Ontario have involved intimate-partner surveillance or privacy violations by a male partner of their female ex or current partner.[646] While intimate partner and gender-based surveillance

---

[644] Bailey, "Implicitly Feminist", *supra* note 581 at 214. See also Valerie Steeves, "If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective" (2008) 50 Canadian Journal of Criminology and Criminal Justice 331 (examining the discrepancy between the judicial understanding of privacy and what is known about people's actual online experiences and expectations).

[645] Government of Canada, "Making an Accessible Canada for Persons with Disabilities" (last updated February 4, 2022; accessed February 15, 2022) online: < https://www.canada.ca/en/employment-social-development/programs/accessible-canada.html>.

[646] Notably in the NCDII cases the courts have recognized the gender dynamics in privacy violations, but this has not been recognized widely throughout tort law yet.

is clearly an issue that drives tort law claims, the dynamics of intimate partner surveillance can be too easily overlooked through the non-reflective use of an "objective" reasonable person standard.

Through the lens of evolving the privacy torts in line with substantive equality values, it is notable that the Supreme Court has already recognized, for instance, that systemic colonialism,[647] racism,[648] and sexism,[649] exist in society and in the legal system, and that this can mean that a 'reasonable person' legal standard requires more context and nuance in the judicial analysis than is granted at first blush. In other words, where the court has recognized that systemic forces are at play in an interaction between either private individuals or individuals and the state, the court has also acknowledged that to understand how these forces affect the parties (and to resolve the legal dispute), a degree of subjectivity is necessary in the analysis.

Perhaps the clearest example of this was in L'Heureux-Dubé and McLachlin JJ's reasons (concurring in outcome with Cory J's majority reasons) in *R v RDS*.[650] RDS, a Black youth, had been charged with resisting arrest and other charges relating to an interaction with a police officer. The trial judge, Justice Sparks, who is also Black, indicated an awareness that police officers in the local community tended to be racist toward young Black men. The Crown appealed her acquittal of RDS

---

[647] The SCC has explicitly recognized anti-Indigenous racism within society and the legal system on a number of occasions, and has recognized the intersection between anti-Indigenous racism and sexism/misogyny more recently as well. E.g., *R v Williams,* [1998] 1 SCR 1128 (court recognizes anti-Indigenous racial prejudice within society, which will be alive in the context of jury selection. Drawing on *Charter* values, including equality, the Court held that the judge should have exercised his discretion to allow Williams to challenge jurors for cause related to concerns of bias against him); *R v Gladue*, [1999] 1 SCR 688 (the SCC emphasized the need for judges to consider systemic and background factors when sentencing an Indigenous person, because of the ways in which systemic and direct discrimination lead to overrepresentation of Indigenous individuals in the criminal law system and a qualitatively more harmful experience of that system); in *R v Ipeelee*, [2012] 1 SCR 433 at para 60 the SCC stated quite clearly that "courts must take judicial notice of such matters as the history of colonialism, displacement, and residential schools and how that history continues to translate into lower educational attainment, lower incomes, higher unemployment, higher rates of substance abuse and suicide, and of course higher levels of incarceration for Aboriginal peoples." See also *R v Barton*, 2019 SCC 33, *R v Kokopenace*, 2015 SCC 28.

[648] The SCC has recognized racism in general, and anti-Black racism in particular, are also present throughout Canadian society and in the legal system. *R v Parks*, 1993 CanLII 3383 (ONCA): recognized that overt and subconscious racism toward Black people exists in Canada; *R v Golden*, [2001] 3 SCR 679 para 83. See also *R v Zora,* 2020 SCC 14.

[649] The SCC has recognized sexist myths and tropes throughout society and the legal system, particularly in relation to sexual assault, that are especially harmful to women, children, and people with disabilities. See e.g., *R v Mills*, [1999] 3 SCR 668; *R v Quesnelle*, 2014 SCC 46; *R v Ewanchuck*, [1999] 1 SCR 330.

[650] *R v RDS*, [1997] 3 SCR 484 [*RDS*].

alleging a reasonable apprehension of bias in her decision. The Supreme Court was asked to consider whether Justice Sparks' comments about her knowledge of how police have been known to lie on the stand and to overreact in interactions with non-white groups raised a reasonable apprehension of bias. The test to assess reasonable apprehension of bias considers what the "reasonable person" would think of the comments. The majority reasons held that the comments did not raise a reasonable apprehension of bias, though similar comments could in different circumstances. L'Heureux-Dubé and McLachlin JJ's concurrence rejected that analysis, finding that not only did the comments not raise an apprehension of bias, they were entirely acceptable and conducive to a fair trial and resolution of the case, as a reflection of the Justice Sparks' own lived experience and knowledge of the local community.

In assessing what the perspective of a reasonable person would think of Justice Sparks' comments, L'Heureux-Dubé and McLachlin JJ explained that the reasonable person would have an understanding of the community,[651] including "the history of discrimination faced by disadvantaged groups in Canadian society protected by the *Charter*'s equality provisions."[652] They lay-out their understanding of the 'reasonable person' from whose perspective the legal analysis is to take place, in a highly nuanced and contextualized way as follows:

> The reasonable person is not only a member of the Canadian community, but also, more specifically, is a member of the local communities in which

[651] *RDS, ibid* Para 37: "It follows that one must consider the reasonable person's knowledge and understanding of the judicial process and the nature of judging as well as of the community in which the alleged crime occurred."
[652] *RDS, ibid* para 46. "The reasonable person, identified by de Grandpré J. in *Committee for Justice and Liberty*, *supra*, is an informed and right-minded member of the community, a community which, in Canada, supports the fundamental principles entrenched in the Constitution by the *Canadian Charter of Rights and Freedoms*. Those fundamental principles include the principles of equality set out in s. 15 of the *Charter* and endorsed in nation-wide quasi-constitutional provincial and federal human rights legislation. The reasonable person must be taken to be aware of the history of discrimination faced by disadvantaged groups in Canadian society protected by the *Charter*'s equality provisions. These are matters of which judicial notice may be taken": *RDS* para 46. The justices referred approvingly to Doherty J.A.'s decision in *Parks*, where he explained in regard to anti-Black racism: "Racism, and in particular anti-black racism, is a part of our community's psyche. A significant segment of our community holds overtly racist views. A much larger segment subconsciously operates on the basis of negative racial stereotypes. Furthermore, our institutions, including the criminal justice system, reflect and perpetuate those negative stereotypes." *R v Parks* (1993), 15 OR (3d) 324, leave to appeal denied at 342.

> the case at issue arose (in this case, the Nova Scotian and Halifax communities). Such a person must be taken to possess knowledge of the local population and its racial dynamics, including the existence in the community of a history of widespread and systemic discrimination against black and aboriginal people, and high profile clashes between the police and the visible minority population over policing issues. The reasonable person must thus be deemed to be cognizant of the existence of racism in Halifax, Nova Scotia. It follows that judges may take notice of actual racism known to exist in a particular society.
>
> […]
>
> We conclude that the reasonable person […] is a person who approaches the question of whether there exists a reasonable apprehension of bias with a complex and contextualized understanding of the issues in the case. The reasonable person understands the impossibility of judicial neutrality, but demands judicial impartiality. The reasonable person is cognizant of the racial dynamics in the local community, and, as a member of the Canadian community, is supportive of the principles of equality.[653]

The *RDS* decision lays out a contextual assessment of what is "reasonable" in a given set of circumstances drawing on *Charter* equality values to guide this assessment. The Supreme Court has also contextualized the reasonable person standard in the context of assessing whether a claimant was detained by police, in the context of a s. 9 *Charter* challenge for arbitrary detention. In both *R v Grant,*[654] and more recently *R v Le*,[655] the Court explained explicitly how the race of the claimant and knowledge of police mis-treatment of racialized communities factor into the assessment of whether a 'reasonable person' would have believed they were being detained. In fact, the majority in *Grant* identifies a number of characteristics including minority status, age, physical stature, and level of sophistication, as pertinent to this analysis.[656] In other words, the court will consider what a reasonable person *in the shoes of the plaintiff*, given all the contextual characteristics relevant to an

[653] *RDS* at paras 47 and 48 (internal citations removed).
[654] *R v Grant*, [2009] 2 SCR 353 [*R v Grant*].
[655] *R v Le*, 2019 SCC 34 [*R v Le*].
[656] *R v Grant, supra* note 655 at para 44

interaction with police, might do or believe. The Court noted that, though the analysis is predominantly an objective one, the claimant's subjective perspective can be relevant "in assessing the reasonableness of any perceived power imbalance between the individual and the police."[657]

The majority in *Le* was clear that the race of the claimant and the ways in which the police interact with racialized members of the community can factor explicitly into the analysis of whether a reasonable person with the claimant's characteristics would believe there has been a detention.[658] The objective "reasonable person" standard is to be situated within the context of the encounter, as the majority says in *Le* at para 82:

> A reasonable person in the shoes of the accused is deemed to know about how relevant race relations would affect an interaction between police officers and four Black men and one Asian man in the backyard of a townhouse at a Toronto housing co-operative.[659]

While these cases engage *Charter* claims and interactions with the state, each of these cases emphasize the importance, including for substantive equality, in approaching the reasonable person *in the context of the claimant* with a view to the subjective qualities of the interaction.[660] Such an

---

[657] *R v Grant, ibid* para 32. However, the majority does not address Mr. Grant's race and how that would factor into his experience of the interaction with police. Only the concurring reasons by Binnie J note that Mr. Grant is Black and that this might factor into a reasonable person in his shoes feeling as though they cannot walk away from the interaction, contributing to a determination they were psychologically detained: *Grant, ibid* at paras 154-55; 176.

[658] *Le, supra* note 656 at paras 69-106. "Evidence about race relations relevant to the detention analysis, like all evidence of social context, can be derived from "social fact" or the taking of judicial notice. The information necessary to inform the reasonable person can take the form of reliable research and reports that are not the subject of reasonable dispute; and, rarely, direct, testimonial evidence.": at para 71.

[659] *Le, ibid* at para 83: "Evidence about race relations that may inform whether there has been a detention under s. 9, like all social context evidence, can be proved in legal proceedings by direct evidence, admissions, or by the taking of judicial notice. The realities of *Charter* litigation are that social context evidence is often of fundamental importance, but may be difficult to prove through testimony or exhibits. To be sure, social context evidence is a type of "social fact" evidence, which has been defined as "social science research that is used to construct a frame of reference or background context for deciding factual issues crucial to the resolution of a particular case" (*R v Spence*, 2005 SCC 71, [2005] 3 SCR 458, at para. 57)."

[660] *Le, ibid* para 81: "the racial context analysis relevant to the timing of the detention under s. 9 is not inward-looking, but rather focuses on the relational aspect between the police and racialized communities in order to discern what a reasonable person in the circumstances would perceive. The focus under s. 9 is thus on what a reasonable person in the shoes of the accused would perceive […]." Also *Le* at para 75: "the question is how a reasonable person of a similar racial background would perceive the interaction with the police. The focus is on how the combination of a racialized context and minority status would affect the perception of a reasonable person in the shoes of the accused as to whether they were free to leave or compelled to remain. The s. 9 detention analysis is thus contextual in nature and involves a wide-ranging inquiry. It takes into consideration the larger, historic and social context of race relations between the

approach recognizes that the claimant brings into any situation all of their lived experience, which shapes their understanding of the interaction and the potential harm that will be or has been inflicted upon them. While there are important policy reasons to maintain some objective analysis of privacy,[661] evolving the law to approach this objective analysis from the plaintiff's perspective would allow the parties and the court to draw upon more contextual factors that are relevant to determining whether there was a privacy violation in a given scenario. This would allow the court to more closely assess issues like wilfulness, claims of right by defendants, and plaintiff's expectations vis-à-vis remotely-operated technologies. Notably, there are precedents for an objective-subjective type of analysis throughout other areas of law as well, including tort law.[662]

In tort cases involving interpersonal claims, allowing for some subjective consideration and allowing for parties to bring their positionality to bear as pertinent to a contextual analysis, can also be relevant to the defendant. This may arise for instance in counter-arguments with regard to the subjective relationship between the parties (e.g., in persuading the court of which contextual factors shape the nature of the interaction and the plaintiff's reasonable expectations of privacy) and where defences engage a reasonable person analysis. By nuancing the analysis to allow parties to explain how their positionality and subjectivity affects their expectations of others, the court can engage a more nuanced, contextual, and realistic assessment of what a plaintiff ought to normatively expect in a given encounter. This sort of contextual analysis would also assist the court in limiting the scope of the tort in public space, such that the courts can recognize circumstances in which plaintiffs could

police and the various racial groups and individuals in our society. The reasonable person in Mr. Le's shoes is presumed to be aware of this broader racial context."

[661] E.g., the tort would become unpredictable in its application if solely based on subjective standards; also, this could lead to inequitable results where two people experience the same harm but held subjectively different expectations of privacy and are thus differently compensated.

[662] E.g., the tort of assault and the defence of self-defence allow for consideration of the objective reasonable person in the *subjective position* of the plaintiff.

not reasonably expect privacy, not based on the inequitable historical trajectory of the tort, but rather based on a more comprehensive understanding of the context of the interaction between the parties.

For instance, such a balancing of subjective-objective contextual factors in assessing the plaintiff's privacy claim could be engaged in a case like *Vertolli*.[663] This was the privacy dispute arising in Ontario in which the plaintiff, a police officer who pulled over the defendant Crawford, was suing Crawford and YouTube for intrusion upon seclusion as a result of a video Crawford filmed of the incident, and subsequently posted on YouTube. While the decision in this case was simply a motion to dismiss, which the plaintiff successfully defeated as the court found he had a reasonable cause of action (he has not yet succeeded in proving his claim), were the case to have gone further it may engage some factors discussed throughout this sub-section. The plaintiff was an on-duty police officer at the time of the incident. He had pulled over the defendant. The plaintiff acknowledged in the video that it was within the defendant's right to record the interaction. However, the plaintiff argues that subsequently posting the video on YouTube intrudes upon his seclusion. YouTube refused to remove the video, as the company found there was no violation of privacy.

