Major Research Paper

Cybersecurity and Data Privacy: The Potential for an International Legal Framework, based on the European Union's Regulation

MRP 6999: Major Research Paper

Professor Roland Paris

Student No: 300309816

E. Mégane M. G. Wong Kwan Wing

Faculty of Social Sciences

University of Ottawa

21 August 2024

Introduction

With the advent of technology, there have been dramatic changes in our daily lives and our reliance on technology. The latter's growing influence and presence can be seen in our personal and professional lives, enabling us to communicate in real time irrelevant of our geographical location. There has been meteoric progress and development in recent years in the technological sector as a whole. The increasing popularity and use of social media platforms as a means of communication and information has further contributed to our reliance on digital means of communication. More recently, the dazzling innovation in artificial intelligence (AI) technology is further showcasing how technology will be intertwined with society in the future. However, lightning speed development in technology is equally bringing to light vital questions concerning data protection and management, particularly regarding data privacy. There has been growing scrutiny worldwide as to how data privacy is being protected and managed by companies, especially Big Tech firms such as the GAFAM (Google, Apple, Facebook, Amazon, Microsoft). With data breaches and access to personal data by third-party companies, users are often unaware of how their data is being handled and used and by whom. As a result, governments worldwide have been trying to devise stricter regulations that provide better protection to individuals and their personal data. The European Union has enacted the General Data Protection Regulation (GDPR) in response to privacy concerns over personal information and as a way to counter the lack of transparency over data management by companies.

This major research paper aims at analysing the importance of data privacy and the potential for an international legal framework based on the European Union's regulation, namely the GDPR. Although national-level regulation provides a level of protection to a certain extent, there is a lack of standardised protection for users. Given that companies and their data processing are not necessarily geographically bound to one country, having an

international level of regulation provides a uniform level of protection to users worldwide, regardless of geographical location. The methodology used to examine the research question will be a literature review of primary and secondary sources. Primary sources will include existing legislation, such as the GDPR, and secondary sources will focus on reviews and scholarly articles. The paper will be divided into the following sections: (i) the importance of data privacy and why it should be internationally regulated, (ii) the European Union's legislative framework – namely the GDPR and the rights involved with data privacy (iii) the prospects and challenges of it being adopted or adapted internationally. The conclusion will provide a summary of the important points analysed throughout the research paper; notably, how the European Union is a leading regulatory power – showcased by the adoption of GDPR-like legislation in over 150 countries – as well as the increasing concern over data privacy by key stakeholders.

Importance of Data Privacy and Reasons for International Regulation

In recent years, there has been growing concern on the topic of privacy in the digital realm from users as well as lawmakers. With the rapid advances and development being made in the technological sector, it is important to analyse how this progress impacts society. Amongst the panoply of digital platforms, social media platforms and services have become widely popular and are used daily by millions of individuals globally. In addition, the Internet of Things (IoT) has enabled the connection of physical objects among themselves and with the Internet, interfaces can be created to facilitate the user's daily life.[1] In order to be able to have access to and interact with digital platforms and services, it is imperative to provide some personal information to be able to use them.[2] Therefore, personal information and user

[1] Guilherme Mucelin, 'Internet of Things and Consumers' Privacy in a Brazilian Perspective: Digital Vulnerability and Dialogue of Sources,' 287-302 in Georg Borges and Christoph Sorges, *Law and Technology in a Digital Society* (Springer 2022) 287.
[2] Guilherme Mucelin, 'Internet of Things and Consumers' Privacy in a Brazilian Perspective: Digital Vulnerability and Dialogue of Sources,' (2022), 288.

data have become coveted assets for big tech companies, as well as smaller businesses and startups.[3]

As users, we have become accustomed to handing over personal data and information in order to access those digital platforms and services, without necessarily thinking of what it entails in terms of data protection. When signing up for digital platforms or services for example, we are all subjected to agreeing to the terms and conditions of the company.[4] However, most users do not take the time to read the terms and conditions of those websites as they only want to access and use the platforms; thus, they are not knowledgeable of what they have actually agreed to.[5] We just sign up for the services without really thinking who collects our data and what they do with our personal information.[6] As a result of this 'free supply' of personal information and data, the commercialisation of the latter has become the norm within the industry – namely due to targeted marketing, customised digital services and market predictions.[7] The structure of the data economy has for a long time been designed in a way that conceals the industry's operations and practices from the general public and lawmakers.[8] Until recently, data has long been considered to be company property despite originating from users' behaviour and personal data given.[9]

However, in recent years, there has been growing scrutiny over how companies use and manage personal data and information – whether from the general public or

[3] Hossein Rahnama and Alex Pentland, 'The New Rules of Data Privacy,' in Harvard Business Review (25 February 2022), https://hbr.org/2022/02/the-new-rules-of-data-privacy
[4] BBC, 'Terms and Conditions Explained: What are they all about?' (17 February 2017), https://www.bbc.co.uk/newsround/38992576
[5] Ibid.
[6] Louis Menand, 'Why do we care so much about privacy?' in The New Yorker (11 June 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy
[7] Hossein Rahnama and Alex Pentland, 'The New Rules of Data Privacy,' (2022).
[8] Ibid.
[9] Ibid.

governments.[10] Although the data economy is structured in a way to obscure its operations to users, even those who should be aware and who should have the knowledge of who has access to the data and who is using it, do not actually know.[11] The increasing number of data breaches and misusage has contributed to the questioning and reviewing of how data privacy and data protection are actually maintained by companies.[12] One of the most prominent leaks that has antagonised the scrutiny of data privacy and management by Big Tech companies and governments are the Edward Snowden's disclosures.[13] The leaks happened in May 2013 and revealed how the United States' National Security Agency (NSA) and the United Kingdom's Government Communications Headquarters (GCHQ) were gathering information through internet and phone surveillance.[14] The NSA was able to perform its surveillance by directly tapping "into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication in a surveillance programme known as Prism."[15] On the other hand, the UK's GCHQ conducted its surveillance by spying on fibre-optic cables carrying international communications and sharing those data with the NSA.[16] Through its spying operations, the GCHQ was able to gather a larger amount of data than the NSA, "tapping into 200 fibre-optic cables to give it the ability to monitor up to 600 million communications every day,"[17] over the span of 18 months. As a result of this disclosure, US intelligence agencies were forced to admit mass surveillance programs performed on their

[10] Swish Goswami, 'The Rising Concern Around Consumer Data and Privacy,' in Forbes (14 December 2020), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=5ded3eee487e
[11] Louis Menand, 'Why do we care so much about privacy?' (2018).
[12] Naim Çinar and Sezgin Ateş, 'Data Privacy in Digital Advertising: Towards a Post-Third-Party Cookie Era,' 55-77, in Michael Filimowicz (eds), *Privacy: Algorithms and Society* (Routledge 2022), 55.
[13] BBC, 'Edward Snowden: Leaks that exposed the US spy programme,' (17 January 2014), https://www.bbc.com/news/world-us-canada-23123964
[14] Ibid.
[15] BBC, 'Edward Snowden: Leaks that exposed the US spy programme,' (2014).
[16] Ibid.
[17] BBC, 'Edward Snowden: Leaks that exposed the US spy programme,' (2014).

own population.[18] The revelations enabled the general public to be informed about governments' spying activities and showcased how privacy was being infringed by government agencies.[19]

In addition, amongst the growing cases of high-profile data breaches, the Cambridge Analytica scandal further fuelled the increasing concern over data privacy and management.[20] The scandal revealed the harvesting of personal data of millions of Facebook users by the consulting firm Cambridge Analytica and the latter offering that information to clients, comprising of the Trump campaign as well.[21] Until then, most people had never really thought of looking into how much personal data Big Tech firms, such as Facebook, have on them. In order to test how much data Facebook has on its users, the Times' lead-consumer technology writer accessed his data and was stupefied by the scope of personal data that Facebook had, as well as the extensive list of companies his data has been sold to.[22] The case of Cambridge Analytica depicted how personal data can be misused to target and influence voters in an election.[23] Moreover, it is to be noted that the Cambridge Analytica scandal did not involve any data breaches; the leaks were able to take place due to the big data economy that composes the foundation of the Internet and the systemic structure of Facebook in gathering data and exploiting it for monetary purposes.[24][25][26]

---

[18] David Smith, 'What's really changed 10 years after the Snowden revelations?' in *The Guardian* (7 June 2023), https://www.theguardian.com/us-news/2023/jun/07/edward-snowden-10-years-surveillance-revelations
[19] Ibid.
[20] Guy Aridor et al., 'The effect of privacy regulation on the data industry: empirical evidence from the GDPR,' 695-730, in *The RAND Journal of Economics* (Wiley 2023), 695-696.
[21] Louis Menand, 'Why do we care so much about privacy?' (2018).
[22] Ibid.
[23] Amnesty International, 'The Great Hack: Cambridge Analytica is just the tip of the iceberg,' (24 July 2019), https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/
[24] Ibid.
[25] Julia Carrie Wong, 'The Cambridge Analytica scandal changed the world – but it didn't change Facebook,' in *The Guardian* (18 March 2019), https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
[26] Louis Menand, 'Why do we care so much about privacy?' (2018).

Both revelations unveiled the dark side of the Big Data economy – from both the private and public sector – and reframed users' perspectives on how Big Tech firms and governments actually manage our data. More fundamentally, both high-profile scandals revealed the general lack of privacy that users actually have on online platforms and the scope of personal information that can easily be gathered on the latter. So far, personal data has been deemed to be a commodity that Big Tech companies can exploit, with barely any repercussions. According to Shoshana Zuboff, the exploitation of data and the structure of the Big Data economy can be attributed to surveillance capitalism.[27] She makes the parallel between industrial capitalism and surveillance capitalism; the difference lays whereby the latter "audaciously lays claim to private experience for translation into fungible commodities that are rapidly swept up into the exhilarating life of the market."[28] Its beginning has roots in Google and was developed at Facebook with the spread of targeted advertising, leading to a new reasoning of accumulation.[29] As a result, global tech firms have convinced us to yield our privacy for the purposes of convenience.[30] Therefore, surveillance can be understood as ""a new economic order" and "an expropriation of critical human rights that is best understood as a coup from above"."[31] In essence, our private experiences has become the last possible territory to commodify.

At the heart of surveillance capitalism and the issues it raises, the fundamental right to privacy remains largely unaddressed. With targeted advertising and predictive algorithms, surveillance capitalism seeps into our daily lives with the aim of insidiously influencing our decisions and behaviour towards the most profitable outcomes for businesses; infringing

[27] Joanna Kavenna, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy',' in *The Guardian* (4 October 2019), https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy
[28] Shoshana Zuboff, 'Surveillance Capitalism and the Challenge of Collective Action,' 10-29, in *New Labor Forum* (2019), 11.
[29] Ibid.
[30] Julia Carrie Wong, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy',' (2019).
[31] Julia Carrie Wong, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy',' (2019).

upon our free will and privacy.[32] Thus, the era of surveillance capitalism "is a titanic struggle between capital and each one of us."[33] It is important to highlight that despite surveillance capitalism's anchoring in the digital realm through technology, technology should not be conflated with surveillance capitalism itself.[34] Rather technology is the means through which surveillance capitalism can be executed: "The economic orientation is the puppet master; technology is the puppet."[35] Therefore, the numerous high profile scandals and leaks have enabled the awakening of users to the reality of the Big Data economy that pervades the digital world. This in turn has been leading to the questioning of the right to privacy and to what extent the latter can actually be preserved and respected in an increasingly digital global society.