The facts in the decision do not provide any further contextual details. However, it is notable that the parties agreed that the filming itself was permissible. The analysis above and in Chapter 3 has identified different impacts of visually observing someone, *vs* filming that person, *vs* then making subsequent use of the footage. In such an interaction the defendant could not simply argue that the plaintiff had no expectation of privacy vis-à-vis posting the video solely because he was visible to the defendant, as the defendant went beyond observation, to also permanently record and share the interaction. That said, the privacy analysis here should also ask whether an on-duty police officer ought to reasonably expect privacy from the person whom they have detained? Drawing on contextual factors the court should consider the power-imbalance between the parties,

[663] *Vertolli, supra* note 296.

the manner in which being on-duty and in uniform places one in a position of public responsibility and visibility, and the fact that the interaction specifically engaged that public responsibility. Based only on the factors provided in the decision, an officer in this position may not reasonably expect privacy vis-à-vis the filming if the normative implications of such an expectation would be to entrench an even deeper vulnerability for people detained by police than already exists in the power dynamic between these parties. The reasoning should *not* be that when an officer is in public space, they can expect no privacy simply by virtue of being in public space.

The defendant's subsequent posting of the video engages further contextual considerations, for which the motion decision only provides minimal facts. This case is framed as an intrusion upon seclusion, presumably because publication of a private fact had not yet been recognized in Ontario. Drawing on the *Charter* values analysis outlined above, I suggest that the same normative and contextual analysis should inform the question of whether sharing video on the Internet is a highly offensive intrusion, and/or a private fact for the purpose of the publication tort. The court might ask whether, in all the circumstances, the plaintiff ought to be able to expect that the interaction would not be made available to the public at large? While there may be other factors that would support the plaintiff's claim that were not provided in the brief *Vertolli* decision, again the fact that the plaintiff was on-duty and engaged in his public function, one which involves asserting power over the defendant, and without any factors to suggest the filming or publication were driven by stereotyping or discriminatory grounds (which could be pertinent to a normative analysis), the court could find that the subsequent publication of the video did not violate the plaintiff's privacy.

This reasoning would be distinguishable from a case of a publication of, for example, Ring footage showing a plaintiff engaged in everyday personal activities in public spaces. Such footage should be much more likely to come within the scope of invading one's private life, when the plaintiff is engaged in private daily activities, as opposed to a public service function. Again, the

finding in *Vertolli* should be driven by other factors than an overly simplistic finding that solely because the encounter arose in a public space, the plaintiff therefore has no right to privacy. More details would be needed to finally resolve the *Vertolli* case, but a subjective-objective and normative analysis of the claim would encourage the parties to frame their arguments within the nuanced context of the interaction. Furthermore, a normative, contextual analysis that considers the parties subjective lived experience and is underpinned by the value of substantive equality, can be even further nuanced by a direct consideration of the *value* of public space itself and the relevance of this space in the privacy conflict. This is the subject of the next and final sub-section.

Recognizing the Value of Public Space, and the Role Privacy Plays in Shaping Public Space

Chapter 5 discussed some of the ways in which a person can experience privacy harm specifically because they are in public space – e.g., where surveillance undermines one's ability to express themselves, to participate in the public community, or to access spaces that are purportedly open to the public. Accordingly, where privacy rights are not recognized in public space, those who experience surveillance in such a way that it causes public space privacy harms like exposure and transparency may lose access to or use of public space. In other words, privacy rights can play a role in equitable access to and use of public spaces. The theory of public space privacy harm set out in Chapter 5 suggests that rather than reforming the torts by eliminating or minimizing the negative impact of public space location in the REP analysis, judges should instead shift their thinking to understand the *value* that public space location can have in the privacy analysis. For a court considering the normative expectations of privacy in the plaintiff's circumstances, substantive equality and expressive freedom values should support a recognition that public space location can be a positive factor supporting a plaintiff's claim of privacy in certain circumstances.

Sossin and Friedman point out that the *Charter* value of expressive freedom has been relied upon at all levels of legal decision-making including court, administrative, and tribunal decision-making.[664] It has arisen as a *Charter* value influencing the development of tort law, in particular in defamation jurisprudence.[665] It has also arisen in cases dealing with journalist-sourced privilege and picketing.[666] The SCC decision, *Dolphin Delivery*, which first introduced the role of *Charter* values into private litigation, involved secondary picketing and freedom of expression values.

Expressive freedom values protect the quest for truth, the promotion of individual self-development, and participation in the community.[667] The *Charter* right of freedom of expression under s. 2(b) has a spatial nexus. The court will consider the characteristics of a place where s. 2(b) rights are said to be infringed in assessing whether there has been a *Charter* violation. This assessment includes considering whether the place is one where free expression typically occurs, and whether the place is one that is compatible with open public expression.[668] Free expression values and protections are stronger in such places.

In *Montreal (City),* the SCC confirmed that free expression in public spaces is the default expectation.[669] Chief Justice McLachlin and Justice Deschamps explain: "One aspect of free expression is the right to express oneself in certain public spaces. Thus, the public square and the speakers' corner have by tradition become places of protected expression."[670] The court recognized

---

664 Sossin and Friedman, *supra* note 530 at 416-418.
665 *Hill, supra* note 520; *Grant v Torstar, supra* note 525.
666 *R v National Post*, 2010 SCC 16 (re: source privilege); *RWDSU Local 558 v Pepsi-Cola Canada Beverages (West) Ltd*, [2002] 1 SCR 156 at paras 106-107 (re: picketing).
667 *R v Keegstra*, [1990] 3 SCR 697 (also cited in *Hill, supra* note 520 at para 104): "Hate propaganda contributes little to the aspirations of Canadians or Canada in either the quest for truth, the promotion of individual self-development or the protection and fostering of a vibrant democracy where the participation of all individuals is accepted and encouraged." See also the phrasing in Irwin Toy: (1) democratic discourse; (2) truth-finding; and (3) self-fulfillment: *Irwin Toy Ltd. v Quebec (Attorney General)*, [1989] 1 SCR 927, at 976.
668 *Montréal (City) v 2952-1366 Québec Inc*, [2005] 3 SCR 141 at para 76 [*Montreal (City)*].
669 *Montreal (City), ibid* at paras 64, 72-74.
670 *Montreal (City), ibid* at para 61. Also, at para 81: "Viewed from the perspective of locus, the expression falls within the public domain. Streets are clearly areas of public, as opposed to private, concourse, where expression of many varieties has long been accepted."

that not all expression in public space will be protected, but one's presence in public space does lend weight to a claimant's argument.[671]

Chapter 5 lays out some of the ways in which access to public spaces and expressive values can be limited by surveillance. Law and social science research support the recognition that surveillance can stifle or chill how one behaves and communicates with others – surveillance has a panoptic effect on people under its gaze.[672] Scholarship examining the social value of privacy, some of which was introduced earlier in Chapter 5, also emphasizes the importance of privacy to a thriving social realm and political system.[673] Where interpersonal surveillance has the effect of limiting how one engages in or uses public space, expressive freedom values, in conjunction with substantive equality values and a normative approach to a privacy assessment, would support a recognition of individual privacy and rights in public spaces in certain circumstances.

It would be up to the plaintiff to explain to the court how their access to or use of space was affected by surveillance. Expressive freedom is often seen in conflict with privacy – for instance, where privacy laws threaten to prevent journalistic investigation, or publication of images in the public interest.[674] However, depending on the circumstances of a case, where such surveillance

---

[671] E.g., *Committee for the Commonwealth of Canada v Canada*, [1991] 1 SCR 139, 77 DLR (4th) 385; *Calgary Airport Authority v Canadian Centre for Bio-Ethical Reform*, 2019 ABQB 29; *Batty v Toronto*, 2011 ONSC 6862; *Federated Anti-Poverty Groups of BC v Vancouver (City)*, 2002 BCSC 105. Courts have prioritized interests of pedestrian and vehicular efficiency over the interests of individuals in making non-dominant use of public spaces, including for protest and income generating through e.g., panhandling, See: Nicholas Blomley, *Rights of Passage: Sidewalks and the Regulation of Public Flow* (New York: Taylor & Francis, 2010); Kristen Thomasen, "Robots and Public Space", *supra* note 88.

[672] E.g., Jon Penney, "Understanding Chilling Effects" (2022) 106 Minnesota Law Review (forthcoming) available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855619; see also Valerie Steeves, "Privacy, Free Speech and Community: Applying Human Rights Law to Cyberspace" in Steven Hick, Edward F Halpin, Eric Hoskins (eds) *Human Rights and the Internet* (London: Palgrave Macmillan, 2000).

[673] Reagan, "Common Good", *supra* note 423; Hughes, "Social Value of Privacy", *supra* note 426; Valerie Steeves, "Reclaiming the Social Value of Privacy," *supra* note 428.

[674] The ONCA in *Jones* and Mackey in "Privacy and the Media," *supra* note 549 for example have suggested that expression interests could justify relevant defences to intrusion upon seclusion. E.g., *Jones, supra* note 27 at para 73.

impedes one's use of or access to shared and community spaces, such surveillance engages forms of privacy harm that *also* limit expressive freedom.[675]

Zeliony v Dunn, for instance, offers an opportunity to consider the role of location in the plaintiff's claim. This was the case in which the defendant was operating a Ring doorbell camera that faced into the shared entryway space between the parties' condominiums, through which the plaintiff had to pass to access her home. The case does not engage public space, rather shared space, and parties did not raise any issues regarding expressive freedom. Nevertheless, the facts can allow for some consideration of the importance and value of public (or shared) space in the privacy analysis.

The court held that the common, shared nature of the entry way space lowered Ms. Zeliony's REP in the circumstances.[676] The court also referred to the fact that there was no evidence that Mr. Dunn's camera filmed inside Ms. Zeliony's private unit.[677] But the plaintiff also made clear in her evidence, reflected in the court's decision, how the surveillance was affecting her ability to move between her home and the public world. Mr. Dunn used various settings on the Ring camera such that sometimes it was recording the shared spaces outside the neighbouring homes, and other times it was not. Nevertheless, the plaintiff's arguments suggest that she was perpetually worried that it could be recording her movements. Consideration of the exposure impact of the recording on Ms. Zeliony is relevant to her privacy claim.

In considering whether the plaintiff ought to be able to reasonably expect privacy in this case, additional factors not considered by the court might include that one at least ought to be able to

---

[675] The SCC has previously addressed such balancing between privacy in public and expressive freedom in other legal contexts, on which courts can draw. See e.g., *Aubry, supra* note 50. See also the balancing in *MA v Ryan*, *supra* note 551 while not engaging expressive freedom, engaging another important *Charter* value in balance with privacy. See also Richards, *Intellectual Privacy*, supra note 467.

[676] *Zeliony, supra* note 17 at para 29.

[677] *Zeliony, ibid* at para 31. Implying if she could connect the surveillance to her private property, then she may have had a more persuasive case, drawing back to the 'man's castle' approach to privacy analyses.

avoid or disengage from unwanted surveillance, and in this case, the location of the filming appeared to make that impossible for the plaintiff. Also, on a normative level, courts might find that people should be able to expect not be subjected to (potentially pervasive) surveillance from a person with whom they are engaged in an active dispute, especially where that surveillance cannot be spatially avoided. The tense relationship between the parties led to the surveillance, but it may also arguably have aggravated the privacy experience for the plaintiff. It seems from the plaintiff's own evidence that this was the case for her. This surveillance apparently affected her to the extent that she sold her unit and moved to a new location.[678] That a plaintiff must alter their spatial behaviour, in this case to a fairly extreme degree, should factor into a normative REP analysis.

This is not to say all of these factors should be considered alone, they must be considered within all of the circumstances some of which also support the defendant's claims. Nevertheless, these factors should be considered. While the expressive freedom concerns are not front and center in the court's decision in *Zeliony*, one might consider (depending on further facts), for example, whether this surveillance curbs or undermines a 'reasonable person' in the plaintiff's position from participation in the neighbourhood or condominium community. By selling her unit and moving away, the plaintiff's conduct suggests this dispute had a substantial impact that included a spatial dimension – the need to leave the space, and perhaps a community/neighbourhood, to avoid the conflict.

In *Zeliony* there were other circumstances at issue, which are worth considering here for completeness of the analysis. The court weighed Ms. Zeliony's "minimal," if any, REP against Mr. Dunn's interests in protecting his property. I suggest based on the above discussion that Ms. Zeliony may actually have a strong REP. She relied on that shared space and had to make regular use of it, therefore she ought to be able to expect freedom from threat of pervasive surveillance and

[678] E.g., *Zeliony, supra* note 17 at para 7.

interpersonal policing by someone with whom she is in a dispute. This higher expectation, weighed against the "claim of right" might alter the court's ultimate decision. Notably, the claim of right argument, as previously discussed, also engages the historical trajectory of the torts that I have argued courts should reject. I am not suggesting that by rejecting reliance on this historical trajectory, the court can never consider property damage or property interests in a privacy assessment. Rather, property interests should not simply override all privacy interests.

In *Zeliony*, the property damage *engaged* privacy interests – first, tampering with a light, and then with a surveillance camera; not that this justifies property damage, rather, in a similar case the evidence may suggest that surveillance is *not* an effective or reasonable response to damage arising from privacy concerns. In this case, the condominium board had stepped in to mediate with the parties in regards to the tampering with the defendant's property. From a defendant's view, the damage might make the use of the camera feel more valid, and Mr. Dunn did modify the settings so the camera would not always record. But courts must be cautious that 'claim of right' is not interpreted so broadly as to permit surveillance whenever the defendant has, even a mistaken, belief that surveillance is justified to protect privacy.[679] Having rejected the supremacy of property interests, the court would be presented with a high REP – driven by an understanding of the spatial impact of the surveillance – for a plaintiff who has clearly asserted their concerns with surveillance. That surveillance itself seems to be part of the motivator for the property damage and tampering. I would argue *Zeliony* was not an appropriate case for claim of right to override expectations of privacy.

In all of the circumstances, considering the high REP, and the defendant's perceived claim of right, based solely on the facts known from the decision (which may have been presented differently under a different interpretation of the statute), the plaintiff would appear to have a claim for

[679] E.g., *Zeliony, supra* note 17 at para 33.

violation of her privacy, for which damages might be mitigated by the defendant's justifications for using the camera. Such a finding, that the plaintiff's privacy has been invaded by a Ring system, finds support in other jurisdictions as well.[680]

I also note that in support of the 'claim of right' assessment in *Zeliony*, the court drew upon a defence set out in the Manitoba *Privacy Act*, which can be raised by a defendant where their impugned conduct is reasonable, necessary for, and incidental to the defence of property (s. 5(c)). Ideally, courts should not use defences to justify a finding that a plaintiff has no *prima facie* claim. This case sets a precedent suggesting there is no violation of privacy in analogous circumstances, when some of the court's reasoning would actually only be appropriate after a finding of a *prima facie* claim, in considering whether or not a defendant has a defence.[681] The Manitoba tort could be interpreted by courts more generously knowing that the legislature has specifically identified occasions where a *violation of privacy* (i.e., a successful *prima facie* claim) can be defended, such that there would be no liability for the defendant. The presence of defences to the statutory privacy torts plays a crucial policy role in constraining the scope of the tort; but can and should only arise in defence of the defendant's actions (rather than in narrowing the scope of a plaintiff's statutory rights).

In further regards to balancing countervailing arguments in a privacy dispute, statutory defences also already include some protections for freedom of expression.[682] At common law, self-defence

---

[680] E.g., Dan Milmo, "Amazon asks Ring owners to respect privacy after court rules usage broke law" (October 14, 2021) The Guardian, available online: <https://www.theguardian.com/uk-news/2021/oct/14/amazon-asks-ring-owners-to-respect-privacy-after-court-rules-usage-broke-law> (UK court upholds harassment claim by one neighbour against another for use of Amazon Ring, under UK *Data Protection Act 2018* and UK *General Data Protection Regulation*.

[681] The court provides no direct discussion of defences in the decision. However, briefly, having found a violation of privacy, the court in *Zeliony* would then go on to consider if that violation was reasonable and *necessary* for purposes of protecting property. Relevant factors here might include that the tampering has stopped, that the condominium board has stepped in (perhaps allowing for an alternative resolution to the dispute, rendering surveillance less or not necessary), and that the surveillance seems to be an aggravating factor in the tampering (perhaps making it a less reasonable response).

[682] See e.g., B.C. *Privacy Act*, s 2(3)(a) stipulating that it is not a violation of privacy if a matter is published in the public interest or constitutes fair comment on a matter of public interest. Similar provisions exist in Saskatchewan's *Privacy Act* at s. 4(2); Manitoba's *Privacy Act* at s. 5(f) and Newfoundland's *Privacy Act* at s. 5(2).

and consent are widely accepted defences to intentional torts. Additionally, courts have developed free expression-protecting defences for defamation, which could be influential for the development of privacy defences too.[683] Defendants have a number of opportunities to defend their conduct, without narrowing the scope of the privacy rights in public spaces. With regard to expressive freedom specifically, I suggest that these interests can be engaged both by plaintiffs and defendants, particularly when surveillance engages public spaces. Ultimately, I argue that the intersection of substantive equality and expressive freedom dictate that it is relevant to the court's analysis of a plaintiff's claim if their use of and access to public space has been compromised by surveillance.

Conclusion

This chapter has argued that in light of the quasi-constitutional nature of the privacy torts and the judicial recognition that the common law should evolve in line with *Charter* values, reform to the privacy torts is necessary and possible. Such reform could make the torts a more relevant legal mechanism in interpersonal technology-mediated privacy disputes. Notably, the *Charter* value of privacy does *not* exclude privacy in public spaces – and thus nor should the torts. When considering both privacy and substantive equality values together, there is a legal basis for evolving the torts in a way that recognizes privacy in public spaces. In particular, courts should assess what degree of privacy plaintiffs ought to be able to expect vis-à-vis interpersonal surveillance considering the long-term implications of the impugned surveillance on society, and valuing substantive equality in the meaningfulness and application of the law. In recognizing the social benefit of privacy, where surveillance compromises a plaintiff's use of or access to a shared or communal space, this should give *greater weight* to the plaintiff's REP, rather than less, as has often been the case in the

[683] E.g., Mackey, "Privacy and the Media," *supra* note 549.

jurisprudence to date. Finally, courts should reject the historical and inequitable view that privacy interests arise exclusively from seclusion or secrecy, particularly associated with private property and the home. Privacy has spatial value, which is pertinent to both private and public spaces. Chapters 5 and 6 have proposed that the value of privacy to and in public space is important and pertinent to tort law. To summarize generally, the reform arguments made in this chapter, on the basis of various *Charter* values, are:

1. **Value of Public Space**: Courts should not use public space location as a signal that a plaintiff has no privacy. Instead, courts should take a nuanced approach to privacy that recognizes the *value* of privacy to one's experience of public space (supported by privacy and expressive freedom *Charter* values, and drawing on the theory in Chapter 5).
2. **Normative Analysis of Privacy Expectations**: The REP analysis should be *normative*, not descriptive, and the normative analysis should reject any reliance on the discriminatory historical trajectory of the privacy torts. Specifically, the wholescale exclusion of privacy torts from public spaces renders the tort substantively inequitable, excluding protection in particular for those who experience greater violations in public space or who have less access to the private spaces where privacy is currently exclusively recognized. This substantive inequality must be rejected through a more nuanced normative analysis of privacy (drawing on privacy and substantive equality *Charter* values), that considers expectations of privacy with a view to the long-term consequences and impact of the decision for privacy and substantive equality.[684]
3. **Recognition of the Plaintiff's Subjectivity**: Courts should engage a *subjective-objective* privacy analysis. The privacy analysis should be made from the position of a reasonable

[684] Paraphrasing the SCC approach to *Charter* s. 8, per *Spencer, supra* note 552 at para 18.

person in the shoes of the plaintiff, with regard to an understanding of what they should normatively (per 1) be able to expect in public space. This should include an understanding of privacy harms like exposure and transparency, e.g., where a reasonable person in the plaintiff's position loses access to/experience of public space. (Supported by substantive equality and privacy values, and the latter portion of this argument is also supported by expressive freedom *Charter* values).

Chapter 7 – Recommendations and Conclusion

This chapter concludes the thesis by summarizing the key ways in which a conceptualization of public space privacy harm, and a *Charter* values approach to the privacy torts, would change the privacy tort analysis. As different privacy torts are available across Canada, this chapter examines more broadly how the principles derived from the earlier chapters could inform a reformed approach to a privacy analysis across jurisdictions – be it through an REP test, consideration of whether an invasion is into 'private affairs' and is 'highly offensive', or whether a publication engages a 'private fact.' By placing value on privacy in public spaces, the court's assessment of a plaintiff's privacy, and its balancing of a plaintiff's privacy interests with the legal, and especially property, interests of defendants should also look different. For instance, as in *Zeliony*, where the REP is perceived to be low or absent, it is easy for courts to find property protection outweighs privacy in a balancing analysis. However, where the REP is high, such a balance would be more likely to look different, and fall in favour of the plaintiff's claim. In this latter category of cases, courts may allow for successful claims even where the defendant's property might be engaged or in the case of drones, where the defendant also has an interest in the use of that space. Different provinces also offer different defences and exceptions to the privacy torts. Where a plaintiff's privacy interests are high, it is legally more appropriate and analytically preferable to validate the privacy interest at play, but then excuse the defendant's conduct on the basis of a defence in appropriate circumstances.

Summary of Argument

In the preceding chapters I have argued that the increasing popularity of remote-operated personal-use technologies, like drones and sophisticated home surveillance systems, will result in more interpersonal surveillance in public spaces. Socio-technical systems like drones and home

surveillance systems do not emerge in a vacuum. Rather, how they emerge and gain popularity can be guided by social and legal norms. Tort law is the primary area of law that regulates interpersonal non-contractual relationships in the common law in Canada. Nevertheless, tort law, as currently constituted, is not well equipped to address interpersonal privacy conflict in public spaces. Privacy torts, which are the dominant and most logical route for a plaintiff seeking to vindicate a privacy intrusion, are explicitly and implicitly embedded in notions of property and the related theories of secrecy and seclusion. The courts have thus declined to recognize the operation of the privacy torts in public space. I have argued that this is the wrong approach. There is nothing indicated in the statutory torts to bar their application in public spaces. There is scholarly support for the same interpretation of the common law torts – arguing that these torts can be understood to operate in public spaces. For both the statutory and common law torts, this spatial exclusion has been a matter of interpretation.

After examining the inequitable roots of the relationship between privacy and property in the torts, I argued that there is jurisprudential support to move away from the historical association and into a more substantively equitable interpretation of privacy within tort law. Specifically, I have argued that *Charter* values are relevant to a judicial understanding of privacy torts and that courts have indeed already relied on *Charter* values when interpreting the torts. However, while courts have already relied on *Charter* values when interpreting privacy torts, they have relied on an unduly limited understanding of the *Charter* value of privacy. Recognizing privacy in public space should not simply extend the secrecy/seclusion theory of privacy into specific public space circumstances. The *Charter* jurisprudence has evolved to recognize the possibility of privacy in public. Furthermore, there are other relevant *Charter* values that support a more fulsome recognition of privacy in public spaces, including substantive equality and expressive freedom values.

This thesis drew upon privacy scholarship to argue for the judicial recognition of public space privacy harm; more specifically, a judicial recognition of the negative impact of surveillance on one's experience and equitable use of shared public spaces. Incorporating the proposed theory of privacy into the range of judicial understandings of privacy would allow courts to pay appropriate attention to the spatial impact of privacy in public spaces, as they already do in private spaces. This thesis has not sought to diminish the recognition of privacy in private, but rather to draw upon the spatial import courts give to privacy already and extend a similar importance to privacy in public spaces. Such an approach can be supported jurisprudentially by *Charter* values. The next sub-sections summarize what such an approach would mean for the application of the statutory torts, and the common law torts.

Key Take-Aways for Statutory Torts

As noted in Chapter 3, statutory torts share many common features, with some minor modifications across the provinces. Under statute, the question of whether a plaintiff's privacy has been violated depends on how much privacy "is reasonable in the circumstances." Chapter 6 addresses this component of the tort and proposes various reforms to the current analysis. As I propose in Chapter 6, what is considered reasonable in the circumstances should be driven by a normative assessment of what a reasonable person in the plaintiff's shoes would expect with a view to the long-term implications for privacy and substantive equality. When a privacy conflict arises in public space this analysis should include a consideration of the spatial impact of surveillance on the plaintiff. I have included several examples above of how courts can apply these principles in relation to Ring systems (e.g. *Zeliony*), and surveillance of publicly visible spaces (e.g. *Milner*, *Vertolli*, etc).

A plaintiff's claim must also be balanced with the defendant's interests and justifications for their conduct, as articulated in several places throughout the statutory torts. First, most statutory

torts require willfulness on the part of the defendant, thus excluding unintentional invasions of privacy. The torts also require that a defendant act "without claim of right." I have commented above on how "claim of right" should not be interpreted so broadly as to permit pervasive public space surveillance.[685] For example, courts should not recognize a broad "claim of right" based on protecting one's property from the public through the use of pervasive surveillance, especially (though not exclusively) where that surveillance extends beyond the defendant's property and into public or shared spaces. The notion of "claim of right" in the context of a public space privacy conflict should be interpreted through the lens of the *Charter* values discussion laid out in Chapter 6, with a view to balancing a plaintiff's privacy interests with the legal interests and rights of the defendant.

I have discussed an application of the statutory torts in relation to the Ring surveillance system in the above Chapter.[686] One could also imagine in the context of drone use that a defendant may argue a claim of right based on having a right under drone regulation to operate in a particular area. Drawing on the above analysis, this would be too general a claim. The claim of right should specifically engage the right to intentionally film the plaintiff. Such a right is not granted under the regulations guiding the operation of drones in Canada. The general notion that drones are permitted to operate in certain areas, for example, should be insufficient on its own to justify public or shared-space surveillance, and/or subsequent public sharing of any collected information.

This does not mean, however, that all instances of drone or home surveillance information collection automatically would give rise to a tort claim. A defendant's interests, as well as societal interests, can and should also be considered within the court's assessment of whether the plaintiff's expectation of privacy "is reasonable in the circumstances." *Vertolli* provides a hypothetical example;

[685] See e.g., pages 95-96.
[686] See e.g., pages 225-228.

where a defendant reasonably worries their legal rights will be violated by a plaintiff (assessed on a subjective-objective basis as noted in Chapter 6), they *may* have a reasonable interest in surveilling the encounter to protect themselves and their rights, or to vindicate any violations. As in that case, in the context of an on-duty uniformed officer pulling over a defendant driver, there would be a power imbalance between the parties that might factor into the defendant's reasonable concerns prompting surveillance. This might legitimately lower the plaintiff's expectation of privacy in the circumstances. For instance, through a subjective-objective lens the court would consider that the plaintiff in *Vertolli* was in a position of wielding publicly authorized power over the defendant, such that there could be no expectation of privacy in the collection of information. Where, for instance, alternative measures exist for addressing a defendant's concerns, surveillance (or subsequent sharing or use of information) may be considered unreasonable, as discussed at greater length above in regards to *Zeliony* and *Milner*.[687] The statutes allow for a contextual balancing of interests, one I have argued should be done with a view to recognizing the substantive equality and expressive interests of the parties, particularly as pertaining to their conduct within or experience of public spaces.