The human right to privacy is amongst one of the most fundamental rights that is protected by law at the regional, national, and international level.[36] Under the United Nations' Universal Declaration of Human Rights (UDHR), article 12 of the Declaration stipulates an individual's right to privacy, as well as the right to be protected by law against such interference or attack.[37] The International Covenant on Civil and Political Rights (ICCPR) equally stipulates the right to privacy and its protection under article 17 of the Covenant.[38] Despite the non-binding nature of the UDHR, it sets out the protection of fundamental human rights, with the aim of being applied at regional and global levels.[39] In addition, the European Convention on Human Rights (ECHR) sets forth the right to privacy – but differs slightly in

[32] Ibid.
[33] Julia Carrie Wong, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy',' (2019).
[34] Shoshana Zuboff, 'Surveillance Capitalism and the Challenge of Collective Action,' (2019), 11.
[35] Shoshana Zuboff, 'Surveillance Capitalism and the Challenge of Collective Action,' (2019), 11.
[36] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' 1-401, in *Privacy and the Role of International Law in the Digital Age* (Oxford University Press 2023), 1.
[37] Universal Declaration of Human Rights (adopted 10 December 1948) 217 A(III) (UNGA), art. 12.
[38] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (hereinafter ICCPR), art. 17.
[39] Universal Declaration of Human Rights (adopted 10 December 1948) 217 A(III) (UNGA), art. 12.

wording to the definition of privacy in the UDHR and the ICCPR.[40] The right to privacy is protected under article 8 of the ECHR as such:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[41]

Therefore, under such a definition – particularly paragraph 2 of article 8 – it can be understood that the right to privacy is not absolute; the condition for its limitations however is laid out by law.[42]

The origin of the right to privacy dates from the 19th century through the article of Samuel. D. Warren and Louis Brandeis in the Harvard Law Review in protest to the invasive activities of journalists.[43][44][45][46] They defined privacy as the right to be left alone notably "based on a principle to "inviolate personality"."[47] Their article has fuelled the argument about privacy and has been further defined by Alan Westin as "the right of the individual to

[40] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' 589-604, in *International Community Law Review* (Brill, 21 November 2023), 592.
[41] European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953), as amended by Protocols Nos. 11, 14 and 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, art. 8.
[42] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 592.
[43] Jeroen van den Hoven et al., 'Privacy and Information Technology,' in Edward N. Zalta (eds), *The Stanford Encyclopedia of Philosophy* (20 November 2014), https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=it-privacy
[44] Privacy Commissioner of Canada, 'Privacy as a fundamental right in the digital age,' (24 February 2023), https://www.priv.gc.ca/en/opc-news/speeches/2023/sp-d_20230224/
[45] Louis Menand, 'Why do we care so much about privacy?' (2018).
[46] Priscilla M. Regan, 'Social values and privacy law and policy,' 161-175, in Gloria González, Rosamunde Van Brakel and Paul de Hert (eds), *Research Handbook on Privacy and Data Protection Law* (15 March 2022), 161.
[47] Jeroen van den Hoven et al., 'Privacy and Information Technology,' (2014).

decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public."[48] This definition puts the emphasis on the individual right and individual control and influenced much of the legal and philosophical thinking around privacy from the late 1960s to the 1980s.[49] Simultaneously, a sociological conception of privacy emerged whereby the latter was perceived as a constituent of a well-functioning civilisation, although it did not garner as much attention.[50]

Whilst these definitions of privacy enable us to have a better understanding of what it encompasses, it should be noted that they arose at a time when the digital environment as we know it was virtually non-existent; data collection and digital technologies were absent.[51] Thus, upholding the right to privacy in our current digital era will imply facing new challenges and threats.[52] The novel threats are proving to be "complex, dynamic, geographically unbounded, and involve multiple, and often obscure actors."[53] The issue of digital technologies and the Big Data economy in regards to the right to privacy gained the attention of the international community in the 2010s.[54] The problem of mass surveillance of individuals by states was addressed in multiple reports by United Nations Special Rapporteur Frank La Rue.[55] Subsequently, the Snowden disclosures and the Cambridge Analytica scandal solely proved that surveillance in the digital era was common practice in the data economy and eventually led to strong distress on safeguarding individuals' right to privacy.[56]

[48] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 161.
[49] Ibid.
[50] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 162.
[51] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 593.
[52] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 1.
[53] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 1.
[54] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 593.
[55] Ibid.
[56] Ibid.

Given that privacy is a broad concept, developments in the United States' laws make a distinction between constitutional (or decisional) privacy and tort (or informational) privacy.[57] Constitutional privacy consist of the "freedom to make one's own decisions without interference by others in regard to matters seen as intimate and personal."[58] On the other hand, tort privacy refers to individuals' interest in having control over access to their personal information.[59] Moreover, when addressing the right to privacy, it is important to take into consideration the value that is given to privacy by individuals. There are three main values associated with privacy: common, public and collective.[60] The common value of privacy is founded on "the notion that all individuals value some degree of privacy and have some common perceptions about privacy."[61] Thus, despite differences in individual definition of privacy and what should be considered public and private, everyone recognises the importance of privacy.[62] The common value of privacy is associated with the notion that it is important for the development of a category of individual that constructs the foundation of the outlines of society that we share together.[63] Secondly, the public value of privacy refers to the importance of privacy to the democratic political system.[64] It emphasises the right to privacy as a fundamental one in constraining the use of state power, as well as the development of commonality.[65] Lastly, the collective value of privacy emanates from the argument that "technology and market forces are making it harder for any one person to have privacy without all persons having a similar minimum level of privacy."[66] Given the increasing digitalisation of society, it is challenging to uphold an individual's privacy level

[57] Jeroen van den Hoven et al., 'Privacy and Information Technology,' (2014).
[58] Jeroen van den Hoven et al., 'Privacy and Information Technology,' (2014).
[59] Ibid.
[60] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 164.
[61] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 164.
[62] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 164.
[63] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 164.
[64] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 165.
[65] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 165.
[66] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 167.

untouched by others, namely due to social networking platforms whereby others may disclose information that involves the privacy of others – knowingly or unknowingly.[67] Therefore, the collective value of privacy is becoming more and more apparent due to the omnipresence and the intricacy of communications systems on which most of modern life takes place, as well as the Big Data economy that results from and powers those organisations.[68]

Although the right to privacy is recognised to be a fundamental human right globally – notably through the UDHR, it is often discussed and protected for individuals considered to be adults (over 18 years of age). However, children's privacy has equally become a prevalent concern as they are increasingly exposed to the digital world. In general, the Convention on the Rights of the Child (CRC) sets a standard as to what a child should be protected against and the rights that they have.[69] More specifically, article 16 of the CRC stipulates the right of a child to privacy without unlawful interference, as well as protection by law against any interference to this right.[70] In 2008, the 30th International Conference of Data Protection and Privacy Commissioners released a resolution on the online privacy of children – otherwise known as the Strasbourg Resolution.[71] The concern of children's online privacy is notably due to the large amount of personal data that are being gathered from and about children through online networks.[72] According to the Resolution, children's online privacy is a unique predicament for three inter-connected reasons.[73] Firstly, the Resolution underlines the increased vulnerability of children to pressures in disclosing personal information: "they lack

[67] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 167.
[68] Priscilla M. Regan, 'Social values and privacy law and policy,' (2022), 167.
[69] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (hereinafter CRC).
[70] CRC, art. 16.
[71] Valerie Steeves and Milda Mačėnaitė, 'Data protection and children's online privacy,' 358-374, in Gloria González, Rosamunde Van Brakel and Paul de Hert (eds), *Research Handbook on Privacy and Data Protection Law* (15 March 2022), 358.
[72] Ibid.
[73] Ibid.

the experience, technical knowledge and tools to mitigate those risks."[74] In addition, the creation of a lasting digital archive risks impacting children more than adults, as such a record can challenge their privacy, security and dignity at present or later on in life.[75][76] Lastly, the Resolution reinforces the principles and the rights outlined in the CRC as well as the protection of these rights – including the right to privacy and its protection.[77][78]

With the rapid expansion and evolution of modern technologies, regulatory frameworks – whether national or international – are not widespread and comprehensive enough to ensure the protection of privacy of individuals nationwide and worldwide. Although the right to privacy has been recognised since the end of the 19th century and was enshrined in the UDHR and the ICCPR, there is still a lack of comprehensive international regulation when it comes to online privacy and its protection in the modern digital era. Despite the national adoption of laws governing technology and online privacy in countries around the world, there is no degree of uniformity when it comes to legal protection, as each country has diverging approaches.[79] As noted by the UN Special Rapporteur on the right to privacy, domestic and international legislations regarding privacy and data collection are vague in nature.[80] The report equally emphasises the need for better regulation on personal data processing activities, as well as the implicit requirement of effectively enforcing regulation; more specifically, it stipulates that sole acknowledgement of and the formulation of legislation is not enough, in a democratic system of government, to enforcing regulation.[81]

---

[74] 30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Children's Privacy Online,' (Strasbourg, 17 October 2008), para 4.
[75] 30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Children's Privacy Online,' (Strasbourg, 17 October 2008), para 7.
[76] Valerie Steeves and Milda Mačėnaitė, 'Data protection and children's online privacy,' (2022), 358.
[77] Ibid.
[78] 30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Children's Privacy Online,' (Strasbourg, 17 October 2008), para 8-9.
[79] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 2.
[80] Ana Brian Nougrères, Special Rapporteur on the right to privacy, 'Report: Right to privacy: Note by the Secretary-General,' (20 July 2022) UN Doc A/77/196, para 2.
[81] Ana Brian Nougrères, 'Right to privacy: Note by the Secretary-General,' (2022), para 2.

Therefore, having an international legislative framework will set a uniform standard of protection to the right to privacy, as well as ensuring its enforcement.

On a global level, the first treaty to address the processing of personal data is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also known as Convention 108) adopted by the Council of Europe in 1981.[82] The Convention provides a basis of protection to the right to privacy – including transborder flow of data – and to this day, remains valid with various amendments over time.[83][84] The amendments to Convention 108 allow it to better tackle challenges that arise from ongoing developments in technologies over the years.[85] Moreover, the Special Rapporteur report based its regulatory analysis on seven legislative documents, namely: the General Data Protection Regulation (GDPR) of the European Union, the modernised Convention 108, the United Nations Guidelines, the Ibero-American Standards, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, and the OAS Principles.[86] Nonetheless, the seven treaties are only at the regional level and can only be implemented by states that are members of those organisations. Thus, the principles stated in those legal documents are binding only to those member states and are limited in scope of reach.

Although these treaties do address the importance and protection of privacy regarding personal data and its processing, they remain broad and only provide protection regionally. Big Tech companies – such as the GAFAM– operate on a global scale and provide services to individuals in most countries. The transnationalisation of digital operations inevitably brings

[82] Naim Çinar and Sezgin Ateş, 'Data Privacy in Digital Advertising: Towards a Post-Third-Party Cookie Era,' (2022), 56.
[83] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, (28 January 1981).
[84] Naim Çinar and Sezgin Ateş, 'Data Privacy in Digital Advertising: Towards a Post-Third-Party Cookie Era,' (2022), 56.
[85] Ibid.
[86] Ana Brian Nougrères, 'Right to privacy: Note by the Secretary-General,' (2022), para 12.

about the transnationalisation of privacy threats that affect individuals worldwide.[87] Furthermore, it is important to highlight that most of the vital physical and technical infrastructure – as well as services – of the Internet are possessed and provided by private corporations.[88] In consequence, though Internet users worldwide are dependent on their infrastructures and services, the majority of those companies are regulated by one or more states, which themselves may adopt varying procedures.[89] Moreover, most of the services and products offered in the digital space are bound by private contractual procedures between firms and users.[90] Often times, those terms of use (or otherwise, terms and conditions) are non-negotiable, but also lengthy and use technical terms that are difficult to comprehend by lay users.[91][92]

In addition, given that most of the Internet and the services provided through the latter are privatised, it inevitably denotes the concentration of power of technology companies – which can nowadays be comparable to those of governments, if not more so powerful.[93] Thus, Big Tech companies can equally impact the enjoyment to human rights on par with governments – particularly the right to privacy.[94][95] Despite the growing power of technological companies – for instance, GAFAM – no international human rights treaties state the need for personal data protection, except the European Union's Charter of Fundamental Rights.[96] According to Amnesty International, a mix of political and regulatory solutions are needed to tackle the data-driven business model; more specifically "Human

[87] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 2.
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] BBC, 'Terms and Conditions Explained: What are they all about?' (2017).
[93] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 2.
[94] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 597.
[95] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 2.
[96] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 597.

rights provide the only international, legally binding framework that can capture the multi-faceted ways in which the business model is impacting our lives and what it means to be human."[97] Yet, to this day, international human rights law lacks in power in restricting Big Tech firms' influence in general.[98] As showcased in the Cambridge Analytica scandal, Facebook settled the legal action by paying a fine amounting to $725 million over the data breach.[99] This settlement showcases the preference of technological firms to be fined, rather than be regulated – particularly when they make astronomical amounts of pure profit every year.[100][101]

To this day, most large-scale exploitations in connection to personal data protection have been perpetrated by both corporations and governments.[102] However, most – if not all - human rights treaties concentrate entirely on states' actions, rather than those of private corporations.[103] Therefore, at the international level, there is no treaty or convention that regulates the actions of private companies in regards to the right to privacy and data protection. Most of large-scale infringement of personal data protection by governments are mass surveillance operations.[104] The issue with such operations is not solely the collection and storage of personal data, but more so the interception of communication that impedes on the right to privacy.[105] After the Snowden disclosures, the Council of Europe pressed member and observer states to accept a multilateral treaty named 'Intelligence Codex' for intelligence services; the Codex stipulated the laws regulating cooperation for the purposes of the fight

---

[97] Amnesty International, 'The Great Hack: Cambridge Analytica is just the tip of the iceberg,' (2019).
[98] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 2-3.
[99] Shiona McCallum, 'Meta settles Cambridge Analytica scandal case for $725m,' in *BBC* (23 December 2022), https://www.bbc.com/news/technology-64075067
[100] Amnesty International, 'The Great Hack: Cambridge Analytica is just the tip of the iceberg,' (2019).
[101] Joanna Kavenna, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy',' (2019).
[102] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 598.
[103] Ibid.
[104] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 599.
[105] Ibid.

against terrorism and organised crime.[106] The Codex has been a missed opportunity to regulate mass surveillance; nonetheless, it received no support from states.[107] The lack of support from states to regulate such an intrusive practice equally demonstrates the lack of urgency and willpower to respect and ensure the right to privacy of individuals. Consequently, the two principal actors that have the power to access and protect individuals' personal data and their right to privacy are also those that infringe on our privacy – and at times, even in tandem.[108]

On top of the aforementioned reasons, the advent of artificial intelligence (AI) further brings about the concern of privacy and data protection. As AI relies mainly on the collection and analysis of personal data to produce results and enhance its system, the privacy of users is violated.[109] The actual and future implications of the capabilities of AI are still a mystery; corporations and governments should tread cautiously on its development, as it could result in a pandora's box. Already, the use of machine learning to profile individuals to influence their behaviour by Big Tech companies – such as Facebook – is a cause for concern.[110] Such a model might support the fuelling of discrimination; companies and governments could easily misuse data analytics to target individuals based on particular characteristics, such as race, ethnicity, gender or religion.[111] According to a recent report from Amnesty International, the use of new technologies by public and private actors in migration systems globally exacerbates the prospect that the human rights of individuals on the move will be violated –

[106] Ibid.
[107] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 600.
[108] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 3.
[109] Privacy Commissioner of Canada, 'From state surveillance to surveillance capitalism: The evolution of privacy and the case for law reform,' (16 June 2021), https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210616/
[110] Amnesty International, 'The Great Hack: Cambridge Analytica is just the tip of the iceberg,' (2019).
[111] Ibid.

including the right to privacy.[112] Many of the instruments being used in the processing of movement of people are governed by private corporations whose business model is embedded in data extraction and accumulation for profit.[113] Therefore, it is evident that the protection of users' privacy and their right to the latter is primordial as it is intrinsically linked to other fundamental human rights.[114]

On an international level, the European Union takes personal data protection and the right to privacy very seriously in comparison to other countries and regions.[115] The mention of personal data protection in the European Union Charter of Fundamental Rights as a separate right and the introduction of the General Data Protection Regulation (GDPR) showcase the spearheading of the European Union in regard to data protection and privacy.[116] In addition, the European Court of Justice stipulated that "the right to respect for private life constituted a fundamental right protected by the legal order of the Community (now the Union)."[117] As previously mentioned, Convention 108 was among the first treaty to regulate personal data processing – further depicting the European Union's effort in providing protection on personal information. Convention 108 is often referred to in the European Court of Human Rights' judgements as a reference to the level of protection under which personal information should be maintained.[118] In terms of regulation, the GDPR is deemed to be the "toughest privacy and security law in the world."[119] Although it was implemented by the European Union, it regulates companies worldwide that collect and store data on individuals

---

[112] Amnesty International, 'New technology and AI used at borders increases inequalities and undermines human rights of migrants,' (21 May 2024), https://www.amnesty.org/en/latest/news/2024/05/global-new-technology-and-ai-used-at-borders-increases-inequalities-and-undermines-human-rights-of-migrants/
[113] Ibid.
[114] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 1.
[115] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 597.
[116] Ibid.
[117] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 597.
[118] Ibid.
[119] Ben Wolford, 'What is GDPR, the EU's new data protection law?" https://gdpr.eu/what-is-gdpr/

in the European Union.[120] Therefore, with the adoption of the GDPR, the European Union is emphasising its stance on data privacy and security.[121] The next section of the paper will analyse the GDPR and the impact it has had so far on regulating protection personal information – as well as its penalties on companies who violate users' data privacy.

The Potential for an International Legal Framework?

This next section of this research paper will analyse the feasibility of an international regulatory framework that would govern the digital economy, particularly when it comes to data privacy and the rights that it encompasses. Firstly, we will focus on the European Union's regulatory approach to data privacy; then we will examine the feasibility of scaling the latter's legislative framework to a global level, as well as the obstacles and challenges that the adoption of an international legal framework might face when it comes to regulating the digital economy.

European Union's Approach to Data Privacy

As we have analysed in the previous section of this research paper, the European Union has been a pioneer in terms of legislation aiming at regulating the digital space. Amongst the first international treaty to address the need for regulation when it comes to the processing of personal data adopted by the Council of Europe.[122] Furthermore, the adoption and implementation of the GDPR showcased the willingness of the European Union to protect users' data and provide more transparency and control to individuals over their personal information and its processing.[123] The European Union's approach to regulation is principally human-centric and puts at the core of its laws the individual and collective rights

[120] Ibid.
[121] Ibid.
[122] Naim Çinar and Sezgin Ateş, 'Data Privacy in Digital Advertising: Towards a Post-Third-Party Cookie Era,' (2022), 56.
[123] Ben Wolford, 'What is GDPR, the EU's new data protection law?".

of its citizens.[124] According to Anu Bradford, the European framework regarding the legislation of the digital economy "views the government as having a central role in both steering the digital economy and in using regulatory intervention to uphold the fundamental rights of individuals, preserve the democratic structures of society, and ensure a fair distribution of benefits in the digital economy."[125] Therefore, the government has a more interventionist presence that has often been lacking at an international level when it comes to the digital space and protecting users' rights.

The adoption of the European Declaration on Digital Rights and Principles for the Digital Decade by the European Parliament, Council, and Commission in 2022 further highlights the human-focused approach of the European Union.[126] In addition, the Declaration identifies core values that guide European policymaking, namely democracy, fairness and fundamental rights.[127] While these values do not pertain solely to the European Union, they are "directly engrained in the EU's regulatory instruments with the goal of ushering in a human-centric, democracy-enhancing, rights-preserving, and redistributive digital economy where technology is harnessed for human empowerment."[128] By maintaining that its vision of the digital economy is grounded in laws, the European Union thus rejects the techno-libertarian notion of an anarchic internet, rather promoting that digital innovation needs to be firmly rooted in the rule of law.[129] This notion of a rights-driven regulatory framework is vehemently supported by European citizens, and public opinion surveys have demonstrated that there is consequential support for more substantial regulation in the digital realm.[130] Thus, there is political and ideological harmony between policymakers and citizens

[124] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (Oxford University Press, 2023), 1-599, 105.
[125] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 105.
[126] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 106.
[127] Ibid.
[128] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 106.
[129] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 107.
[130] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 107.

when it comes to digital regulation, in comparison to other countries where partisanship prevails over important policy issues, including digital regulation.[131] This could be one of the reasons why the European Union has been able to implement more stringent policies regarding the digital economy.

The European Union's commitment to fundamental rights is reflected in its regulatory modus operandi to "data protection, artificial intelligence, and online content regulation – all policy areas that have become central pillars of the European regulatory model."[132] Given that fundamental rights are at the core of the European approach to legislating the digital economy, they provide a value-based foundation for European integration and directing the European Union's regulatory activities and its involvement globally across all policy areas.[133] Moreover, the entry into force in 2009 of the Charter of Fundamental Rights of the European Union (EU Charter) further immerses constitutional rights into treaties.[134] This Charter particularly protects crucial rights involved with the ongoing digital evolution of economies and societies, comprising of "the protection of privacy and personal data, the freedom of expression, and nondiscrimination principles."[135] By ensuring that those principles are at the core of policymaking, the European Union is recognising the need to restrict government surveillance, the exploitation of personal data by technology companies, as well as the need to protect users from discrimination by regulating algorithms, especially with the advent of artificial intelligence.[136]

The growing concern over data privacy worldwide is namely due to the rights that are involved with the management and protection of data and how privacy is ensured within data

[131] Ibid.
[132] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 110.
[133] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 110.
[134] Ibid.
[135] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 110.
[136] Ibid.

processing. The right to privacy is at the centre of the European Union's rights-based approach to regulating the digital economy; the doctrine behind such an approach to data privacy is to cultivate self-determination of individuals by allowing them to have greater control over their information.[137] In addition, the right to data privacy is closely associated to human dignity in European discourse and is considered to be inviolable.[138] The European Union's General Data Protection Regulation (GDPR) is considered to be "a global 'golden standard' on how to protect individuals' personal data from exploitation by governments or private companies alike."[139] It enumerates new obligations that are addressed under the rights of the data subject in chapter three of the Regulation.[140][141] The chapter covers articles 12 to 23, identifying and enumerating fundamental rights relating to individuals' rights over their personal data.[142] More specifically, articles 12 to 22 provide further details of each of those data subjects' rights individually.[143] The right to be informed is highlighted under articles 12 to 14 whereby those who have access to users' personal data should inform them of any rectification, erasure or restriction of processing of the latter.[144] In addition, users have the right to request who are those to whom their data has been disclosed.[145] The right to information under the GDPR is the first right that is addressed in the regulation when it comes to the data subject. Despite all users' rights being deemed as equal, the right to information is distinct as "it exemplifies the principle of transparency and represents the focal

[137] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 112.
[138] Ibid.
[139] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 112.
[140] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 112.
[141] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (hereinafter GDPR).
[142] GDPR, art. 12-23.
[143] GDPR, art. 12-22.
[144] GDPR, art. 11-14.
[145] Ibid.

point for all other rights."[146] Thus, the right to information can be viewed as primus inter pares within the GDPR and sets the standard for the other rights.

Following the right to information, the right of access illustrates a crucial element in strengthening users' control over their personal information.[147] Article 15 of the GDPR addresses the right of access by the data subject which allows the latter to be made aware of any processing of their personal data and access to the data, as well as the purpose of the processing and the categories of data that is being used and who the data will be disclosed to.[148] Having access to personal information is likely to involve individuals and promote their self-determination regarding the latter, but equally elicits scrutiny of organisations' information practices and can bring to light any misuse of data.[149] Moreover, it equally protects privacy and creates a balance of power between data subjects and data controllers.[150] Thus, the right of access provides an option to verify whether one's data has been processed and by which entity. Article 16 of the GDPR looks at the right to rectification whereby an individual is ensured the right to have information about him or her rectified if the data is inaccurate.[151] By allowing individuals to rectify information about them, it enables data subjects to have accurate information related to them to be processed and be kept up to date.

The right to erasure (also known as the right to be forgotten) is often associated to data privacy in relation to regulating the digital economy in this data-driven world. Under the GDPR, the right to be forgotten is one of the new obligations that the European Union recognises as key in regulating data privacy.[152] The right to erasure is covered under article

---

[146] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (Oxford University Press, 2021), 1-268, 64.
[147] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 104.
[148] GDPR, art. 15.
[149] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 105.
[150] Ibid.
[151] GDPR, art. 16.
[152] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 112.