Principles Engaged in a Common Law Privacy Tort Hypothetical

Throughout the analysis above I have discussed several examples of decisions arising under the statutory torts. In this subsection consider the application of the common law torts to a hypothetical public space privacy conflict. There are limits to conducting an analysis in the hypothetical – namely that it is difficult to develop sufficient facts for a scenario without skewing those facts in a desired (rather than a perhaps more complex real world) direction. Accordingly, for the purpose of this final analysis, I will identify areas for reformed thinking in the application of the

[687] See e.g., pages 207-208.

common law torts to a briefly described scenario, acknowledging that these principles will be applied differently in otherwise complex and nuanced scenarios. To come full circle, I will consider the hypothetical set out at the start of this thesis of a drone operator intentionally flying a drone over individuals relaxing and socializing on a public beach.[688]

Some general principles emerge from the discussion throughout this thesis, especially Chapters 5 and 6. With regards to privacy in public space, individuals concerned about privacy violations should not be excluded from a tort remedy on the basis that they are in public space. Analysis of whether something constitutes "private affairs" or a "private fact" should not be driven by a property analysis but instead based on whether someone, in the plaintiff's position, *ought* to be able to reasonably expect privacy in the "fact" or "affair" vis-à-vis the defendant. In this hypothetical, the court might consider whether the defendant's conduct in using the drone would undermine a reasonable person's ability to utilize that space as a result of the collection of information, or physical intrusion by the drone. In the context of a beach, this could include conduct like singling out the plaintiff for non-consensual photographs, which could undermine one's ability to enjoy a beach particularly considering social norms at a beach relating to states of dress/undress. This may also include conduct that creates a physical interference with one's privacy (even absent filming), like following someone with a drone (harkening back to exposure and subjective privacy harms). Where someone is singled out only briefly through a defendant's conduct and there are no additional aggravating factors, this might still engage a plaintiff's "private affairs" but could be deemed outside the scope of liability on the basis that it is not "highly offensive."

The "highly offensive" qualifier, where interpreted through a normative, subjective-objective lens, can provide a helpful mechanism for balancing a court's assessment of competing interests between the parties. As noted, courts could allow that a single image collected from a drone (or Ring

[688] See above in Chapter 1 at pg 2.

camera) could constitute a "private affair" depending on the situation, but contingent on the circumstances that collection might not be considered "highly offensive." Through this element, courts can dismiss *de minimis* claims without setting a precedent whereby all single images are necessarily considered acceptable regardless of further circumstances. Circumstances like repeated photography, or capturing a plaintiff's daily movements or routines, or using remotely operated surveillance to intimidate a plaintiff can all be aggravating factors that rise to the level of "highly offensive." Similarly, consideration of the privacy dynamics engaged through a remote-technology might prompt a highly offensive invasion of privacy. For instance, in the context of drone surveillance, circumstances like being monitored from above, in a context where it can be difficult or impossible to move away from the source of the surveillance (and thus assert self-help response to the surveillance), and where the plaintiff may experience added discomfort and/or concern on account of information inequality (not knowing who is operating the drone or why) might aggravate the privacy analysis such that the plaintiff can establish that the intrusion was "highly offensive."[689] Each of these conditions appeared relevant in the beach hypothetical.

Further, evaluating the defendant's conduct through a substantive equality lens would also mean that discriminatory targeting on the basis of identity (e.g., gender, as was implied in the beach example that introduced the thesis) should be considered an aggravating factor – increasing the likelihood that the conduct was "highly offensive." A single image or instance of surveillance can be highly offensive when viewed through this lens, particularly when considering the normative impact this kind of filming has on access to public space for members of the targeted community.

Similarly, if collected information was subsequently used by the defendant or shared with others, the plaintiff may establish a transparency/objective privacy harm. Publication and false light tort claims should also not be excluded on the basis that conduct occurred in public space. Where

[689] See e.g., Bracken-Roche, "Politics of Verticality", *supra* note 11.

drone operators are allowed to collect and/or share any images or information from a public beach solely on the basis that the beach is public, the normative implications of this (which is the current state of tort) will be to exclude or discourage people like the accused (who was upset by the use of the drone) from using public beaches. Where this exclusion occurs on the basis of discriminatory grounds, the absence of legal protection (on the implied or explicit basis of property rights) perpetuates social inequality. Parties to a claim should have the opportunity to present such arguments to the court and have them considered as part of the normative analysis of a privacy claim.

Additionally, the foregoing analysis indicates that a privacy intrusion can occur through a physical intrusion, and/or collection, use or distribution of information. A privacy intrusion need not be linked to a property intrusion. If the drone remains at a distance, the intrusion will likely pertain to information collection/use/distribution; however, courts should not immediately reject a claim solely on the basis the technology was not filming if legitimate concerns about privacy forced an exposure/subjective privacy harm. Again here, the technology is relevant to the analysis in various ways, including the possible creation of a power imbalance between the parties (where an individual on the beach is rendered powerless/passive by virtue of not knowing who is operating the drone or why[690]).

Accordingly, by rejecting a historical reliance on property to assess privacy interests, and instead viewing privacy interests through a normative and subjective-objective lens and with an appreciation of the importance of privacy for a flourishing experience of public space, courts can adapt the current common law privacy torts to address increasingly common interpersonal remote surveillance. Similarly, courts or provinces could recognize a new tort more explicitly framed

[690] See e.g., Bracken-Roche, "Politics of Verticality", *supra* note 11.

through reliance on these principles, and justified on the basis of evolving the law in line with *Charter* values.

Tort Law & Systemic Factors in Interpersonal Privacy Conflicts

Tort law allows for the litigation of individual harms. It also, importantly, can play a role in setting norms around what forms of conduct are not permissible by attaching legal consequences to undesirable actions. Tort law can provide the legal backdrop to alternative modes of dispute resolution between individuals engaged in a conflict, which may be initiated through demand letters or the statement of claim in an action. Tort law has also been cited for its role in prompting institutional and structural change, particularly when many plaintiffs litigate their individual harms together in a class action, or where the engaged conduct implicates liability insurance providers (and associated policies around insurable conduct), as may be especially relevant in the context of home surveillance systems.[691] All of this is pertinent to the examination of how tort would resolve increasingly common interpersonal technology-mediated privacy conflicts, as above.

There are, nevertheless, some significant limits to tort law's individualistic lens. For example, broader changes to societal norms and systems would be needed to address the *root* of some of the privacy conflicts contemplated in this thesis. For instance, where individual homeowners are encouraged by police, in partnership with Amazon, to install Ring devices on their home and subsequently share information, privacy torts may importantly provide a modicum of protection for those targeted for surveillance and may provide an in-road for dispute resolution. However, in this example, individual homeowners are not the primary cause of the surveillance, and might believe

[691] My gratitude to Prof. Jennifer Chandler for raising this latter point.

they are doing the right thing, or at least acting lawfully.[692] In the complex web of a Ring-police-homeowner relationship those concerned with privacy and surveillance will be more concerned with the establishment of a sophisticated commercially-operated neighbourhood surveillance infrastructure. While individual homeowners are the first point of contact with the legal system,[693] it is commercial and state institutions that make the surveillance network possible. Further, at the root of the privacy and surveillance concerns in this example are broader social norms motivating individuals to opt into their role within the surveillance network. This includes ideas about the threat of crime (which may also be stoked through advertising), who is 'good' or 'bad' or perceived to be out of place, who belongs in a neighbourhood, who needs to be protected and from whom, *etc.* Individual litigation of one privacy conflict, no matter how nuanced, will not on its own address these societal level issues. Developing privacy torts that can address interpersonal privacy conflicts in public space may be a necessary, but not sufficient, step toward addressing concerns relating to the development of complex surveillance infrastructures in public spaces.

Nevertheless, should courts recognize that individuals have privacy rights in public space that can be violated through the use of surveillance in certain contexts, this would provide some foundation to other legal responses to broader systems of surveillance. Class actions for instance are not possible without a recognition of individual rights; and creative legal arguments engaging vicarious liability require the recognition of a tortious harm.[694] While negligence actions are typically engaged where individuals are concerned about harm perpetuated through the design and use of products, negligence requires a plaintiff to prove damage which may not currently be possible in

---

[692] See e.g., Rinaldo Walcott, *On Property* (Biblioasis, Windsor, ON: 2021), *supra* note 415 at 28 on the notion of "deputization" and interpersonal policing (particularly in relation to anti-Black interpersonal surveillance and white supremacy).
[693] See e.g., Madeleine Clare Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction" (2019) 5 Engaging Science, Technology, and Society 40-60.
[694] E.g., while novel (and possibly difficult to establish), a creative vicarious liability claim might consider whether a homeowner could act as an agent of a commercial or state entity in collecting information about plaintiffs.

many instances of privacy harm. Recognizing the application of the intentional tort may be the only mechanism through tort law for vindicating privacy concerns where there is no associated financial loss or physical injury. Tort law does not provide a perfect mechanism through which to engage social concerns about surveillance. Nevertheless, tort law provides one possible avenue within the dominant legal system in the common law provinces of Canada, and thus I have proposed in this thesis, needs to be more deeply considered and nuanced.

Overall Conclusion

In this thesis, I have posited that increasingly sophisticated personal-use technical systems like drones and home surveillance systems will make interpersonal privacy conflicts in public spaces more common. I then considered whether the privacy torts, which specifically vindicate interpersonal privacy harm, could be relevant to such public space privacy conflicts. The current interpretation of the privacy torts in the common law provinces in Canada suggests that they will not be useful in addressing public space privacy conflict, which may leave complainants with little if any legal recourse for perceived privacy harms. This appears to be the case because of the inequitable historical underpinnings of the privacy torts, and what and whom they were originally envisioned to protect. In particular, the unnuanced exclusion of public spaces from the scope of the tort reflects patriarchal and colonial norms of the past that persist today. However, I have also showed that privacy harms can and do occur in public space, and in fact, surveillance can even be harmful specifically because of its spatial impact in public (and not simply as an extension of protections of the home, private property, and secrecy). I have argued that this historical interpretation, one which simplistically excises public space from the scope of the torts, should be rejected. Such a rejection would allow the privacy torts to evolve closer in line with some of the particular norms of the Canadian legal system; especially *Charter* values.

A *Charter* values approach to the existing privacy torts would allow for at least several specific reforms that would provide nuance to the application of these torts and better reflect the reality of interpersonal privacy conflicts, particularly against the backdrop of the increasing prevalence of sophisticated personal-use surveillance technologies. I have proposed that courts should at least approach the analysis of reasonable expectations of privacy (sometimes alternatively captured in the notion of "private affairs" and the question of whether a reasonable person would find an invasion of privacy "highly offensive"), through a normative and not a descriptive lens. This lens asks what level of privacy individuals *ought* to be able to expect, with a view to the long-term consequences for privacy and substantive equality. It is concerned with the broader implications of a precedent that allows for certain forms of interpersonal surveillance. I have also proposed that in assessing what the reasonable person ought to be able to expect, courts should consciously consider the plaintiff's subjectivity and positionality through a subjective-objective analysis. Courts would ask what the reasonable person, in the plaintiff's position, ought to be able to expect in a given set of circumstances. This might open the analysis to hearing evidence, for instance, on the gendered nature of voyeuristic privacy harm, or the racial dynamics of interpersonal policing, or the ableist stereotypes engaged in insurance surveillance. Finally, in carrying out this analysis, I have argued that courts should also be explicit about the value of privacy in creating public and community spaces, and how surveillance can undermine the public nature of public space for a plaintiff.

At various stages of the analysis, I have also highlighted how defendants' interests could be considered and balanced, including in elements already embedded in the existing legal tests, through the normative analysis of privacy expectations, as well as through the judicial recognition of defences to common law torts. When courts engage a subjective-objective assessment of the plaintiff's REP in the context of the relationship and interaction between the parties, this analysis should include consideration of countervailing interests of defendants within the context of the parties' interaction

and relationship. In other words, the *Charter* values approach I have advocated for in this thesis should be relevant to both plaintiffs and defendants, as well as society more broadly, in the litigation of privacy claims. Substantive equality, privacy, expressive freedom, and other values engaged by plaintiffs' and defendants' conduct should be captured in the normative assessment of what degree of privacy a plaintiff could expect in the circumstances of a dispute.

Ultimately, this thesis has argued that public space is important, that privacy and freedom from surveillance are crucial to the health and value of public space, and that the privacy torts have a role to play in navigating interpersonal privacy conflicts in public spaces. If tort law fails to address privacy in public spaces this not only leaves many complainants without vindication but also continues to permit a gap in the socio-legal environment that allows for the creation and deployment of more sophisticated surveillance technologies throughout public space. Accordingly, the privacy torts ought to develop to at least recognize the increasing breadth and depth of surveillance in public space.

Bibliography

Legislation

A By-law to regulate the fortification of land and protective elements applied to land and to prohibit excessive fortification of land and excessive protective elements being applied to land in relation to the use of land within the City of Burlington, By-Law No. 108- 2002 (Burlington, ON).

Aeronautics Act, RSC 1985, c A-2.

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

City of Hamilton By-Law No. 10-122 (Hamilton, ON).

Criminal Code, RSC 1985, c C-46.

Fortification of Land By-law PW-8 2002 (London, ON).

Interpretation Act, RSBC 1996, c. 238.

Intimate Images and Cyber-protection Act, SNS 2017, c 7.

Intimate Images Protection Act, RSNL 2018, c I-22.

Personal Information Protection of Electronic Documents Act, SC 2000, c 5.

Privacy Act, RSBC 1979, c. 336.

Privacy Act, RSC, 1985, c P-21.

Privacy Act, RSN 1990, c P-22.

Protecting Victims of Non-consensual Distribution of Intimate Images Act, RSA 2017, c P-26.9.

The Privacy Act, RSM 1987, c P-125.

The Privacy Amendment Act, 2018, SS 2018, c 28.

The Privacy Act, RSS 1978, c P-24.

Jurisprudence

Canadian Jurisprudence

Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, [2013] 3 SCR 733.

Andrews v Law Society of British Columbia, [1989] 1 SCR 143.

Ari v Insurance Corporation of British Columbia, 2015 BCCA 468 (CanLII).