17 of the regulation.[153] It stipulates that data subjects have the right to request erasure of personal data that concerns them under several conditions outlined in paragraphs (a) to (f) of paragraph 1 of the article.[154] This right can be upheld upon multiple grounds: under paragraph (a) of article 17, data subjects can ask for deletion of data that is no longer necessary in relation to the purposes for which it was collected.[155] Under paragraph (b) of the article, data can be erased if the data subject withdraws consent and there is no legal basis for the processing of data.[156] Paragraph (c) of article 17 enables deletion of data if the user objects to the processing of their personal information based on a particular situation.[157] In addition, paragraph (f) provides erasure of data in the case where personal information of children have been collected, usually via social networks.[158] Such a provision denotes the importance of the right to erasure as children in particular do not necessarily have the maturity to understand the data they generate and provide and how such information might affect their life in the future.[159] Lastly, paragraphs (d) and (e) of article 17 pertain to erasure of data in compliance with a legal obligation on the part of the controller and if the processing is unlawful.[160] These provisions under article 17 showcase the importance of the right to be forgotten and demonstrate how the rights-based approach of the European Union deems it to be of utmost importance in regards to protecting data privacy and regulating the data-driven economy.

---

[153] GDPR, art. 17.
[154] Ibid.
[155] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 141.
[156] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 142.
[157] Ibid.
[158] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 144.
[159] Ibid.
[160] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 145.

Furthermore, article 18 of the Regulation addresses the right to restriction of processing under any one of the four conditions outlined in paragraph 1 of the article.[161] Thus, if processing has been restricted, the consent of the individual is needed to process their data.[162] In addition, users have the right to request who are those to whom their data has been disclosed.[163] Furthermore, the concept of data portability is flexible and ambiguous and can be used in various contexts and defined in multiple ways.[164] The GDPR acknowledges personal data portability as an intrinsic aspect of the European Union's data protection law.[165] The requirement on data portability as part of data protection law was made in 2012 by the European Commission in the drafting of the GDPR.[166] Article 20 addresses the right to data portability whereby data subjects can access and transfer their personal data across different services.[167] Under the GDPR, the right to portability comprises two components: firstly, the right of individuals to obtain a copy of their information, and secondly, the transmission of the data to another controller without impediment.[168] Articles 21 and 22 of the GDPR cover key rights that are in connection to profiling and algorithmic decision-making.[169] The right to object under article 21 stipulates the right of a user to object to the processing of their personal data, including profiling and for direct marketing purposes.[170][171][172] Article 22 addresses the right to not be subjected to automated decision-making, which includes

[161] GDPR, art. 18.
[162] Ibid.
[163] Ibid.
[164] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 159.
[165] Ibid.
[166] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 162.
[167] GDPR, art. 20.
[168] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 163.
[169] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 189.
[170] GDPR, art. 21.
[171] Helena U. Vrabec, 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (2021), 201.
[172] Ibid.

profiling, unless it is with the user's consent or to fulfil a contract between the individual and the data controller.[173]

These fundamental rights enable users to have more control over their personal data and the processing of these data, as well as who has access to them. In addition to those rights of the data subject under Chapter three of the GDPR, there is equally the right to consent and the withdrawal of consent under article 7 of the Regulation.[174] Being able to withdraw consent that has been previously given by the user is an important aspect of article 7, as it enables data subjects to withdraw consent at any time and facilitates the removal of consent just as it facilitates giving consent.[175] More often than not, users are expected to provide their consent to companies, however it remains challenging to withdraw consent once it has been given. Moreover, with the increasing use of social media platforms, a growing concern arises when it comes to children's personal data and their right to consent. Article 8 of the GDPR does address the right of the child to consent, whereby those 16 years of age and above should provide consent to their data processing, and for those below 16 years of age, the consent should be given by the holder of parental responsibility.[176] Such an article was put in place as children are often less aware of the risks and consequences regarding their personal data, as well as their rights relating to data processing and what it entails.[177]

The GDPR also covers rights pertaining to complaints, damages, compensation and liability. Under article 77 of chapter eight of the regulation, every user has the right to file a complaint with a supervisory authority if they deem that the processing of their personal data has been infringed under the GDPR.[178] Therefore, some level of legal protection and action is

[173] GDPR, art. 22.
[174] GDPR, art. 7.
[175] Ibid.
[176] GDPR, art. 8.
[177] GDPR, recital 38.
[178] GDPR, art. 77.

ensured in the event that personal data processing is in violation of the GDPR. Furthermore, article 82 ensures the right to compensation and liability when an individual has suffered material or non-material damage due to a violation of the GDPR.[179] It also holds accountable controllers and processors of data in the event that they have infringed or not complied with the GDPR, with the sole exemption in the case that the damage results from no fault of the controller or processor.[180] By implementing the right to compensation and liability, the data subject can be reassured that they can be compensated if they incur damages and on the other hand, controllers and processors have an incentive to comply with the GDPR in order to not face penalties. Thus, there is a standard of protection for data subjects and the processing of their personal data, with recourse to compensation in the case of non-compliance.

Given lightning speed innovation in the field of artificial intelligence (AI) in recent years, it is imperative to legislate how data is processed and protected as basic rights are involved. In addition to the GDPR as a regulatory framework to ensure the protection and regulation of data privacy and processing, the European Union is equally looking forward to advancing and protecting the fundamental rights of its citizens in the realm of AI. With the advances made in AI, the European Union is amongst the first to acknowledge the need to protect fundamental rights and to develop regulatory apparatus to ensure the protection of those rights.[181] Despite the growing prevalence and opportunities that AI offers as an instrument for better decision-making, the end-use of AI by companies remains contentious.[182] Given the way AI-driven algorithms are trained, they are bound to have built-in biases that can in turn have life-altering experiences and discriminate, such as in the case

[179] GDPR, art. 82.
[180] Ibid.
[181] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 113-114.
[182] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114.

of recruitment and immigration.[183][184] Aware of both the possibilities and dangers that AI evokes, the European Union has taken the initiative to regulate this area by encouraging the development and deployment of AI, while pursuing to mitigate the dangers related to it.[185]

The European Commission thus announced a proposal for a regulation stipulating consistent laws on AI in April 2021.[186] Known as the AI Act, it seeks to "promote ethical, trustworthy, and human-centric AI development, ensuring a high level of protection of fundamental rights,"[187] and is expected to enter into force on the 1st of August 2024.[188] The collection of personal data is sine qua non for training AI and threatens individuals' fundamental right to privacy – an issue that is amplified when AI technologies, for example facial recognition, are used for mass surveillance purposes.[189] Therefore, according to the AI Act, "any AI must be free of bias, respectful of citizens' right to privacy, and otherwise consistent with fundamental rights embedded in the EU Charter and Treaties."[190] This notion is further reinforced under article 10 of the AI Act that addresses data and data governance and highlights the possibility of biases and the negative impact of the latter on fundamental rights of individuals.[191] In order to balance between the development of new AI systems and the protection of fundamental rights involved in using AI, the proposed European regulation proceeds with a risk-based approach to legislation.[192] The Act separates AI applications into

---

[183] Ibid.
[184] Amnesty International, 'New technology and AI used at borders increases inequalities and undermines human rights of migrants,' (21 May 2024).
[185] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114.
[186] Ibid.
[187] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114.
[188] White & Case, 'AI Watch: Global regulatory tracker – European Union,' (16 July 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union#:~:text=After%20final%20approval%20by%20the,provisions%20listed%20in%20Article%20113.
[189] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114.
[190] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114.
[191] Regulation EU 2024/… of the European Parliament and of the Council of … laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act), (hereinafter AI Act).
[192] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114.

four categories based on the risk level they pose – unacceptable, high, limited and minimal risk – and adapts the legal obligations accordingly.[193] The categorisation of 'unacceptable risk' comprises of AI systems that influence human behaviour and subvert their free will by using concealed strategies.[194] In addition, AI systems that have recourse to social scoring by governments as well as the government's use of real-time facial recognition for law enforcement basis are prohibited under the AI Act.[195]

Furthermore, the European Union asserts that AI exists for the convenience of humans and ought to be managed by humans.[196] Several European Union documents further emphasise this human-centric approach to AI, such as the 2019 'The Ethics Guidelines for Trustworthy AI' which laid the foundations for the development of the proposed AI Act.[197] The European Commission equally puts emphasis on "the importance of a human-centric AI that improves the lives of individuals while respecting their rights and preserving their human dignity."[198] It can be said that the European Union's proposed AI legislation is the first of its kind internationally and attests to its dedication to "ethics, trust, fundamental rights, and dignity as key principles guiding AI development."[199] Albeit the adoption of several ethics codes by tech companies to reduce the risks associated with AI, they are often insufficient in safeguarding basic rights of users and their personal data.[200] Therefore, by striving for binding laws on AI, the European Union certifies the supremacy of the rule of law and democracy as its underpinning for its regulatory framework, while enabling its citizens to exert a counterbalancing power to companies and their AI-driven business model.[201] This

[193] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 114-115.
[194] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 115.
[195] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 115.
[196] Ibid.
[197] Ibid.
[198] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 115.
[199] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 115.
[200] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 115.
[201] Ibid.

further reflects the European Union's rights-based and human-centric approach to regulation when it comes to technology and data processing. The following table provides an overview of the proposed AI Act and the GDPR:[202]

	AI ACT	GDPR
Scope	The development, placing on the market or deployment of AI systems and models	Any processing of personal data regardless of the technical devices used (including processing to develop an AI model or system (training data), and processing performed using an AI system)
Targeted actors	Mainly providers and deployers of AI systems (to a lesser extent importers, distributors and authorized representatives)	Data controllers and processors (including providers and deployers subject to the AI Act)
Approach	Risk-based approach to health, safety or fundamental rights, including through product safety and market surveillance with regard to AI systems and models	Principle-based approach, risk assessment and accountability
Main mode of conformity assessment (non-exhaustive)	Internal or third-party conformity assessment, including through a risk management system and against harmonised standards	Accountability principle (internal documentation) and compliance tools (certification, code of conduct)
Main applicable sanctions	Product recall or market withdrawal Administrative fines of up to €35m or 7% of the global annual turnover	Formal notice (which may require the processing operation to be brought into conformity, to be limited temporarily or permanently, including on a periodic penalty payment) Administrative fines of up to €20 million or 4% of global annual turnover

The feasibility of an International Legislative Framework comparable to the EU?

This section aims at analysing the feasibility of an international legislative framework comparable to the European Union in regard to protecting data privacy and regulating the

[202] CNIL, 'Entry into force of the European AI Regulation: the first questions and answers from the CNIL,' (12 July 2024), https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil.

digital economy. It will be divided into two parts: the first part will examine the prospects of the adoption/adaptation of a global regulatory framework similar to the European model, and the second section will analyse the challenges of developing and implementing such a judicial constitution.

Prospects of Adoption/Adaptation

With recent developments in the technological sector globally, there has been increased scrutiny regarding how technology companies process and manage personal data of users worldwide. It has equally brought into question the rights associated with the use of technology, namely the right to privacy – particularly in a data-driven world. Today's technological economy relies on the foundation laid by the United States (US) and its dominant tech companies.[203] Since the dot-com bubble in the 1990s, the US government has expanded opportunities in connection with the technological world by championing for "an open, unregulated, and private sector-led digital economy – both at home and abroad."[204] By championing values that support a free market and free internet domestically, the US equally recognised the importance of exporting those values at an international level.[205] In order to promote such values at a global scale, the US has promoted an ""internet freedom agenda", according to which innovation must be free from government regulation or censorship, or else economic and political progress will be compromised."[206] In practice, such an agenda implies depending on private power to mold the digital economy globally – private power which is mainly consolidated in large US tech firms.[207] This is reflected through the most powerful tech companies worldwide known as the GAFAM, which are solely US-based

[203] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 257.
[204] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 257.
[205] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 257.
[206] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 257.
[207] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 257.

companies. Thus, they often exercise unrestricted power economically, politically and culturally in foreign societies.[208]

Given the accrued power of big tech companies worldwide, governments and individuals have become more wary of companies' data processing practices.[209] Governments have become more proactive in countering the unrestrained power that technology companies yield and protecting their citizens' fundamental rights.[210][211] Major scandals in relation to data – such as the Snowden revelations and the Cambridge Analytica scandal – have equally raised awareness of the importance of privacy in the digital economy and how the latter can be regulated. The adoption of the GDPR has drawn further attention to individuals' rights and obligations in relation to personal data processing.[212] This further showcases the spearheading of the European Union in crafting regulatory frameworks governing the digital space. Furthermore, the GDPR has been espoused as a global standard for data privacy by several American giants, such as Google, Microsoft, Apple and Meta, and is regarded as the "world's most extensive legal regime for data protection."[213][214] Anu Bradford argues that the reason for the compliance of such powerful US companies to the European Union's regulation resides in the 'Brussels Effect'.[215] The latter can be understood as a way to describe the European Union's "unilateral power to regulate the global marketplace."[216][217] Although at

[208] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 257.
[209] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 258.
[210] Kriangsak Kittichaisaree, 'Public International Law of Cyberspace,' in Pompeu Casanovas & Giovanni Sartor (eds), *Law, Governance and Technology Series* (Springer, 2017), 1-376, 47.
[211] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' in *LSE IDEAS*, (May 2018), 1-12, 3.
[212] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' *Information & Communications Technology Law*, (Routledge, 2020), 22-44, 22.
[213] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 31.
[214] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 324.
[215] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 324.
[216] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 324.
[217] Anu Bradford, 'The Brussels Effect: How the European Union Rules the World,' (Oxford University Press, 2020), 1-404, xiv.

first the Brussels Effect arose from the internal aim of striving for European integration by means of regulation, it has now gained an external proportion confirming the European Union as the international regulatory hegemon.[218]

Due to the Brussels Effect, the European Union has become a leading actor in the realm of regulation – particularly regarding data protection – and further highlights the unique ability of the European Union and the potential for the adoption of international regulatory framework based on its model. The European Union legislative framework regarding data protection has remarkably impacted other countries' legal approach, such as Japan, Mauritius, or Georgia.[219] Dubbed as the 'gold' standard, the European Union's Regulation has become "a reference point for works carried out worldwide on the implementation of legal instruments in the field of data protection."[220] For example, Mauritius has amended its Data Protection Act in order to comply and be in line with the European and international standards and best practices.[221] In addition, Mauritius adopted the National ICT Policy to accommodate for the country to be potentially acknowledged by the European Union as a third country with a satisfactory level of protection.[222] To date, almost 150 countries have adopted national privacy legislation, with the majority being similar to the European Union's data protection apparatus.[223] Therefore, the European regulatory framework is globally recognised to be a standard that should be upheld and emulated; the

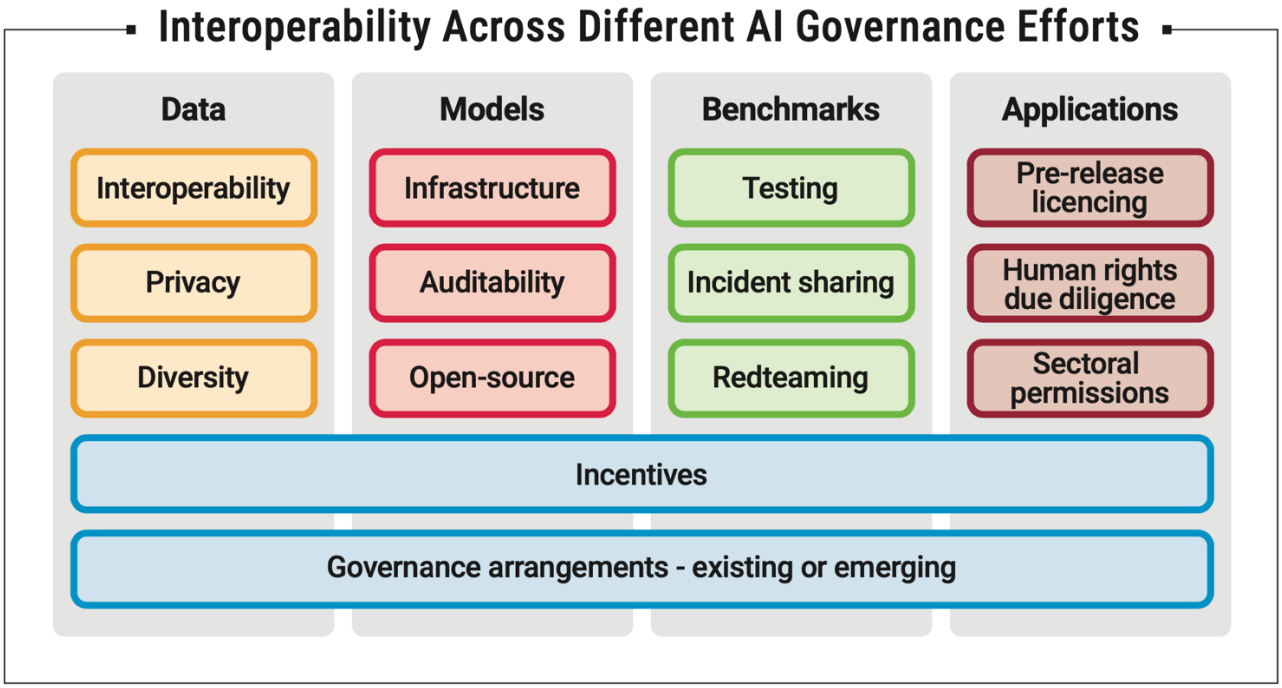
[218] Anu Bradford, 'The Brussels Effect: How the European Union Rules the World,' (2020), 7.
[219] Urszula Góral, 'The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond,' in *Acta Juris Stetinensis*, (2021), 101-113, 102.
[220] Urszula Góral, 'The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond,' (2021), 102.
[221] Alex B. Makulilo, 'The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius,' in *The International Journal of Human Rights*, (Routledge, 2021), 117-146, 119.
[222] Alex B. Makulilo, 'The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius,' (2021), 119.
[223] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 325.

enactment of the GDPR is equally an example of how data protection can successfully be governed at a supranational level.[224]

Moreover, the proposal of the European AI Act denotes the importance of regulating the digital economy as evolving technologies emerge. Given the recent developments in AI, there has been mounting pressure to monitor and regulate its use as well as the protection of data. At a national level, the US has drafted a Blueprint for an AI Bill of Rights that aims at supporting "the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems."[225] It is a non-binding document and does not embody US government policy.[226] Furthermore, the United Nations has produced a report addressing the several aspects that are linked to AI: namely the lack of global governance, the risks and challenges, and the need for international governance.[227] Within its report, the Advisory Body on AI enumerates the risks associated with AI under six categories – individuals, groups, society, economy, (eco)systems, and values and norms.[228] Each category reflect the risks that the European Union legislative framework identified and aims to protect in regards to AI. The report equally underlines the lack of governance relating to AI, as well as how existing frameworks are fragmented and regional.[229] In addition, it emphasises the need for self-regulation, domestic regulation, and international regulation to prevent and alleviate the risks that AI brings forward.[230] The report equally highlights how the absence of common principles and guidelines across domestic and

[224] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 31.
[225] United Nations Advisory Body on Artificial Intelligence, 'Interim Report: Governing AI for Humanity,' (December 2023), 1-28, 2.
[226] Ibid.
[227] United Nations Advisory Body on Artificial Intelligence, 'Interim Report: Governing AI for Humanity,' (2023), 8.
[228] United Nations Advisory Body on Artificial Intelligence, 'Interim Report: Governing AI for Humanity,' (2023), 9-10.
[229] United Nations Advisory Body on Artificial Intelligence, 'Interim Report: Governing AI for Humanity,' (2023), 10.
[230] Ibid.

multinational risk management frameworks have convoluted the governance aspect of AI.[231] The Advisory Body equally proposes a simplified schema for contemplating the emanating AI landscape in the following graph, with the aim of developing it further in its next phase of work:[232]



To this day, the majority of large-scale wrongdoing in regard to personal data protection has been perpetrated by corporations and states alike.[233] Due to increased cyberattacks from states against other states, there has equally been growing calls from technology companies to regulate cyberspace.[234] The escalation of countries' operations is eliciting cogitation about the militarisation of digital space.[235] The latter is a source of concern for policy and decision makers, as well as important actors within the private

[231] United Nations Advisory Body on Artificial Intelligence, 'Interim Report: Governing AI for Humanity,' (2023), 12.
[232] Ibid.
[233] Bartosz Ziemblicki, 'Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,' (2023), 598.
[234] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' in *Journal of Law & Cyber Warfare*, (2018), 3-55, 5.
[235] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 5.

sector.[236] In 2017, at the RSA Conference in San Francisco, Brad Smith, the president of Microsoft, urges the need for a Digital Geneva Convention that would overlook the governance of technology and the protection of citizens in the digital realm.[237][238][239] He draws a parallel between the Fourth Geneva Convention and its protection of civilians during times of war and the need for a Digital Geneva Convention to protect individuals from nation-state attacks.[240] After highlighting the issue of countries' cyberattacks, Smith proposed three responses to such actions. First, he contends for greater prudence in that firms and individuals need to do more individually and collectively regarding cybersecurity.[241] Then, he puts forward reasons for a new international treaty.[242] In particular, he underscores how governments worldwide "came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace."[243] Lastly, Smith suggest that the international technology sector ought to operate as a "neutral Digital Switzerland."[244][245]

So far, neither states or companies have determined their roles in the digital space.[246] The appeal of Microsoft for a Digital Geneva Convention further embodies the company's

---

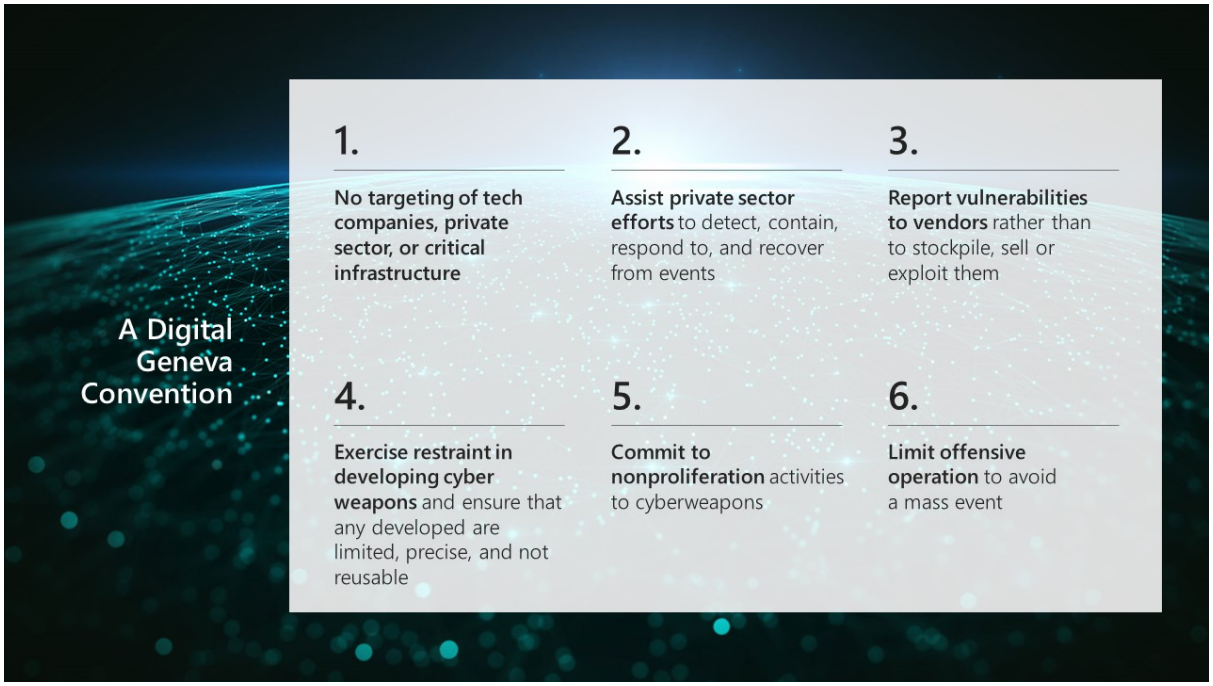
[236] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 7.
[237] Brad Smith, 'The need for a Digital Geneva Convention,' (14 February 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.
[238] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' (2018), 6-7.
[239] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 7.
[240] Brad Smith, 'The need for a Digital Geneva Convention,' (2017), n.a.
[241] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' (2018), 6.
[242] Ibid.
[243] Brad Smith, 'The need for a Digital Geneva Convention,' (2017), n.a.
[244] Ibid.
[245] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' (2018), 7.
[246] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 6.

commitment to regulate cyberspace. Through an internal memorandum communicated by Bill Gates in 2002, the company has asserted its priority regarding cybersecurity and has since situated itself as a pioneering organisation in conducting cybersecurity norms, institutions and values whose commitment encompasses the industry, and decision and policy makers.[247] Given that Microsoft is practically present in every country worldwide, there is an economic incentive to have established international cooperation among states to adopt corresponding laws and norms to preserve Microsoft's competitive advantage in the market.[248] By putting forward the need for a Digital Geneva Convention, Microsoft takes the lead among tech companies to regulate cyberspace and maintain its competitive edge.