Asm Sabbir Ahmed v Canadian Light Source Inc., 2018 SKQB 320.

Aubry v Éditions Vice-Versa, [1998] 1 SCR 591.

Avery v Attorney General of Canada et al., 2013 NBQB 152.

Azak v Chisholm, 2018 BCSC 1051.

Baldwin v Morningstar, 2019 ONSC 1276.

Batty v Toronto, 2011 ONSC 6862.

Bazley v Curry, [1999] 2 SCR 534.

Bettel v Yim (1978), 20 OR (2d) 617.

Bhadauria v Seneca College, [1981] 2 SCR 181.

Bigstone v St. Pierre, 2011 SKCA 34.

Bracken v Vancouver Police Board, 2006 BCSC 189 (CanLII).

Bresnark v Thomson Reuters Canada Limited, 2016 ONSC 5105.

Broutzas v Rouge Valley Health System, 2018 ONSC 6315.

Calgary Airport Authority v Canadian Centre for Bio-Ethical Reform, 2019 ABQB 29.

Canadian National Railway Co v Canada (Canadian Human Rights Commission), [1987] 1 SCR 1114.

Candelora v Feser, 2019 NSSC 370.

Candelora v Feser, 2020 NSSC 177.

Capital District Health Authority v Murray, 2017 NSCA 28.

Caplan v Atas, 2021 ONSC 670.

Clements v Clements, [2012] 2 SCR 181.

Colet v The Queen, 1981 CanLII 11 (SCC), [1981] 1 SCR 2.

Committee for the Commonwealth of Canada v Canada, [1991] 1 SCR 139, 77 DLR (4th) 385.

Condon v Canada, 2018 FC 522.

Cooper v Hobart, [2001] 3 SCR 537.

Dagg v Canada (Minister of Finance), [1997] 2 SCR 403.

Davis v McArthur (1969), 1969 CanLII 757 (BCSC), 10 DLR (3d) 250, 72 WWR 69 (BCSC).

Davis v McArthur (1970), 1970 CanLII 813 (BCCA), 17 DLR (3d) 760, [1971] 2 WWR 142 (BCCA).

Dawe v Nova Collection Services (Nfld) Ltd. (1998), 160 Nfld & PEIR 266 (NLPC).

Demcak v Vo, 2013 BCSC 899 (CanLII).

Doucette v Nova Scotia, 2016 NSSC 25.

Douez v Facebook, 2017 SCC 33.

Duncan v Lessing, 2018 BCCA 9.

Éditions Écosociété Inc. v Banro Corp., 2012 SCC 18.

Eldridge v British Columbia (Attorney General), [1997] 3 SCR 624.

ES v Shillington, 2021 ABQB 73.

Facilities Subsector Bargaining Association v British Columbia Nurses' Union, 2009 BCSC 1562 (CanLII).

Federated Anti-Poverty Groups of BC v Vancouver (City), 2002 BCSC 105.

Fiala v Cechmanek, 2001 ABCA 169 (CanLII).

Fouad . Wijayanayagam, 2015 BCCA 272.

Fraser v Canada (Attorney General), 2020 SCC 28.

Getejanc v Brentwood College Assn. (2001), 6 C.C.L.T. (3d) 261, 2001 BCSC 822 (CanLII).

Grant v Torstar Corp., [2009] 3 SCR 640.

Grech v Scherrer, 2018 ONSC 7206.

Griffin v Sullivan, 2008 BCSC 827 (CanLII).

Hagan v Drover, 2009 NLTD 160.

Harding (Re), 2014 LSBC 29.

Harrison v Carswell, [1976] 2 SCR 200.

Heckert v 5470 Investments Ltd, 2008 BCSC 1298.

Hill v Church of Scientology, [1995] 2 SCR 1130.

H.J. Heinz Co. of Canada Ltd. v Canada (Attorney General), [2006] 1 SCR 441.

Hollinsworth v BCTV, A Division of Westcom TV Group Ltd., [1998] B.C.J. No. 2451(BCCA).

Hung v Gardiner, 2002 BCSC 1234 (CanLII).

Hunter v Southam, [1984] 2 SCR 145.

Hynes v Western Regional Integrated Health Authority, 2014 CanLII 67125 (NL SCTD).

Irwin Toy Ltd. v Quebec (Attorney General), [1989] 1 SCR 927.

Jane Doe 464533 v ND, 2016 ONSC 541.

Jane Doe 464533 v ND, 2016 ONSC 4920.

Jane Doe 72511 v NM, 2018 ONBSC 6697.

Jones v Tsige, 2012 ONCA 32 (CanLII).

Kahkewistahaw First Nation v Taypotat, [2015] 2 SCR 548.

Lac Minerals Ltd. v *International Corona Resources Ltd.*, [1989] 2 SCR 574.

L.A.M. v J.E.L.I., 2008 BCSC 1147.

Larizza v The Royal Bank of Canada, 2017 ONSC 6140.

Lavigne v Canada (Office of the Commissioner of Official Languages), [2002] 2 SCR 773.

Lee v Jacobson (1992), 87 DLR (4th) 401 (BCSC) reversed (1994), 120 DLR (4th) 155 (BCCA) but reasoning reaffirmed in *Malcolm v Fleming*, [2000] BCJ No 2400 (SC).

Leung v Shanks, 2013 ONSC 4943.

Lupuliak v Condominium Plan No 8211689, 2022 ABQB 65.

M(A) v Ryan, [1997] 1 SCR 157.

Madco Investments Ltd. v Western Tank & Lining Ltd., 2017 BCSC 219.

Marson (nee Doucette) v Nova Scotia, 2017 NSCA 17.

Milner v Manufacturers Life Insurance Company, 2005 BCSC 1661.

Milton v Savinkoff (1993), 18 CCLT (2d) 288 (BCSC).

Miron v Trudel, [1995] 2 SCR 418.

Mohl v University of British Columbia, 2009 BCCA 249 (CanLII).

Montréal (City) v 2952-1366 Québec Inc, [2005] 3 SCR 141.

Mustapha v Culligan of Canada Ltd., [2008] 2 SCR 114.

Niemela v Malamas, 2015 BCSC 1024.

Pelletier v Collins, 2012 SKQB 318.

Peters-Brown v Regina District Health Board, 1995 CanLII 5943 (SKQB).

Pia Grillo c Google inc., 2014 QCCQ 9394.

Powell v Shirley, 2016 ONSC 3677 affd 2018 ONCA 632.

Quebec (Attorney General) v A, 2013 SCC 5.

Quebec (Attorney General) v Alliance du personnel professionnel et technique de la santé et des services sociaux, [2018] 1 SCR 464.

R v Barton, 2019 SCC 33.

R v Colarusso, [1994] 1 SCR 20.

R v Edwards, [1996] 1 SCR 128.

R v Ewanchuck, [1999] 1 SCR 330.

R v Fearon, 2014 SCC 77, [2014] 3 SCR 621.

R v Gladue, [1999] 1 SCR 688.

R v Golden, [2001] 3 SCR 679.

R v Grant, [2009] 2 SCR 353.

R v Ipeelee, [2012] 1 SCR 433.

R v Jarvis, 2019 SCC 10, [2019] 1 SCR 488.

R v Jarvis Factum of the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic; Factum of the Intervener, Women's Legal Education and Action Fund Inc., SCC Court File No: 37833.

R v Kapp, [2008] 2 SCR 483.

R v Keegstra, [1990] 3 SCR 697.

R v Kokopenace, 2015 SCC 28.

R v Jarvis, 2019 SCC 10, [2019] 1 SCR 488.

R v Le, 2019 SCC 34.

R v Marakah, [2017] 2 SCR 608.

R v Mills, [1999] 3 SCR 668.

R v National Post, 2010 SCC 16, [2010] 1 SCR 477.

R v Parks (1993), 15 OR (3d) 324.

R v Patrick, 2009 SCC 17, [2009] 1 SCR 579.

R v Salituro, [1991] 3 SCR 654.

R v Spence, 2005 SCC 71, [2005] 3 SCR 458.

R v Spencer, 2014 SCC 43, [2014] 2 SCR 212.

R v Stillman, [1997] 1 SCR 607.

R v Tessling, [2004] 3 SCR 432.

R v Quesnelle, 2014 SCC 46, [2014] 2 SCR 390.

R v RDS, [1997] 3 SCR 484.

R v Ward, 2012 ONCA 660 (CanLII), 97 CR (6th) 377.

R v Williams, [1998] 1 SCR 1128

R v Wise, [1992] 1 SCR 527.

R v Wong, [1990] 3 SCR 36.

R v Zora, 2020 SCC 14.

Racki v Racki, 2021 NSSC 46.

Rancourt-Cairns v Saint Croix Printing and Publishing Company Ltd, 2018 NBQB 19.

Ratt v Tournier, 2014 SKQB 353.

Reference re Subsection 18.3(1) of the Federal Courts Act, 2021 FC 723.

Robert v Assis, 2017 ONSC 1685.

RWDSU v Dolphin Delivery Ltd., [1986] 2 SCR 573.

RWDSU Local 558 v Pepsi-Cola Canada Beverages (West) Ltd, [2002] 1 SCR 156

Saadati v Moorhead, [2017] 1 SCR 543.

Silber v British Columbia Television Broadcasting System Ltd (1985), 69 BCLR 34, 25 DLR (4th) 345 (BCSC).

Singh-Boutilier v Ontario College of Social Workers and Social Service Workers, 2015 ONSC 5297.

Somwar v McDonald's Restaurants of Canada Ltd., (2006) OTC 28 (Superior Court).

St. Pierre v Pacific Newspaper Group Inc. and Skulsky, 2006 BCSC 241.

Sauve v Canada, 2015 FC 739.

TeBaerts v Penta Builders Group Inc, 2015 BCSC 2008.

T.K.L. v T.M.P., 2016 BCSC 789.

TransMountain Pipleline ULC v Mivasair, 2018 BCSC 1909.

Trout Point Lodge Ltd. v Handshoe, 2012 NSSC 245.

Tucci v Peoples Trust Company, 2017 BCSC 1525 (CanLII).

Tucci v. Peoples Trust Company, 2020 BCCA 246.

Turkson v TD Direct Investing, A Division of TD Waterhouse Canada Inc., 2016 BCSC 732 (CanLII), aff'd 2017 BCCA 147 (CanLII).

Quebec (Attorney General) v COPA, [2010] 2 SCR 536.

Quebec (Attorney General) v Lacombe, [2010] 2 SCR 453.

Vanderveen v Waterbridge Media Inc., 2017 CanLII 77435 (ON SCSM).

Vertolli v YouTube LLC, 2012 CanLII 99832 (ON SCSM).

VonMaltzahn v Koppernaes, 2018 NSSC 192.

Wasserman v Hall, 2009 BCSC 1318.

Wiseau Studio et al. v Richard Harper, 2017 ONSC 6535.

Withler v Canada, [2011] 1 SCR 396.

Yenovkian v. Gulian, 2019 ONSC 7279.

Zeliony v Dunn, 2021 MBQB 136 (CanLII).

International Jurisprudence

Boggs v Meredith, US District Court Western District of Kentucky at Louisville, Civil Action No. 3:16-CV-00006-TBR (U.S.).

Entick v Carrington, 1765] EWHC KB J98 (UK).

Garrat v Dailey, 46 Wash 2d 197 (1955) (US).

John Baker Orange v Ring LLC and Amazon.com Inc. Statement of Claim, US District Court Central District of California, Case No: 2: 19-cv-10899 (US).

Murray v Express Newspapers [2008] EWCA Civ 446, [2009] Ch 481 at para 36 (UK).

Scott v Shepherd, 96 Eng Rep 525 (KB 1773) (UK).

Semayne's Case (January 1, 1604) 5 Coke Rep. 91 (UK).

Government Documents

Canada Gazette, Part I, Volume 151, Number 28: Regulations Amending the Canadian Aviation Regulations (Unmanned Aircraft Systems), Regulatory Impact Assessment, online: <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-07-15/html/reg2-eng.php>.

Canada Gazette, Part I, Volume 151, Number 28: Regulations Amending the Canadian Aviation Regulations (Unmanned Aircraft Systems) (July 15, 2017), online: <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-07-15/html/reg2-eng.php>.

The Legislative Assembly of Manitoba, Thursday May 14, 1970, 8:00am.

The Legislative Assembly of Manitoba, Thursday June 18, 1970, 2:30pm.

The Legislative Assembly of Saskatchewan, Thursday March 21, 1974.

Pearce, Dennis, Enid Campbell and Don Harding, *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission* (Australian Government Publishing Service, 1987).

Transport Canada, "Transport Canada's Drone Strategy to 2025" (2021), online: <https://tc.canada.ca/sites/default/files/2021-03/TC223-Drone-Strategy-ENG-ACC.pdf>.

WIPO: WO2019133764A1, "Locating a person of interest using shared video footage from audio/video recording and communication devices" inventors: James Siminoff, Mark Troughton, Aviv Gilboa, Darell SOMERLATT, Alex Jacobson (2018), Google Patents, online, <https://patents.google.com/patent/WO2019133764A1/en>.

Secondary Materials: Books & Book Chapters

Ahmed, Sara, *Strange Encounters: Embodied Others in Post-Coloniality* (Oxfordshire, UK: Routledge, 2000).

Alexander, Michelle, *The New Jim Crow: Mass Incarceration in the Age of Colorblindness* (New York: The New Press, 2010).

Allen, Anita, *Uneasy Access: Privacy for Women in a Free Society* (Totawa, New Jersey: Rowan & Littlefield 1988).

Arendt, Hannah *The Human Condition* (Chicago: University of Chicago Press, 1958).

Backhouse, Constance, *Colour-Coded: A Legal History of Racism in Canada, 1900-1950* (Toronto: University of Toronto Press, 2007).