Moreover, the Digital Geneva Convention proposed by Microsoft has three noteworthy characteristics. Firstly, it reconceptualises the conventional multi-stakeholder governance model of digital space splitting each stakeholder into selected action areas.[249] It can be conceived as states being signatories to the Convention, while the private sector will abide to their respective industry principles, and an NGO would be responsible for inquiring into cyber attacks.[250] Secondly, the Digital Geneva Convention has recourse to humanitarian lexicon akin to that used by civil society organisations.[251] The Convention depicts cyber-attacks as an international humanitarian issue that can solely be tackled with the involvement of tech firms.[252] In addition, there is allusion made regarding the role of tech companies being similar to the Red Cross as 'first responders' during cyber-attacks: "As the Fourth Geneva Convention relies on the Red Cross to help protect civilians in wartime, protection against

[247] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 7.
[248] Ibid.
[249] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 8.
[250] Ibid.
[251] Ibid.
[252] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 9.

nation-state cyberattacks requires the active assistance of the tech sector."[253][254] Lastly, the proposal for such a Convention is supported by senior leadership in the technology sector.[255] The following infographic summarises the proposed Digital Geneva Convention by Brad Smith:[256]



Furthermore, states are not only fighting horizontal battles with each other in the digital economy, but they are equally battling vertical conflict against technology firms who are active in their markets – private companies who command tremendous private power that is comparable to emerging empires.[257] These vertical battles are particularly challenging for two main reasons: firstly, technology companies are both targets as well as instruments for states.[258] In other words, these companies are perceived as allies and enemies alike to

[253] Brad Smith, 'The need for a Digital Geneva Convention,' (2017), n.a.
[254] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 9.
[255] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' (2018), 9.
[256] Brad Smith, 'The need for a Digital Geneva Convention,' (2017), n.a.
[257] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 13.
[258] Ibid.

governments, enabling them to fulfil some policy goals, while impeding others.[259] Thus, the difficulty for states will be to find the right balance between inflicting regulatory constraints and the ability of these tech companies to exercise their role as powerful tools in battles whereby governments rely on their power.[260] Secondly, the nature of the global marketplace renders these vertical battles more difficult, as tech companies have various suzerains.[261] Therefore, due to diverging demands from different states, it is virtually impossible to comply to all those demands simultaneously.[262] US tech companies operating in China come across a challenging balancing act. As an example, Apple has been a vigorous proponent of data privacy and civil rights in the US and the European Union.[263] However, numerous concessions have been made in exchange for being able to operate in China.[264] This goes on to illustrate how vertical battles repeatedly conflict, abandoning companies with the complex – and oftentimes impossible – duty of selecting which governments' demands to adhere to. By having an international legislative framework, such conflicts could be constrained and regulated without impeding on the interests at play.

Given that the European Union benefits from the Brussels Effect, adopting an international legal framework akin to the European Union's GDPR could enhance data privacy and protection on a global level. What makes the Brussels Effect unique to the European Union is that "the jurisdiction must have regulatory capacity as well as the political will to generate stringent rules in order to be a unilateral global regulator."[265] At present times, only the European Union meets these additional requirements – aside from market size – across diverse policy areas.[266] In addition, the Brussels Effect solely happens when there is

[259] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 14.
[260] Ibid.
[261] Ibid.
[262] Ibid.
[263] Ibid.
[264] Ibid.
[265] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 327.
[266] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 327.

regulation of inelastic targets, such as consumer markets.[267] This reinforces the fact that consumers cannot escape to less regulated territories, which would compromise the European Union's legislative power.[268] Moreover, European standards become international only when companies deem that the benefits of abiding to a single legislative norm surpass the benefits of cashing more lax tax standards in other markets.[269] Given that the European Union has emerged as an essential market for various Big Tech companies – such as Apple, Google and Meta – there is an economic incentive for the latter to adhere to the European standard of data privacy and regulation. Therefore, developing and enacting an international regulatory instrument based upon the European Union approach could be the way forward in legislating the digital economy and the rights associated with the latter.

Rojszczak argues that the praxis of national regulation to the digital space is unsuccessful based on experience.[270] Therefore, there is a necessity to have as prerequisite the universality of the enacted data protection approach to ensure its effectiveness.[271] He believes that there is the potential to craft a "new international agreement that could be the source of effective mechanisms of privacy protection in cyberspace, even if only partially accepted by individual states."[272] The proposal is outlined throughout the following points:[273]

> (1) the formal basis should be an international agreement of a legally binding nature;
>
> (2) the subject matter of this treaty should be the establishment of an international organization competent to define requirements and supervise their observance in the field of data processing in cyberspace;

---

[267] Ibid.
[268] Ibid.
[269] Ibid.
[270] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 39.
[271] Ibid.
[272] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 39.
[273] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 39-40.

(3) the way to achieve this goal should be granting the organization the competencies needed to enact its own standards of conduct and legal norms in relation to cyber- space, of a regulatory and not strictly protective nature;

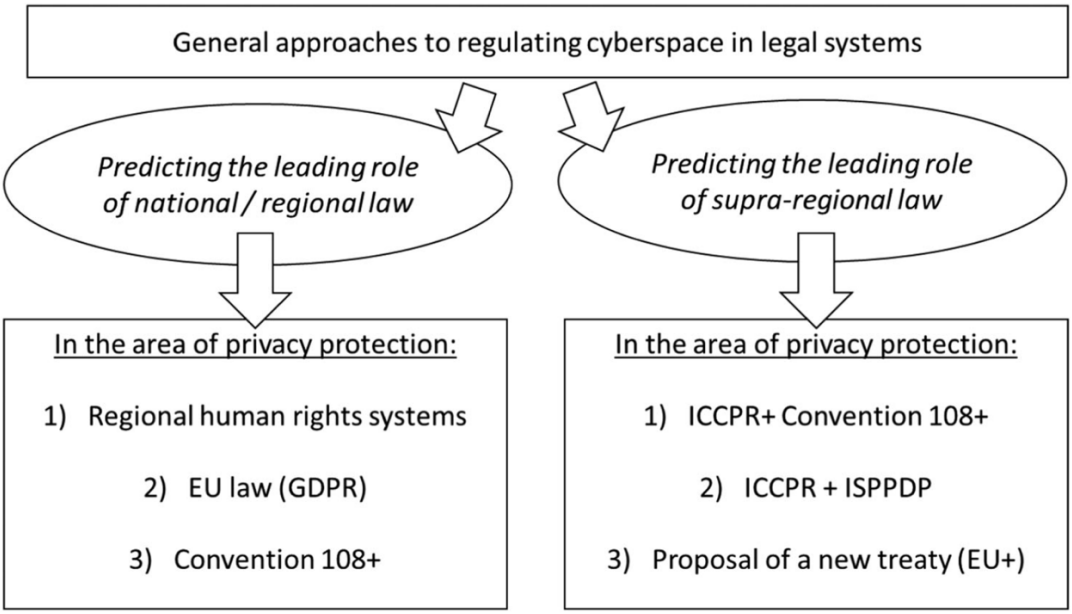
(4) the law enacted by the organization should be directly effective in the legal systems of the states party to the convention;

(5) within the framework of the treaty, an authority competent to develop guidelines and recommendations should be established – similar to WP29 (an element of soft-law and market self-regulation),

(6) the treaty should appoint or indicate a judicial authority; however, submission to the dispute settlement procedure should not depend on the parties' discretion, and judgments passed should have an erga omnes effect.

The author argues that this proposal differs from the European legislation as its only focal point is the implementation of a committed function, without a political or economic relation with the states of a certain part of the world.[274] For convenience, the proposal has been defined as 'EU+'.[275] The adoption of the EU+ proposal would result in the conception of a reliable data processing domain, operating in countries that acceded the treaty.[276] Thus, the EU+ proposal showcases how the European approach to regulation in relation to the digital economy can serve as a foundation to build and develop an international organisation capable of enforcing binding data protection principles in the digital realm.[277] In addition, Rojszczak provides an overview of existing and potential regional and global approaches in regards to governing the digital arena:[278]

[274] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 40.
[275] Ibid.
[276] Ibid.
[277] Ibid.
[278] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 36.



The prospects of adopting/adapting the European Union's regulatory framework regarding data protection and privacy at an international level are optimistic. The enactment of the European GDPR has had a domino effect worldwide; states across the globe are adopting or adapting the European framework on data protection to their national legislation. As previously mentioned, even tech multinationals – such as Microsoft, Apple, and Google – are in favour of data protection regulation and abide by the European standard. The occurrence of legal duplication is flagrant in the realm of data privacy.[279] It is prompted by various reasons, inclusive of the European Union's innate capability to chart legislation that are intended to function in numerous distinct jurisdictions.[280] Above all, what renders the European approach so distinctive is that it represents a modus vivendi among twenty-seven countries.[281] Therefore, the de jure Brussels Effect depicts the feasibility of adopting European standards of data protection at a global scale through an international treaty. Moreover, the de jure Brussels Effect expands on the de facto Brussels Effect: once

[279] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 332.
[280] Ibid.
[281] Ibid.

multinational corporations have modified their global conduct to adhere to European laws, they have an impetus to lobby for European-style legislation in their domestic jurisdictions.[282] This further demonstrates the willingness from both the public and private sector to regulate data protection to protect citizens' rights. Both states and multinational corporations – as well as individuals – benefit from adopting an international legislative approach to data protection. From an international legal perspective, the GDPR could act as a foundation for the development of an international treaty regulating data protection.

Challenges of Adopting an International Treaty

Despite the promise of an international regulatory framework governing data privacy and protection, there are equally challenges that arise with adopting such a global approach. Although the European model of regulation is often emulated at a national and global level, it equally faces challenges when envisaged at an international magnitude. In her book 'Digital Empire: The Global Battle to Regulate Technology', Anu Bradford analyses the three major digital governance models to this day; the European model – which has been analysed in previous sections of this paper – the US model and the Chinese model of governance. The US model of digital governance has conventionally conformed to a market-driven regulatory framework, which has laid the foundation for the digital economy as we know it today.[283] It revolves around "protecting free speech, a free internet, and incentives to innovate."[284] Such a model is influenced by distinguishable techno-optimism, incessant quest for innovation, and the rigorous belief in markets compared to government regulations.[285] In addition, the US governance model believes in tech firms' capability to self-regulate and prefers a limited role

[282] Ibid.
[283] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 7.
[284] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 33.
[285] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 33.

for the government.[286][287] This laissez-faire market rationale is deeply entrenched in the current US legal approach, which comprises of "weakly enforced antitrust laws, an absence of a federal data privacy law, and permissive content moderation rules that shield tech companies from liability, leaving them free to decide whether or not to remove certain harmful content from their platforms."[288] Moreover, in comparison to the European model, the US regulatory framework is harm-based rather than-rights-base, implying that there is no "all-encompassing fundamental right or law that protects privacy and personal data, but rather a system of diverse legal and regulatory acts that cover specific privacy interests and situations that cause cognizable harm."[289] Within the US model, there is the belief that having a non-interventionist approach best contributes to innovation and economic growth.[290] Thus, the US market-driven model of digital governance espouses a more liberal approach to the digital realm, whereby the private sector has greater control and power than the government.

On the other hand, the Chinese model of digital governance finds itself at the opposite side of the spectrum. In comparison to the US model, the Chinese approach relies on a state-driven vision for the digital space.[291] The Chinese government aims to expand the country's technological supremacy while preserving social consonance over its citizens' communications.[292] China is intent on leveraging technology to stimulate its economic growth and development and is equally committed to becoming a global technological superpower.[293] On top of this economic goal, the Chinese government is engaged on

---

[286] Ibid.
[287] Matt Buckley, 'Federal Data Privacy Regulation: Do Not Expect an American GDPR,' in *DePaul Business & Commercial Law Journal*, (2023),147-184, 178.
[288] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 33.
[289] Karlijn van den Heuvel & Joris van Hoboken, 'The justiciability of data privacy issues in Europe and the US,' in in Gloria González, Rosamunde Van Brakel and Paul de Hert (eds), *Research Handbook on Privacy and Data Protection Law* (15 March 2022), 73-108, 81.
[290] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 38.
[291] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 8.
[292] Ibid.
[293] Ibid.

consolidating the political control of the Chinese Communist Party (CCP) by utilising the internet as an apparatus for control, surveillance and propaganda.[294] The use of the digital realm for such ends under the Chinese state-driven model has come under growing criticism in democracies.[295] Therefore, China's custom of using data as a means for social control denotes a distinct departure from the shared European and American perspective where the internet is perceived as essential in enhancing individual liberty and promoting freedom in society.[296] The rise of China as a leading technological power has led to the so-called US-China tech war whereby the US and China are competing for technological hegemony.[297][298] Thus, on one side we have a party advocating for techno-globalism (US), while on the other, techno-nationalism is championed (China).[299] The following table showcases the main principles behind both techno-globalism and techno-nationalism:[300]

TABLE 2.1 Techno-globalism and techno-nationalism in comparison.[20]

Aspect	*Techno-globalism*	*Techno-nationalism*
Typical technology	Market-oriented technology, textile and consumer goods	Defence technology
Promoter	Private sector	U.S. Department of Defense, governments
Interface	Technology transfer possible	Secrecy and security
Difference between technology and living standards	Shortens – to make more technologies available in everyday life	Widens – technology is exclusive and only available in selected domains
Government expenditures	Small to none	Huge
Mode of production	Asian mode of production[21]	Military-industrial complex
Character of intensiveness	Starting from labour intensive	High-technology intensive

[294] Ibid.
[295] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 9.
[296] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 9.
[297] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 72.
[298] Pak Nung Wong, 'Techno-geopolitics: US-China Tech War and the Practice of Digital Statecraft,' in Harsh V. Pant, Frank O'Donnell and Avinash Paliwal (eds), *International Geopolitics in the Age of Disruption*, (Routledge, 2022), 1-123, 22.
[299] Pak Nung Wong, 'Techno-geopolitics: US-China Tech War and the Practice of Digital Statecraft,' (2022), 23.
[300] Ibid.

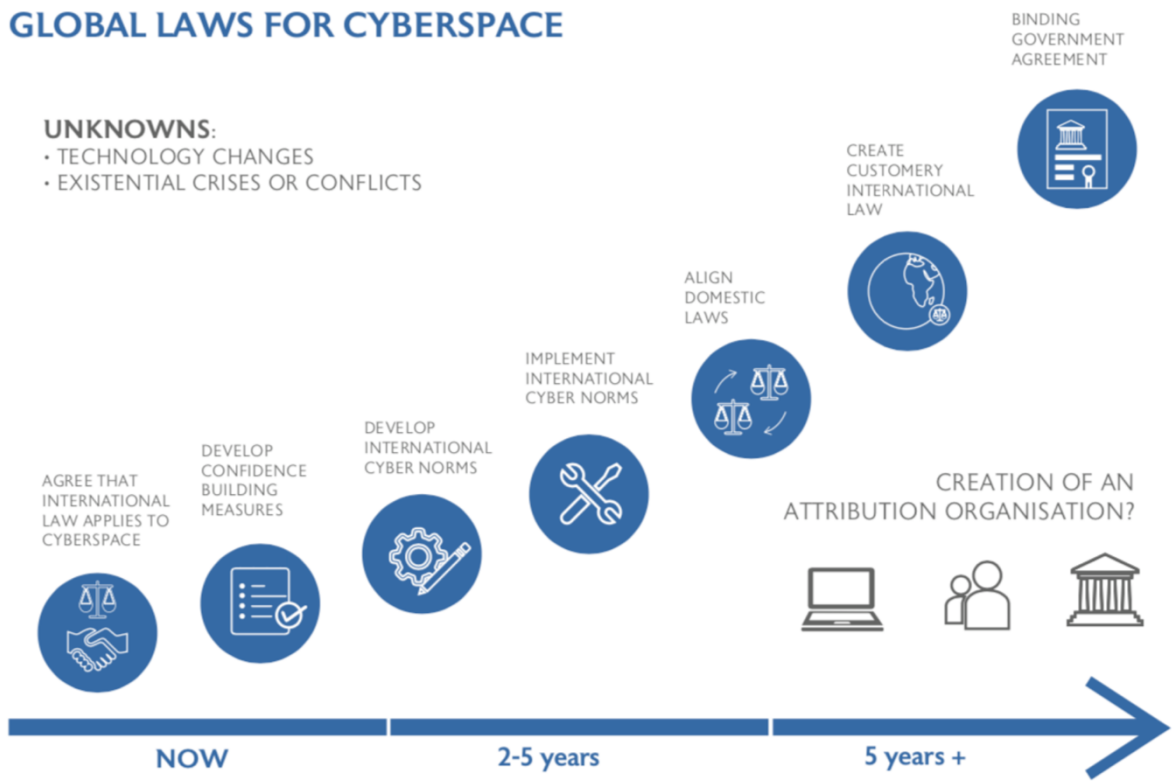
Furthermore, having competing ideologies as to how data privacy should be regulated and protected hinders the opportunity of adopting a global framework to data protection. This in turn leads to states not agreeing on the scope of protection and regulation needed to ensure a harmonisation of standards worldwide. With the three main digital governance model differing from each other, implementing a digital international regulatory framework will be challenging. Even though the European model is rights-driven, some argue that such a legislative framework is over-protective and hindering companies' incentives to innovate, and thereby diminishing technological and economic development.[301] It is imperative to underline that there are few successful tech multinationals that have emerged in Europe, compared to its American and Chinese counterparts. It has been frequently argued that that is the reason for the European Union's stringent regulations.[302] Given that the US and China are often perceived as the leading technological powers, the European Union is commonly disregarded as a bystander caught in between the two powers in the battle for digital hegemony.[303] Despite its position, Europe has been able to establish itself in this contest as the "most powerful regulator of the digital economy, giving it unique leverage to shift the digital economy toward its values."[304] This horizontal battle among states highlights the complexity of regulating the digital space, as well as the differing interests and goals at hand. The lack of a unified and consistent framework incapacitates the prospect of the international data protection standards in warranting consistent data privacy protection.[305]

Moreover, despite the recurrent use of international treaties as a way to regulate various domains, their effectiveness has often been up for debate. Although there exists over 250,000 international treaties aiming to enhance global cooperation, it has been shown that

[301] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 10.
[302] Ibid.
[303] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 11.
[304] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 12.
[305] Kinfe Yilma, 'The 'Privacy Problem' in the Digital Age,' (2023), 111.

the vast majority of them are ineffective and fail at producing their intended effect.[306] In particular, treaties governing human rights and security policy domains only seem to improve in effectiveness with the inclusion of enforcement mechanisms.[307] Calls for international treaties are often made by the array of stakeholders involved; nonetheless, most of them do not take into consideration the "costs of drafting, signing, ratifying, and enforcing them."[308] Therefore, the ineffectiveness of international treaties as a whole challenges the conventional idea that they are the apex mechanism for regulation amongst states and highly effective in achieving desired results. In addition, the adopted drafts of international treaties are generally a watered-down version of what is initially intended. As the drafting of treaties is time-consuming and involves a multiplicity of stakeholder with diverging interests, oftentimes the final draft features regulations that include compromises made amongst states depending on their interests. Furthermore, given that the process of treaty drafting and adoption is lengthy, it poses as a challenge in the realm of digital regulation. With lightning speed advances in the technological sector, it will be challenging to have an international treaty that regulates data protection and privacy given the treaty drafting process. By the time that the global legislative framework is signed by all actors, the digital space would have immensely changed. More so, the adopted regulations might become outdated or misaligned with the current state of technology once the treaty enters into force. The following figure shows the process of creating an international data protection legal framework and depicts the lengthiness of such a process:[309]

[306] Steven J. Hoffman et al., 'International treaties have mostly failed to produce their intended effect,' in Douglas Massey (ed), (PNAS, 17 May 2022), 1-9, 5.
[307] Ibid.
[308] Steven J. Hoffman et al., 'International treaties have mostly failed to produce their intended effect,' (2022), 1.
[309] World Economic Forum, 'Why we urgently need a Digital Geneva Convention,' (29 December 2017), https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention/.



Although the de jure aspect of an international framework might seem appealing, oftentimes the de facto aspect is more difficult to warrant – particularly when it comes to enforcement. A notable example is the failure of the European Union's translation of its rigorous digital laws into successful implementation.[310] Despite having a certain degree of impact, the European model of digital governance has equally had shortcomings in terms of enforcement.[311] The lack of enforcement of the GDPR has frequently left users' data at risk of exploitation.[312] The responsible body for the implementation – the Irish Data Protection Commission (DPC) – has been submerged by the task of enforcing the GDPR against tech multinationals, only submitting a few number of cases under the Regulation.[313] In addition, despite the adoption of the GDPR by companies, the deterrent effect of the latter may wither over the years if no effective implementation is witnessed.[314] A recurrent enforcement

[310] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 139.
[311] Ibid.
[312] Ibid.
[313] Ibid.
[314] Ibid.

apparatus is the use of fines against companies that violate the GDPR; however, those fines do not compare to the revenue of large tech companies. For example, Meta's fine by the FTC seems meagre in comparison to its revenue: "The day this landmark fine was imposed, Meta's stock rose by 1.8 percent, adding $10 billion to its market value."[315] This demonstrates that Big Tech companies may deal with fines as the cost of doing business, and equally as something they can effortlessly indemnify by other benefits – as long as they are not compelled to radically restructure their business models that depend on the exploitation of user data.[316] In order to have an effective international data protection legislative framework, it is imperative to equally have the support and commitment of large technology companies in bettering the digital space. Yet, the approach to enforcement and the concentration of power in tech multinationals paint a grim portrait of the effectiveness of an international regulatory framework.

Conclusion

The ever-progressing technological sector has brought around numerous questions in recent years, namely the issue of privacy in such a data-driven world. With the growing number of data breaches and scandals, there has been increased scrutiny on how multinational technology companies manage and use personal data. Additionally, in recent years, States have had recourse to the Internet as a means to conduct cyber-attacks against other states. Given the concentration of power with states and Big Tech companies in regard to data privacy and regulation, citizens have become preoccupied with their rights relating to their personal data – namely their right to privacy and data protection. There have been growing calls to regulate the digital space, particularly when it comes to data privacy and the protection of personal data. The president of Microsoft, Brad Smith, has urged the need for a

[315] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 140.
[316] Ibid.

Digital Geneva Convention that would regulate cyber space and ensure citizens' fundamental rights and protection in the digital space. At the regional level, the European Union has established itself as the 'golden' standard in legislating data protection and protecting the basic rights of its citizens. The enactment of the GDPR has been perceived as setting a new standard in data protection legislation and has been adapted by several countries in their national jurisdictions. Numerous countries across Africa, Asia, and Latin America have emulated several characteristics of the GDPR, "even while retaining some distinct national features that depart from the text or spirit of the GDPR."[317]

The European model of digital regulation emphasises the protection of the fundamental rights of its citizens first and foremost, while maintaining economic growth and development. What renders it unique is that it applies to twenty-seven countries and enables the harmonisation of laws across the region. By doing so, there is a common set of standards and principles regulating data privacy protection. Adopting an international legislative approach grounded in the European model could be the way forward in regulating the digital space. There are incentives in enacting an international legal framework namely to provide a uniform level of data protection at a global scale and to constrain the almost limitless power that technology multinationals wield. Horizontal and vertical battles can be stifled by adopting a global regulatory approach that would consider the respective interests of all parties involved – including those of individuals. Furthermore, with the advent of artificial intelligence, there has been even more calls to regulate cyberspace from both governments and leading figures in the technological field. Moreover, the Brussels Effect of the European Union showcases how European standards are emulated at national and international levels.