Bailey, Jane and Jasmine Dong, "Toward Survivor-Centred Outcomes for Targets of Privacy-Invasive TFVA: Assessing the Equality-Affirming Impact of *R v Jarvis*" in CL Hunt and Robert Diab (eds) *The Last Frontier: Digital Privacy and the Charter* (Toronto: Thompson Reuters, *forthcoming*).

Bhandar, Brenna *Colonial Lives of Property: Law, Land, and Racial Regimes of Ownership* (Durham NC: Duke University Press, 2018).

Blomley, Nicholas "Begging to Differ: Panhandling, Public Space, and Municipal Property" in Eric Tucker, James Muir & Bruce Ziff, eds, *Property On Trial: Canadian Cases in Context* (Toronto: Irwin Law for the Osgoode Society of Legal History, 2012).

Blomley, Nicholas, "Public Space: Introduction" in Nicholas Blomley, David Delaney & Richard T Ford, (eds) *The Legal Geographies Reader: Law, Power, and Space* (Oxford: Blackwell Publishers, 2001).

Blomley, Nicholas, *Rights of Passage: Sidewalks and the Regulation of Public Flow* (New York: Taylor & Francis, 2010).

Bottomley, Anne "A Trip to the Mall: Revisiting the Public/Private Divide" in Hilary Lim (ed), *Feminist Perspectives on Land Law* (Cavendish: Routledge, 2007).

Broom, H. & R.H. Kersley, *Broom's Legal Maxims* 10th ed (London: Sweet & Maxwell, 1929).

Browne, Simone, *Dark Matters: On the Surveillance of Blackness* (Durham, North Carolina: Duke University Press, 2015)

Cane, Peter, *The Anatomy of Tort Law* (Portland, OR: Hart Publishing, 1997).

Cassels, Jamie, "The Revival of Tort Theory in Canada" in Ken Cooper-Stephenson and Elaine Gibson (eds), *Review of Tort Theory* (Toronto: Captus University Publications, 1993).

Cohen, Julie E., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven CT: Yale University Press, 2012).

Cooper-Stephenson, Ken "Corrective Justice, Substantive Equality and Tort Law" in Ken Cooper-Stephenson and Elaine Gibson, *Tort Theory* (North York, Captus University Publications: 1993)

Crosby, A & J Monaghan, *Policing Indigenous Movements: Dissent and the Security State* (Winnipeg: Fernwood Publishing, 2018)

Davis, Angela *Are Prisons Obsolete?* (New York: Seven Stories Press, 2003).

Delaney, David "Beyond the Word: Law as a Thing of this World" in Jane Holder and Carolyn Harrison (eds), *Law and Geography* (Oxford: Oxford University Press, 2003).

Dulo, Donna, *Unmanned Aircraft in the National Airspace: Critical Issues, Technology, and the Law* (Washington DC: American Bar Association, 2015).

Eubanks, Virginia, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (New York: St. Martin's Press, 2017).

Habermas, Jürgen *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, translated by Thomas Burger & Frederick Lawrence (Cambridge: MIT Press 1989).

Hargraeves, Stuart, "'I'm a Creep, I'm a Weirdo': Street Photography in the Service of the Male Gaze" in Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops (eds) *Surveillance, Privacy, and Public Space* (Routledge Studies in Surveillance Book Series: 2018)

Hartzog, Woodrow *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge: Harvard University Press, 2018).

Hughes, Kristy, "The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse" in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy* (Cambridge: Cambridge University Press, 2015).

Kaba, Mariame, *We Do This 'Til We Free Us: Abolitionist Organizing and Transforming Justice* (Chicago: Haymarket Books, 2021).

Koops, Bert-Jaap and Maša Galič, "Conceptualizing Space and Place: Lessons from Geography for the Debate on Public Privacy" in Tjerk Timan, Bryce Newell, & Bert-Jaap Koops (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Edward Elgar Publishing, 2017).

Layard, Antonia "Freedom of Expression and Spatial (Imaginations of) Justice" in Dimitry Kochenov, Grianne de Burca, Andrew Williams (eds), *Europe's Justice Deficit?* (Oxford: Hart Publishing, 2015)

Lefebvre, Henri, *The Production of Space,* translated by Donald Nicholson-Smith (Oxford: Blackwell Publishers, 2000).

Linden, Allen M. Lewis N. Klar and Bruce Feldthusen, *Canadian Tort Law, Cases, Notes & Materials*, 15th ed (Toronto: Butterworths, 2018).

McCamus, John D "The Protection of Privacy: The Judicial Role" in Rosalie Abella and Melvin Rothman (eds), *Justice Beyond Orwell* (Montreal: Éditions Y. Blais, 1986).

McGill, Jena and Ian Kerr, "Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment" in *Digital Enlightenment Yearbook* (IOS Press, 2012).

Millar, Jason and Ian Kerr, "Delegation, Relinquishment and Responsibility: The Prospect of Expert Robots" in Ryan Calo, Michael Froomkin, Ian Kerr (eds), *Robot Law* (Cheltenham, UK: Edward Elgar Publishing, 2016).

Mitchell, Don, *The Right to the City: Social Justice and the Fight for Public Space* (New York: Guilford Press, 2003).

Moran, Mayo, *Rethinking the Reasonable Person: An Egalitarian Reconstruction of the Objective Standard* (Oxford: Oxford University Press, 2003).

Moreham, NA "Why is Privacy Important? Privacy, Dignity and Development of the New Zealand Breach of Privacy Tort" in J Finn & S Todd (eds), *Law, Liberty and Legislation* (Wellington, NZ: Lexis Nexis, 2008).

Nedelsky, Jennifer, *Law's Relations: A Relational Theory of Self, Autonomy, and Law* (New York: Oxford University Press, 2011)

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009).

Osborne, Philip H., *The Law of Torts*, 6th ed (Toronto: Irwin Law, 2020).

Raab, Charles D., "Privacy, Social Values and the Public Interest" in A. Busch and J. Hofmann (eds), *Politik und die Regulierung von Information* (Politische Vierteljahresschrift, Sonderheft 46, 2012)

Reagan, Priscilla, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

Reagan, Priscilla "Privacy and the Common Good: Revisited" in *Social Dimensions of Privacy*, Beate Roessler and Dorota Mokrosinska (eds) (Cambridge: Cambridge University Press, 2015).

Richards, Neil, *Intellectual Privacy: Rethinking Privacy in a Digital Age* (Oxford: Oxford University Press, 2015).

Rothstein, Adam, *Drone* (New York: Bloomsbury, 2015).

Schoeman, Ferdinand David, *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992).

Selinger, Evan and Woodrow Hartzog, "Obscurity and Privacy" in Joseph Pitt and Ashley Shew (eds) *Routledge Companion to Philosophy of Technology* (London, UK: Routledge, 2016).

Skinner-Thompson, Scott, *Privacy at the Margins* (Cambridge: Cambridge University Press, 2021).

Solove, Daniel J., *Understanding Privacy* (Cambridge MA: Harvard University Press, 2008).

Starblanket, Gina & Dallas Hunt, *Storying Violence: Unravelling Colonial Narratives in the Stanley Trial* (Winnipeg, Manitoba: ARP Books, 2020).

Steeves, Valerie "Privacy, Free Speech and Community: Applying Human Rights Law to Cyberspace" in Steven Hick, Edward F Halpin, Eric Hoskins (eds) *Human Rights and the Internet* (London: Palgrave Macmillan, 2000).

Steeves, Valerie "Reclaiming the Social Value of Privacy" in Ian Kerr, Valerie Steeves, Carole Lucock (eds), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009).

Thomasen, Kristen, "AI and Tort Law" in Florian Martin-Bariteau & Teresa Scassa (eds), *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021).

Thomasen, Kristen, "Flying between the Lines: Drone Laws and the (Re)Production of Public Spaces" in Eric Hilgendorf and Uwe Seidel (eds) *Robotics, Autonomics, and the Law* (Germany: Nomos, 2017).

Thomasen, Kristen and Suzie Dunn, "Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canadas Decision in R v Jarvis" in Jane Bailey, Asher Flynn, Nicola Henry (eds) *Handbook on Technology-Facilitated Violence and Abuse: International Perspectives and Experiences* (Bingley, UK: Emerald Publishing Ltd, 2021).

Uteck, Anne, "Reconceptualizing Spatial Privacy for the Internet of Everything" (PhD Thesis, University of Ottawa Faculty of Law, 2013).

Vergouw, Bas and Huub Nagel, Geert Bondt and Bart Custers, "Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments" in Bart Custers (ed), *The Future of Drone Use* (New York: Springer, 2016).

Walcott, Rinaldo *On Property* (Windsor, ON: Biblioasis, 2021).

Waldman, Ari Ezra, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge, UK: Cambridge University Press, 2018).

Xavier, S, J Hewitt, A Alvez, A Bhatia, B Jacobs & V Waboose, *Decolonizing Law in the Global North and Global South* (London UK: Routledge, 2021).

Secondary Materials: Reports

British Columbia Law Institute, *Report on The Privacy Act of British Columbia* (February 2008), BCLI Report No. 49, online:
<http://www.bcli.org/sites/default/files/Privacy_Act_Report_Website.pdf>.

Bracken-Roche, Ciara et al "Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada," Report to the Office of the Privacy Commissioner of Canada (2014).

Finn, Rachel L., David Wright, Anna Donovan, Laura Jacques, and Paul De Hert, *Privacy, Data Protection and Ethical Risks in Civil RPAS Operations: Final Report for the European Commission* (Brussels: European Commission, 2015).

Gettinger, Dan et al "The Drone Primer: A Compendium of Key Issues" (2014) Report by the Centre for the Study of the Drone, Bard College.

Introna, Lucas and Helen Nissenbaum, "Facial Recognition Technology: A Survey of Policy and Implementation Issues" (2010) Report for the Center for Catastrophe Preparedness and Response (New York: New York University, 2009).

Ngan, Mei, Patrick Grother, and Kayee Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms" (November 2020) NISTIR 8331, available online: <https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report_6b.pdf>.

Office of the Privacy Commissioner of Canada, "Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy?," Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada (March 2013), online: <http://www.priv.gc.ca/information/researchTrecherche/2013/drones_201303_e.asp>.

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia* (October 28, 2020) PIPEDA Findings #2020-004, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/>.

Tulloch, M. *Report of the independent street checks review* (Toronto: Queen's Printer for Ontario, 2018).
Yellowhead Institute, "Land Back: A Yellowhead Institute Red Paper" (October 2019), online <https://redpaper.yellowheadinstitute.org/>.

Young, Hilary and Emily Laidlaw, "Nonconsensual Disclosure of Intimate Images (NCDII) Tort" (August 2019) Uniform Law Conference of Canada, Newfoundland and Labrador, online: <https://ulcc-chlc.ca/ULCC/media/EN-Annual-Meetings/Nonconsensual-Disclosure-of-Intimate-Images-Images_1.pdf>.

Secondary Materials: Articles

Acquisti, Alessandro, Ralph Gross, Frederic D Stutzman, "Face Recognition and Privacy in the Age of Augmented Reality" (2014) 6(2) Journal of Privacy and Confidentiality 1-20.

Adjin-Tettey, Elizabeth, "Discriminatory Impact of Application of *Restitutio in Integrum* in Personal Injury Claims," Taking Remedies Seriously CIAJ 2009 Annual Conference, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2006550>.

Adjin-Tettey, Elizabeth, "Replicating and Perpetuating Inequalities in Personal Injury Claims Through Female-Specific Contingencies" (2004) 49 McGill Law Journal 311.

Aikenhead, Moira "Non-Consensual Disclosure of Intimate Images as a Crime of Gender-Based Violence" (2018) 30(1) Canadian Journal of Women and the Law 117.

Allen, Anita, "Privacy torts: Unreliable remedies for LGBT plaintiffs" (2010) 98(6) California Law Review 1711.

Allen, Anita & Erin Mack "How privacy got its gender" (1991) 10 Northern Illinois University Law Review 441.

Austin, Lisa M. "Privacy and Private Law: The Dilemma of Justification" (2010) 55 McGill Law Journal 165.

Bailey, Jane "Implicitly Feminist?: The Supreme Court of Canada's Decision in R v Jarvis" (2020) 32 Canadian Journal of Women and the Law 196.

Bailey, Jane "Missing Privacy Through Individuation: The Treatment of Privacy Law in the Canadian Case Law on Hate, Obscenity, and Child Pornography" (2008) 31:1 Dalhousie Law Journal 55.

Bailey, Jane "'Sexualized Online Bullying' Through an Equality Lens: Missed Opportunity in *AB v Bragg*?" (2013) 59 McGill Law Journal 709.

Bailey, Jane "Towards an Equality Enhancing Conception of Privacy" (2008) 31(2) Dalhousie Law Journal 267.

Balos, Beverly, "A Man's Home is his Castle: How the Law Shelters Domestic Violence and Sexual Harassment" (2004) 23 St. Louis University Public Law Review 77.

Bender, Leslie, "Teaching Torts as if Gender Matters: Intentional Torts" (1994) 2 Virginia Journal of Social Policy and Law 115.

Bender, Leslie, "Tort Law's Role as a Tool for Social Justice" (1998) 37 Washburn Law Journal 249.

Beswick, Samuel and William Fotherby, "The Divergent Paths of Commonwealth Privacy Torts" (2018) 84 Supreme Court Law Review 225.

Blakey, G. Robert, "The Rule of Announcement and Unlawful Entry: Miller v. United States and Ker v. California" (1964) 112 University of Pennsylvania Law Review 499.

Blomely, Nicholas "Flowers in the Bathtub: Boundary Crossings at the Public-Private Divide" (2005) 36 Geoforum 281.

Blomley, Nicholas "Law, Property and the Spaces of Violence: The Frontier, the Survey, and the Grid" (2003) 93 Annals, Association of American Geographers 121.

Bowman, Cynthia Grant "Street Harassment and the Informal Ghettoization of Women" (1993) 106 Harvard Law Review 517.

Bracken-Roche, Ciara, "Domestic Drones: The Politics of Verticality and the Surveillance Industrial Complex" (2016) 71 Geographica Helvetica 167.

Bridges, Khiara, "Privacy Rights and Public Families" (2011) 34 Harvard Journal of Law & Gender 113.

Buolamwini, Joy & Timnit Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification" (2018) 81(1) Proceedings of Machine Learning Research 1.

Calo, Ryan, "Robotics and the Lessons of Cyberlaw" (2015) 103 California Law Review 514.

Calo, Ryan "The Boundaries of Privacy Harm" (2011) 86 Indiana Law Journal 1131.

Calo, Ryan, "The Drone as Privacy Catalyst" (2011) 64 Stanford Law Review 29.

Cameron, Angela and Paul Daly, "Furthering Substantive Equality Through Administrative Law: Charter Values in Education" (2013) 63 Supreme Court Law Review (2d) 169.

Chandler, Jennifer, "Technological Self-Help and Equality in Cyberspace" (2010) 56(1) McGill Law Journal 39.

Chamallas, Martha, "The Architecture of Bias: Deep Structures in Tort Law" (1998) 146 University of Pennsylvania Law Review 463.

Chao, HaiYang and YongCan Cao, and YangQuann Chen, "Autopilots for Small Unmanned Aerial Vehicles: A Survey" (2010) 8(1) International Journal of Control, Automation, and Systems 36.

Chartrand, Larry, "The Crumbling Wall of *Bhadauria*: If Not Today, Tomorrow" (2009) 44 Supreme Court Law Review 107.

Citron, Danielle Keats "Mainstreaming Privacy Torts" (2010) 98 California L R 1805.

Citron, Danielle Keats "Technological Due Process" (2008) 85 Washington University Law Review 1249.

Citron, Danielle and Daniel Solove, "Privacy Harms" (2022) 102 Boston University Law Review (forthcoming).

Clarke, Roger "Appropriate Regulatory Responses to the Drone Epidemic" (2016) 32 Computer Law and Security Report.

Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance" (1993) 4 Journal of Law & Information Science 4032.

Clarke, Roger, "The Regulation of Civilian Drones: Impacts on Behavioural Privacy" (2014) 30 Computer Law & Security Review 286.

Clarke, Roger, "Understanding the Drone Epidemic" (2014) 30 Computer Law and Security Report 230.

Clarke, Roger, "What Drones Inherit from their Ancestors" (2014) 30(3) Computer Law & Security Review 247.

Cofone, Ignacio and Adriana Roberston, "Privacy Harms" (2018) 69 Hastings Law Journal 1039.

Cohen, Julie, "Privacy, Visibility, Transparency, and Exposure" (2008) 75 The University of Chicago Law Review 181.

Craig, John D.R. "Invasion of Privacy and Charter Values: The Common-Law Tort Awakens" (1997), 52 McGill LJ 355.

Darian-Smith, Eve, "Neighborhood Watch – Who Watches Whom? Reinterpreting the Concept of Neighborhood" (1993) 52 Human Organization 83.

Davis, D. "The harm that has no name: Street harassment, embodiment, and African American Women" (1994) 4 UCLA Women's Law Journal 133.

Dodge, Alexa, "The digital witness: The role of digital evidence in criminal justice responses to sexual violence" (2017) Feminist Theory 1.

Elish, Madeleine Clare, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction" (2019) 5 Engaging Science, Technology, and Society 40.

Friedland, Hadley "Making Space for the Cree Reasonable Person in the Canadian Justice System" (2016) 67 UNB Law Journal 269.

Froc, Kerri "Constitutional Coalescence: Substantive Equality as a Principle of Fundamental Justice" (2012) 42 Ottawa Law Review 411.

Gavison, Ruth "Privacy and the Limits of Law" (1980) 89 Yale Law Journal 421.

Gilman, Michele, "The Class Differential in Privacy Law" (2012) 77 Brook Law Review 1389.

Goodman, Dena, "Public Sphere and Private Life: Toward a Synthesis of Current Historiographical Approaches to the Old Regime" (1992) 31 History and Theory 1.

Goold, Benjamin, "Surveillance and the Political Value of Privacy" (2009) 1 Amsterdam Law Forum 3.

Gotell, Lise, "When privacy is not enough: Sexual assault complainants, sexual history evidence and the disclosure of personal records" (2006) 43 Alberta Law Review 743.

Hafetz, Jonathan L ""A Man's Home is his Castle?": Reflections on Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries" (2002) 8(2) William & Mary Journal of Women and the Law 175.

Harris, Cheryl, "Whiteness as Property" (1993) 106(8) Harvard Law Review 1707.

Hartzog, Woodrow "The Public Information Fallacy" (2019) 99 Boston University Law Review 459.

Heenan, Deirdre "Challenging Stereotypes Surrounding Disability and Promoting Anti-oppressive Practice: Some Reflections on Teaching Social Work Students in Northern Ireland" (2005) 24(5) Social Work Education 495.

Hewitt, Jeffery G, "Land Acknowledgement, Scripting and Julius Caesar" (2019) 88 SCLR 27.

Holden, Paul "Flying Robots and Privacy in Canada" (2016) 14 Canadian Journal of Law and Technology 65.

Hughes, Patricia "Recognizing Substantive Equality as a Foundational Constitutional Principle" (1999) 22 Dalhousie Law Journal 5.

Hunt, Chris, "From Right to Wrong: Grounding a "Right" to Privacy in the "Wrongs" of Tort" (2015) 52(3) Alberta Law Review 635.

Hutchinson, Terry and Nigel Duncan, "Defining and Describing What We Do: Doctrinal Legal Research" (2012) 17 Deakin Law Review 83.

Froomkin, A. Michael, "The Death of Privacy?" (2000) 52 Stanford Law Review 1461.

Froomkin, A. Michael and Zak Colangelo, "Self-Defense Against Robots and Drones" (2015) 48 Connecticut Law Review 1.

Ha-Redeye, Omar, "Class Action Intrusions: A Development in Privacy Rights or an Indeterminate Liability" (2015) 6(1) Western Journal of Legal Studies 1.

Hargreaves, Stuart "'Jones-ing' for a Solution: Commercial Street Surveillance and Privacy Torts in Canada" (2014) 3(3) *Laws* 388.

Hargreaves, Stuart, "'Relational Privacy' & Tort" (2017) 23(3) William & Mary Journal of Women & the Law 433.

Hogg, Peter "Equality as a Charter Value in Constitutional Interpretation" (2003) 20 Supreme Court Law Review 113.

Hunt, Chris DL "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37 Queen's LJ 167.

Hunt, Chris DL "Privacy in the Common Law: A Critical Appraisal of the Ontario Court of Appeal's Decision in Jones v Tsige" (2011) 37 Queen's Law Journal 665.

Kalhan, Anil, "Immigration Surveillance" (2014) 74 Maryland Law Review 1.

Kelly, Lisa "A Tale of Two Cameras: Sex and Surveillance in *R v Jarvis*" (2019) 52 Criminal Reports 126.

Kerr, Ian "Schrödinger's Robot: Privacy in Uncertain States" (2019) 20 Theoretical Inquiries in Law 123.

Kerr, Ian and Jena McGill "Emanations, Snoop Dogs and Reasonable Expectation of Privacy" (2007) 52 Criminal Law Quarterly 392.

Koskela, Hille "'The gaze without eyes': video-surveillance and the changing nature of urban space" (2000) 24 Progress in Human Geography 243.

Layard, Antonia "Public Space: Property, Lines, Interruptions" (2016) 2(1) Journal of Law, Property and Society 1.

Lingel, Jesssa "A Queer and Feminist Defence of Being Anonymous Online" (2021) Hawaii International Conference on Systems Sciences, online: <https://scholarspace.manoa.hawaii.edu/handle/10125/70925>.

MacDonnell, Vanessa "A Theory of Quasi-Constitutional Legislation" (2016) 53 Osgoode Hall Law Journal 508.

Mackey, Jared A "Privacy and the Canadian Media: Developing the New Tort of 'Intrusion Upon Seclusion' With Charter Values" (2012) 2 (1) University of Western Ontario Journal of Legal Studies 3.

MacTavish, L.R. "Uniformity of Legislation in Canada – An Outline" (1947) 25 Canadian Bar Review 36.

Majury, Diana "The Charter, Equality Rights, and Women: Equivocation and Celebration" (2002) 40(4) Osgoode Hall Law Journal 297.

Manokha, I. "Surveillance, Panopticism, and Self-Discipline in the Digital Age" (2018) 16(2) Surveillance and Society 219.

Marks, Mason "Robots in Space: Sharing Our World with Autonomous Delivery Vehicles" (Paper delivered at We Robot, University of Miami School of Law, Coral Gables, FL, 12 April 2019) [unpublished], online: <http://robots.law.miami.edu/2019/wp-content/uploads/2019/03/Mason-Marks-Robots-in-Space-WeRobot-2019-3-14.pdf>.

Mayeda, Graham, "My Neighbour's Kid Just Bought a Drone… New Paradigms for Privacy Law in Canada" (2016) 35(1) National Journal of Constitutional Law 59.

McClurg, Andrew Jay "Bringing Privacy Law Out of the Closet: A Tort Theory for Intrusions in Public Places" (1995) 73 North Carolina Law Review 9.

McNeal, Gregory S., "Drones and Aerial Surveillance: Considerations for Legislators" *Brookings Institution: The Robots Are Coming: The Project on Civilian Robotics,* November 2014 Pepperdine University Legal Studies Research Paper No. 2015/3.

Mizrahi, Sarit "Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things?" (2018) 8 Western Journal of Legal Studies 3.

Moreham, NA, "Privacy in the Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 Law Quarterly Rev 628.

Morrison, Caren Myers "Dr. Panopticon, or, How I Learned to Stop Worrying and Love the Drone" (2014) 27 Journal of Civil Rights and Economic Development 747.

Nelson, S.L. "Sex work and social media: Policy, identity, and privacy in networked publics and counterpublics" (2019) 8(1) Lateral: Journal of the Cultural Studies Association.

Okindegbe, Ngozi "Discredited Data" (2022) 107 Cornell Law Review (*forthcoming*).

Osucha, Eden, "The Whiteness of Privacy: Race, Media, Law" (2009) 24 Camera Obscura 1.

Paton-Simpson, Elizabeth "Private Circles and Public Squares: Invasion of Privacy by the Publication of 'Private Facts'" (1998) 61(3) Modern Law Review 318.

Patton, Jason "Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places" (2000) 2(3) Ethics and Information Technology 181.

Penney, Jon "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31 Berkeley Technology Law Journal 117.

Post, Robert C., "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 California Law Review 957.

Power, Mark C and Darius Bossé, "Une tentative de clarification de la présomption de respect des valeur de la Charte canadienne des droits et libertés" (2014) 55 Les Cahiers de Droit 775.

Prosser, William L, "Privacy" (1960) 48 California Law Review 383.

Reidenberg, Joel, "Privacy in Public" (2014) 69 University of Miami Law Review 141.

Rosenbaum, Dennis P., "The Theory and Research Behind Neighborhood Watch: Is it a Sound Fear and Crime Reduction Strategy?" (1987) 33 Crime & Delinquency 103.

Ruddick, S. "Constructing Difference in Public Spaces" (1996) 17 Urban Geography 132.

Rule, Troy, "Airspace in an Age of Drones" (2015) 95 Boston University Law Review 155.

Ruparelia, Rakhi, "'I Didn't Mean it that Way!: Racial Discrimination as Negligence" (2009) 44 Supreme Court Law Review 81.

Ruppert, Evelyn S. "Rights to Public Space: Regulatory Reconfigurations of Liberty" (2006) 27 Urban Geography 271.

Scassa, Teresa, "Information Privacy and Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy" (2010) 7 Canadian Journal of Law and Technology 193.

Scassa, Teresa, "Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges" (2017) 14(2) SCRIPTed 239.

Scassa, Teresa, "Police Service Mapping as Civic Technology: A Critical Assessment" (2016) 5(3) International Journal of E-Planning Research 13.

Schlag, Chris, "The New Privacy Battle: How the Expanding Use of Drones Continues to Erode our Concept of Privacy and Privacy Rights [Note]" (2012-2013) 13 Pittsburg Journal of Technology Law & Policy 1.

Selinger, Evan and Woodrow Hartzog, "The Inconsentability of Facial Surveillance" (2019) 66 Loyola Law Review 101.

Sossin, Lorne and Mark Friedman, "Charter Values and Administrative Justice" (2014) 67 Supreme Court Law Review (2d) 391.

Steeves, Valerie, "If the Supreme Court Were on Facebook: Evaluating the Reasonable Expectation of Privacy Test from a Social Perspective" (2008) 50 Canadian Journal of Criminology and Criminal Justice 331.

Stewart, Hamish "Normative Foundations for Reasonable Expectations of Privacy" (2011) 54 Supreme Court Law Review 335.

Sutherland, Kate, "Precedent, Principle and Pragmatism: Justice Wilson and the Expansion of Tort Law" (2008) 41 Supreme Court Law Review 131.

Sullivan, Ruth "Statutory Interpretation in a Nutshell" (2003) 82 Canadian Bar Review 51.

Takhshid, Zahra, "Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort" (2020) 1 Buffalo Law Review 139.

Thomasen, Kristen, "Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation" 16(2) Canadian Journal of Law and Technology 307.

Thomasen, Kristen "Robots, Regulation, and the Changing Nature of Public Space" (2020) 51 Ottawa Law Review 275.

Thompson, Scott and Alana Saulnier, "The "Rise" of Unmanned Aerial Vehicles (UAVs) in Canada: An Analysis of Special Flight Operation Certificates (SFOCs) from 2007 to 2012" (2015) 41 Canadian Public Policy 207.

Thompson, Scott and Ciara Bracken-Roche, "Understanding Public Opinion of UAVs in Canada: A 2014 Analysis of Survey Data and Its Policy Implications" (2015) 3 Journal of Unmanned Vehicle Systems 156.