[317] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 335.

This further depicts the feasibility of adopting an international regulatory framework based on the European GDPR.

On top of the entry into force of the GDPR, the proposal of the AI Act further depicts the commitment of the European in regulating the digital world and maintains its global status of a leading regulatory power. In addition, the European model of digital governance differs from the US market-driven model and the Chinese state-driven model. The former embraces a more laxist approach to regulation and allows the accumulation of power within the private sector. On the other hand, the Chinese governance model promotes authoritarian control of cyberspace – leading to state surveillance to control citizens – with stringent regulations. The European model thereby provides a balanced compromise to both extremes: promoting regulations and the protection of fundamental rights, while fostering economic and technological growth. Therefore, the European digital governance approach has greater prospects of being emulated at an international level. In addition, in today's time, there is global widespread consensus that individuals should exercise the same rights online and offline.[318] The European model of governance seeks to promote and enforce the protection of citizens' fundamental rights both online and offline.

Despite the prospect of enacting a global regulatory framework, there are equally challenges that arise in adopting such a legislative framework. First and foremost, it requires the cooperation and collaboration of states as well as the private sector – the two main stakeholders in this issue. Given diverging interests and governance approaches, governments might be unwilling and recalcitrant in adopting a binding international treaty that could limit their power. States that have recourse to cyberspace in order to conduct surveillance operations – such as Russia, China and the United States – have to be persuaded that they

[318] Urszula Góral, 'The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond,' (2021), 108.

benefit more from adopting an international treaty that will considerably limit their cyber operations, as opposed to having no global regulatory framework.[319] Additionally, it should be noted that treaties regulating global areas have been founded on some form of consensus emanating from established custom.[320] However, there is no such custom in the digital domain.[321][322][323] Therefore, the absence of a global consensus considerably hinders the development of an international legislative framework regulating the digital domain. In addition, the process of drafting and enacting an international treaty is time-consuming and costly, further hindering the possibility of such a legislative framework.

Moreover, international law is considered to be an ever-evolving set of legislative principles that are commonly adhered to by states in their relations with one another that bestow rights and impose obligations in both peace and wartime.[324] Given differing views on what should comprise fundamental rights – particularly the right to privacy – and diverging interests, it is challenging to have states to agree and adopt to set principles for all. When considering horizontal and vertical battles – especially the US-China tech war – it is difficult to envision the feasibility of an international digital regulatory framework. The public commentary often predicts binary outcomes, notably choosing between the United States and China: either "a global internet or a fragmented 'splinternet'."[325] This binary way of framing the question at hand blinds us to the existing complex dynamics. A deeper analysis of the interdependencies across key conflicts presupposes that the "internet will not be global, nor

[319] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' (2018), 40-41.
[320] Marcin Rojszczak, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' (2017), 37.
[321] Ibid.
[322] Urszula Góral, 'The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond,' (2021), 108.
[323] Stephan Koloba, 'Is There Really a Need for a New 'Digital Geneva Convention'?" in *Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict*, (2019), 37-52, 51.
[324] David Wallace & Mark Visger, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' (2018), 15.
[325] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 16.

will we witness full decoupling; China will not triumph over the US, nor will the US triumph over China; governments will not declare a complete victory over tech companies, but neither will tech companies detach themselves from government regulation."[326] Rather, the digital domain will likely be represented by what Mark Leonard calls ""the age of unpeace": a geopolitical order where states are too interconnected to fight an all-out war but too discordant to live in genuine peace."[327]

This major research aimed at showcasing the prospects of adopting an international legal framework that emulates the European digital governance model. Despite the optimistic prospects of developing such a global approach, challenges and obstacles remain that hinder the implementation of a supranational legislative framework. Regardless of the increasing calls from both the private and public sector in regulating the digital realm, diverging interests, growing tensions (horizontal and vertical battles) and contrasting governance models render the adoption of an international treaty legislating cyberspace even more challenging. We might witness the development of a global legal framework if all parties involved deem the benefits of having such a framework to outweigh the costs. Ultimately, the drafting and implementation of an international treaty that will regulate digital space and protect the fundamental rights of individuals largely depends on the willingness of states and tech multinationals to put aside their greed and differences in the best interests of their own citizens and their basic rights.

[326] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 16.
[327] Anu Bradford, 'Digital Empires: The Global Battle to Regulate Technology,' (2023), 16.

Bibliography

30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Children's Privacy Online,' (Strasbourg, 17 October 2008).

Amnesty International, 'New technology and AI used at borders increases inequalities and undermines human rights of migrants,' (21 May 2024). https://www.amnesty.org/en/latest/news/2024/05/global-new-technology-and-ai-used-at-borders-increases-inequalities-and-undermines-human-rights-of-migrants/

Amnesty International, 'The Great Hack: Cambridge Analytica is just the tip of the iceberg,' (24 July 2019). https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/

Aridor, Guy et al., 'The effect of privacy regulation on the data industry: empirical evidence from the GDPR,' 695-730, in *The RAND Journal of Economics* (Wiley 2023).

BBC, 'Edward Snowden: Leaks that exposed the US spy programme,' (17 January 2014). https://www.bbc.com/news/world-us-canada-23123964

BBC, 'Terms and Conditions Explained: What are they all about?' (17 February 2017). https://www.bbc.co.uk/newsround/38992576

Bradford, Anu, 'Digital Empires: The Global Battle to Regulate Technology,' (Oxford University Press, 2023), 1-599.

Bradford, Anu, 'The Brussels Effect: How the European Union Rules the World,' (Oxford University Press, 2020), 1-404.

Buckley, Matt, 'Federal Data Privacy Regulation: Do Not Expect an American GDPR,' in *DePaul Business & Commercial Law Journal*, (2023),147-184.

Çinar, Naim and Ateş, Sezgin, 'Data Privacy in Digital Advertising: Towards a Post-Third-Party Cookie Era,' 55-77, in Michael Filimowicz (eds), *Privacy: Algorithms and Society* (Routledge 2022).

CNIL, 'Entry into force of the European AI Regulation: the first questions and answers from the CNIL,' (12 July 2024), https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil.

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, (28 January 1981).

European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953), as amended by Protocols Nos. 11, 14 and 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, art. 8.

Góral, Urszula, 'The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond,' in *Acta Juris Stetinensis*, (2021), 101-113,

Goswami, Swish, 'The Rising Concern Around Consumer Data and Privacy,' in Forbes (14 December 2020). https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=5ded3eee487e

Hoffman, Steven J. et al., 'International treaties have mostly failed to produce their intended effect,' in Douglas Massey (ed), (PNAS, 17 May 2022), 1-9.

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

Kavenna, Joanna, 'Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy',' in *The Guardian* (4 October 2019). https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

Kittichaisaree, Kriangsak, 'Public International Law of Cyberspace,' in Pompeu Casanovas & Giovanni Sartor (eds), *Law, Governance and Technology Series* (Springer, 2017), 1-376.

Koloba, Stephan, 'Is There Really a Need for a New 'Digital Geneva Convention'?" in *Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict*, (2019), 37-52.

Llorente, Raquel Vázquez, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity,' in *LSE IDEAS*, (May 2018), 1-12.

Makulilo, Alex B., 'The long arm of GDPR in Africa: reflection on data privacy law reform and practice in Mauritius,' in *The International Journal of Human Rights*, (Routledge, 2021), 117-146.

McCallum, Shiona, 'Meta settles Cambridge Analytica scandal case for $725m,' in *BBC* (23 December 2022). https://www.bbc.com/news/technology-64075067

Menand, Louis, ‘Why do we care so much about privacy?’ in The New Yorker (11 June 2018). https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy

Mucelin, Guilherme, ‘Internet of Things and Consumers’ Privacy in a Brazilian Perspective: Digital Vulnerability and Dialogue of Sources,’ 287-302 in Georg Borges and Christoph Sorges, *Law and Technology in a Digital Society* (Springer 2022).

Nougrères, Ana Brian, Special Rapporteur on the right to privacy, ‘Report: Right to privacy: Note by the Secretary-General,’ (20 July 2022) UN Doc A/77/196.

Privacy Commissioner of Canada, ‘From state surveillance to surveillance capitalism: The evolution of privacy and the case for law reform,’ (16 June 2021). https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210616/

Privacy Commissioner of Canada, ‘Privacy as a fundamental right in the digital age,’ (24 February 2023). https://www.priv.gc.ca/en/opc-news/speeches/2023/sp-d_20230224/

Rahnama, Hossein and Pentland, Alex, ‘The New Rules of Data Privacy,’ in Harvard Business Review (25 February 2022). https://hbr.org/2022/02/the-new-rules-of-data-privacy

Regan, Priscilla M., ‘Social values and privacy law and policy,’ 161-175, in Gloria González, Rosamunde Van Brakel and Paul de Hert (eds), *Research Handbook on Privacy and Data Protection Law* (15 March 2022).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

Regulation EU 2024/… of the European Parliament and of the Council of … laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act).

Rojszczak, Marcin, 'Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace,' *Information & Communications Technology Law*, (Routledge, 2020), 22-44.

Smith, Brad, 'The need for a Digital Geneva Convention,' (14 February 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Smith, David, 'What's really changed 10 years after the Snowden revelations?' in *The Guardian* (7 June 2023). https://www.theguardian.com/us-news/2023/jun/07/edward-snowden-10-years-surveillance-revelations

Steeves, Valerie and Mačėnaitė, Milda, 'Data protection and children's online privacy,' 358-374, in Gloria González, Rosamunde Van Brakel and Paul de Hert (eds), *Research Handbook on Privacy and Data Protection Law* (15 March 2022).

United Nations Advisory Body on Artificial Intelligence, 'Interim Report: Governing AI for Humanity,' (December 2023), 1-28.

Universal Declaration of Human Rights (adopted 10 December 1948) 217 A(III) (UNGA).

van den Heuvel, Karlijn & van Hoboken, Joris, 'The justiciability of data privacy issues in Europe and the US,' in in Gloria González, Rosamunde Van Brakel and Paul de Hert (eds), *Research Handbook on Privacy and Data Protection Law* (15 March 2022), 73-108.

van den Hoven, Jeroen et al., 'Privacy and Information Technology,' in Edward N. Zalta (eds), *The Stanford Encyclopedia of Philosophy* (20 November 2014). https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=it-privacy

Vrabec, Helena U., 'Data Subject Rights Under the GDPR: With a Commentary through the Lens of the Data-Driven Economy,' (Oxford University Press, 2021), 1-268.

Wallace, David & Visger, Mark, 'Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community,' in *Journal of Law & Cyber Warfare*, (2018), 3-55.

White & Case, 'AI Watch: Global regulatory tracker – European Union,' (16 July 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-europeanunion#:~:text=After%20final%20approval%20by%20the,provisions%20listed%20in%20Article%20113.

Wolford, Ben, 'What is GDPR, the EU's new data protection law?" https://gdpr.eu/what-is-gdpr/

Wong, Julia Carrie, ‘The Cambridge Analytica scandal changed the world – but it didn’t change Facebook,’ in *The Guardian* (18 March 2019). https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

Wong, Pak Nung, ‘Techno-geopolitics: US-China Tech War and the Practice of Digital Statecraft,’ in Harsh V. Pant, Frank O’Donnell and Avinash Paliwal (eds), *International Geopolitics in the Age of Disruption*, (Routledge, 2022), 1-123.

World Economic Forum, ‘Why we urgently need a Digital Geneva Convention,’ (29 December 2017), https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention/.

Yilma, Kinfe, ‘The ‘Privacy Problem’ in the Digital Age,’ 1-401, in *Privacy and the Role of International Law in the Digital Age* (Oxford University Press 2023).

Ziemblicki, Bartosz, ‘Modern Technologies as a Challenge for the Right to Privacy under the European Convention on Human Rights,’ 589-604, in *International Community Law Review* (Brill 21 November 2023).

Zuboff, Shoshana, ‘Surveillance Capitalism and the Challenge of Collective Action,’ 10-29, in *New Labor Forum* (2019).