Tuck, Eve & K Wayne Yang, "Decolonization Is Not a Metaphor" (2012) 1:1 Decolonization: Indigeneity, Education & Society 1.

Villasenor, John, "Observations from Above: Unmanned Aircraft Systems and Privacy" (2013) 36 Harvard Journal of Law & Public Policy 457.

Waldron, Jeremy "Homelessness and Community" (2000) 50(4) UTLJ 371.

Warren, S.D. & L.D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193.

Weinrib, Ernst, "The Special Morality of Tort Law" (1989) 34(3) McGill Law Journal 403.

Woo, Jesse, Jan Whittington & Ronald Arkin, "Urban Robotics: Achieving Autonomy in Design and Regulation of Robots and Cities" (2020) 52 Connecticut Law Review 319.

Wriggins, Jennifer B. "Toward a Feminist Revision of Torts" (2010) 12 Am U Journal of Gender, Social Policy & Law 139.

Zhang, Guangda, Hai-Ning Liang & Yong Yue, "An Investigation of the Use of Robots in Public Spaces" (Paper delivered at the 2015 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Shenyang, 8 June 2015).

Secondary Materials: Online & Media Resources

"Amazon's Ring Leads Google's Nest As 16% Of US Homes Adopt Video Doorbells: Strategy Analytics" (February 13, 2020), Business Wire, online: <https://www.businesswire.com/news/home/20200213005824/en/Amazon%E2%80%99s-Ring-Leads-Google%E2%80%99s-Nest-16-Homes>.

"Class action over forensic hospital strip searches reaches proposed settlement" (Feb 5, 2020) CBC News, online: <https://www.cbc.ca/news/canada/nova-scotia/class-action-suit-strip-searches-1.5452653>.

"Drone Stalker Jailed for Spying on Ex-Girlfriend" (November 20, 2020) BBC News, online: <https://www.bbc.com/news/uk-wales-55018682>.

"Laws Trample on Privacy" *Daily Colonist*, Victoria BC Saturday January 30, 1971 page 8, online: <www.britishcolonist.ca>.

"New Bill to protect privacy," The Province (26 January 1968), in British Columbia, Legislative Assembly, Sessional Clipping Books: Newspaper Accounts of the Debates (microform).

"Windsor Partnership with Amazon Ring Doorbell Could Do More Harm than Good, Experts Say" (January 23, 2020), CBC Windsor, online: <https://www.cbc.ca/news/canada/windsor/windsor-amazon-ring-partnership-could-do-harm-experts-say-1.5437144>.

Adams, Susan, "The Exclusive Inside Story of Ring: From 'Shark Tank' Reject to Amazon's Latest Acquisition" (February 27, 2018) Forbes, online: <https://www.forbes.com/sites/susanadams/2018/02/27/amazon-is-buying-ring-the-pioneer-of-the-video-doorbell-for-1-billion/?sh=dec1594706c2>.

Allain, Rhett, "How Do Drones Fly? Physics, of Course!" (May 19, 2017) WIRED online: <https://www.wired.com/2017/05/the-physics-of-drones/>.

Bendel, Oliver, "Service Robots in Public Spaces", Telepolis (25 June 2017), online: <https://www.heise.de/tp/features/Service-Robots-in-Public-Spaces-3754173.html?seite=all>.

Benton, Joshua, "The Doorbell Company that's Selling Fear" (May 1, 2019) The Atlantic, online: <https://www.theatlantic.com/ideas/archive/2019/05/amazon-owned-ring-wants-report-crime-news/588394/>.

Biddle, Sam "Amazon's Ring Planned Neighbourhood "Watch Lists" Built on Facial Recognition" (November 26, 2019) The Intercept, online: <https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/>.

Boynton, Sean, "Ahmaud Arbery: Murder Charges Laid After Case of Slain Black Man Sparks Outrage in US" (May 7, 2020) Global News, online: <https://globalnews.ca/news/6919350/charges-laid-ahmaud-arbery-shooting/>.

Brown, Nancy "Detective Invaded Privacy" The Daily Colonist, Victoria BC, Saturday December 13, 1969 page 1, online: <www.britishcolonist.ca>.

Butler, Colin "Ex-teacher who filmed students with spy pen, Ontario school board named in $200K civil suit" (April 23, 2021) CBC News, available online: <https://www.cbc.ca/news/canada/london/ryan-jarvis-beal-voyeurism-civil-lawsuit-1.5996802>.

Carr Smyth, Julie "States Push Back Against Use of Facial Recognition by Police" (May 5, 2021) ABC News, online: < https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175>.

Cavoukian, Ann, "Privacy and Drones: Unmanned Aerial Vehicles" (August 2012), online: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-drones.pdf>.

Chapman, Andrew, "Drone Types: Multi-Rotor vs Fixed-Wing vs Single Rotor vs Hybrid VTOL" (June 2016) Australian DRONE Magazine, online at: <https://www.auav.com.au/articles/drone-types/>.

Chen, Brian X, "Your Doorbell Camera Spied on You. Now What?" (February 19, 2020) The New York Times, online: <https://www.nytimes.com/2020/02/19/technology/personaltech/ring-doorbell-camera-spying.html>.

Dellinger, AJ, "How Drones are Being Weaponized and Used to Stalk and Harass People" (September 19, 2019) Mic, online: <https://www.mic.com/p/how-drones-are-being-weaponized-used-to-stalk-harass-people-18784714>.

Dickson, EJ, "How facial recognition technology could bring a slutshaming nightmare" (May 31, 2019) Rolling Stone, online: <https://www.rollingstone.com/culture/culture-features/facial-recognition-technology-porn-stars-sexism-841743/>.

Amy Dodge, "This voyeurism case changed Canadian privacy laws. It also changed this victim's life" (February 12, 2020) CBC News, online: <https://www.cbc.ca/news/canada/london/>.

Farviar, Cyrus, "Cute Videos, But Little Evidence: Police Say Amazon Ring Isn't Much of a Crime Fighter" (February 15, 2020) NBC News, online: <https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026>.

Faviar, Cyrus, ""Drone Slayer" Cleared of Charges: "I wish this had never happened" (October 27, 2015) Ars Technica, online: <https://arstechnica.com/tech-policy/2015/10/drone-slayer-cleared-of-charges-i-wish-this-had-never-happened/>.

Faviar, Cyrus, "Judge Rules in Favor of "Drone Slayer," Dismisses Lawsuit Filed by Pilot" (March 24, 2017) Ars Technica, online: <https://arstechnica.com/tech-policy/2017/03/judge-rules-in-favor-of-drone-slayer-dismisses-lawsuit-filed-by-pilot/>.

Gilliard, Chris, "Caught in the Spotlight" (January 9, 2020) Urban Omnibus, online: <https://urbanomnibus.net/2020/01/caught-in-the-spotlight/>.

Goode, Lauren and Louise Matsakis, "Amazon Doubles Down on Ring Partnerships with Law Enforcement" (January 7, 2020) WIRED, online: <https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/>.

Government of Canada, "Making an Accessible Canada for Persons with Disabilities" (February 4, 2022), online: < https://www.canada.ca/en/employment-social-development/programs/accessible-canada.html>.

Harwell, Drew "Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns" (August 28, 2019) Washington Post, online: <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true>.

Harwell, Drew, "Wrongfully Arrested Man Sues Detroit Police Over False Facial Recognition Match" (April 13, 2021) The Washington Post, online: <https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/>.

Haskins, Caroline "Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement" (July 25, 2019) Motherboard, online: <https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement>.

Hartzog, Woodrow and Evan Selinger, "Obscurity: A Better Way to Think About Your Data Than 'Privacy'" (January 17, 2013) The Atlantic, online: <

https://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/>.

Kaminski, Margot, "Enough with the "Sunbathing Teenager" Gambit" (May 17, 2016) Slate, online: < https://slate.com/technology/2016/05/drone-privacy-is-about-much-more-than-sunbathing-teenage-daughters.html>.

Kolodny, Lora, "Fixed-wing Drones Not Quite Taking Off in Commercial Market, a New DroneDeploy Study Finds" (August 15, 2016) TechCrunch, online: <https://techcrunch.com/2016/08/15/fixed-wing-drones-not-quite-taking-off-in-commercial-market-a-new-dronedeploy-study-finds/>.

Laidlaw, Emily "The Future of the Tort of Privacy" (March 30, 2021) *The Canadian Bar Association National Magazine*, online: <https://www.nationalmagazine.ca/en-ca/articles/law/opinion/2021/the-future-of-the-tort-of-privacy>.

McCabe, Samantha "BC Makes First Moves Against 'Revenge Porn"' (May 13, 2021) The Tyee, online: <https://thetyee.ca/News/2021/05/13/BC-Makes-First-Moves-Against-Revenge-Porn/>.

McFarland, Matt, "Amazon Considers AI-Powered Doorbell Cameras to Stop Package Theft" (May 10, 2019) CNN Business, online: < https://www.cnn.com/2019/05/10/tech/amazon-package-theft/index.html>.

Milmo, Dan "Amazon asks Ring owners to respect privacy after court rules usage broke law" (October 14, 2021) The Guardian, online: <https://www.theguardian.com/uk-news/2021/oct/14/amazon-asks-ring-owners-to-respect-privacy-after-court-rules-usage-broke-law>.

Mola, Rani, "The Rise of Fear-Based Social Media like Nextdoor, Citizen, and now Amazon's Neighbors" (May 7, 2019) Recode, online: <https://www.vox.com/recode/2019/5/7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors>.

Morrison, Sara, "All those hacks got Amazon's Ring sued" (December 27, 2019) Recode, online: <https://www.vox.com/recode/2019/12/27/21039517/amazon-ring-hacking-lawsuit>.

Office of the Privacy Commissioner of Canada Research Group, "Drones in Canada: Will the Proliferation of Domestic Drone Use in Canada Raise New Concerns for Privacy" (2013) online: <https://www.priv.gc.ca/ information/research-recherche/2013/ drones_201303_e.asp>.

Pearson, Jordan, "Meet the 'Drone Vigilante' who Spies on Sex Workers" (April 4, 2016) Vice News, online: <https://www.vice.com/en/article/kb7zga/drone-vigilante-brian-bates-johntv-oklahoma-spies-on-sex-workers>.

Petty, Tawana "Defending Black Lives Means Banning Facial Recognition" (July 10, 2020) WIRED, online: <https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/>.

Pulrang, Andrew "Ableist Narratives that Poison Disability Policy and Disabled People's Lives" (December 27, 2019) Forbes, online: <https://www.forbes.com/sites/andrewpulrang/2019/12/27/ableist-narratives-that-poison-disability-policy-and-disabled-peoples-lives/?sh=7499be137eb6>.

Rech, Natalie "Homelessness in Canada" (July 9, 2019) The Canadian Encyclopedia, online: <https://www.thecanadianencyclopedia.ca/en/article/homelessness-in-canada>.

Rothrock, Kevin "Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses" (April 26, 2016) arsTechnica, online: <https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a-weapon-against-russian-porn-actresses/>

Sonnemaker, Tyler, "Amazon Ring Recruited LAPD Officers as Brand Ambassadors to Help Sell its Products Through Influencer Marketing" (June 17, 2021), Business Insider, online: <https://www.businessinsider.com/amazons-ring-recruited-lapd-officers-as-brand-ambassadors-report-2021-6>.

Stewart, Bonnie, "One Ring to rule them all: Surveillance 'smart' tech won't make Canadian cities safer" (January 21, 2020), The Conversation, online <https://theconversation.com/one-ring-to-rule-them-all-surveillance-smart-tech-wont-make-canadian-cities-safer-129747>.

Sun, Yazhou, "Connecticut Woman Arrested for Assaulting Teenager Flying Drone" (June 10, 2014) ABC News, online: <https://abcnews.go.com/US/conn-woman-arrested-assaulting-teenager-flying-drone/story?id=24076891>.

Thomasen, Kristen, "Drones in Canada: Who Can Regulate What?" (November 5, 2015) CLTS, online: <https://droittech.uottawa.ca/nouvelles/drones-canada-who-can-regulate-what-why-potatoes-might-be-good-drone-regulation>.

Transport Canada, "Find your Category of Drone Operation" (February 19, 2021), online: <https://www.tc.gc.ca/en/services/aviation/drone-safety/find-category-drone-operation.html>.

Transport Canada, "Privacy Guidelines for Drone Users" (May 28, 2019) online: <https://www.tc.gc.ca/en/services/aviation/drone-safety/privacy-guidelines-drone-users.html>

Villasenor, John, "What is a Drone Anyway?" (Apr 12 2012) Scientific American, online: <https://blogs.scientificamerican.com/guest-blog/what-is-a-drone-anyway/>.

Wilson, Kerrisa, "Several arrests made after Toronto clears out large encampment at Trinity Bellwood's Park" (June 22, 2021) CP24, online: < https://www.cp24.com/news/several-arrests-made-after-toronto-clears-out-large-encampment-at-trinity-bellwoods-park-1.5480357>.

Wire, Si, "Bloody Finger Forces [Cleveland] Starter Trevor Bauer to Leave ALCS Game 3" (October 17, 2016), Sports Illustrated, online: <https://www.si.com/mlb/2016/10/18/trevor-bauer-finger-blood-indians-blue-jays>.

You, Tracy, "China unveils 'anti-terrorist' drone: solar-powered aircraft can reach 65,000ft and stay in the air 'for years'" (June 2, 2017) Daily Mail, online: <http://www.dailymail.co.uk/news/article-4566614/China-s-solar-powered-drone-reaches-65-000ft-high.html>.

Zhou, Steven "Toronto-Area Cop Under Investigation for Alleged Islamophobic Posts" (August 7, 2020) Vice News, online: <https://www.vice.com/en/article/y3zbev/toronto-area-cop-under-investigation-for-alleged-islamophobic-posts>.

Zuckerberg, Mark, "The Technology Behind Aquila" Facebook, online: <https://www.facebook.com/notes/mark-zuckerberg/the-technology-behind-aquila/10153916136506634/>.