STATE SURVEILLANCE, THE RIGHT TO PRIVACY, AND WHY WE MAY NEED A NEW INTERNATIONAL INSTRUMENT

A Thesis Submitted to the
College of Graduate and Postdoctoral Studies
In Partial Fulfillment of the Requirements
For the Degree of Master of Laws (LLM)
In the College of Law
University of Saskatchewan
Saskatoon

By

ADEMOLA ADEYOJU

PERMISSION TO USE

In presenting this thesis/dissertation in partial fulfillment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis/dissertation in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis/dissertation work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis/dissertation or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis/dissertation.

Requests for permission to copy or to make other uses of materials in this thesis/dissertation in whole or part should be addressed to:

The Associate Dean,
Research and Graduate Studies
College of Law, University of
Saskatchewan, 15, Campus Drive,
Saskatoon, Saskatchewan S7V 5A6 Canada

OR

The Dean
College of Graduate and
Postdoctoral Studies University of
Saskatchewan
Room 116 Thorvaldson Building, 110 Science Place
Saskatoon, SK S7N 5C9 CANADA

ABSTRACT

Especially since the beginning of the 19th century, surveillance has become an integral part of many states' tool to maintain territorial integrity, inform foreign policies, and prevent foreign and domestic threats. Over the years, the means and modes of state surveillance have become more pervasive, more effective, and cheaper, thanks to incredible advancements in technology.

By its very nature, state surveillance threatens an already endangered notion of privacy for which human beings have historically demonstrated an innate desire. So important is privacy, in fact, that for decades, it has been protected under international law as a fundamental right—a protection that is significant not only because privacy is such an integral right in itself, but also because without privacy, other civil liberties, such as the freedom of thought, belief, opinion and expression, cannot be fully or truly exercised.

As technology continues to enhance states' surveillance capabilities and as new and intrusive means capable of monitoring individuals and entire populations are developed, the idea of a global right to privacy—promoted by international law and its interpretations—crumbles. Not only that, as international law has remained relatively static in the face of changing states' priorities, merging of our physical and digital worlds, and the consequent emergence of new privacy concerns, decades-old international law encounters serious problems.

This thesis identifies and discusses the following key problems: first, as international law has failed to clearly regulate foreign surveillance, states have embraced the tendency to offer lesser privacy protections to foreigners, vis-à-vis their citizens/residents when conducting surveillance, thereby rendering questionable the idea of a universal right to privacy. Second, there are controversies regarding the application of international law to the extraterritorial surveillance activities of states. Third, although mass surveillance, particularly mass foreign surveillance, has become a standard part of some states' national security and foreign relations practices, international law has failed to acknowledge mass (foreign) surveillance as a reality of state surveillance, let alone seek to regulate its deployment. Fourth, there are issues with the privacy guarantees under international law as there is little clarity on what the 'right to privacy' actually entails.

Having identified and examined these problems, this thesis concludes that current international law rules on privacy are no longer adequate. The thesis then proposes the making of an international cyber surveillance and privacy instrument to resolve identified problems and set

baseline standards for the conduct particularly of foreign and mass surveillance, in an ultimate bid to maintain some privacy in an increasingly connected and surveilled world. In other words, this thesis makes doctrinal arguments that highlight the flaws or lacunas in current international law on privacy and surveillance, and suggests the making of a new binding international instrument that would clarify current rules and address apparent lacunas.

ACKNOWLEDGMENTS

I am grateful to God for the mental, physical, and psychological strength to undertake and successfully complete this research work. Also, I appreciate the College of Graduate and Postdoctoral Studies and the College of Law, University of Saskatchewan for the generous financial award which has enabled me to complete my LLM program. I am especially grateful to Professor Barbara von Tigerstrom for her exceptional supervision and support throughout the course of my program at the College of Law. I would also like to express my sincere gratitude to Professor Robin Hansen and Professor Mark Carter for their insights and perspectives. I also appreciate my friends and colleagues within the College for their words of encouragement.

TABLE OF CONTENTS

Chapter 1

1.1 Introduction and Background

On 10 December, 1948, shortly after the Second World War, world leaders adopted what is probably the most important international instrument in human history—the Universal Declaration of Human Rights ("UDHR").[1] The first instrument among the International Bill of Rights[2], the UDHR is so significant that it has paved the way for the adoption of more than 80 other treaties, and has become the most translated document in history.[3]

Of the rights protected under the UDHR, the right to privacy stands out. From when it was first conceived on the international scene as an inalienable human right, the right to privacy has gone on to enjoy universal recognition. It is now guaranteed under tens of other international documents, protected by the constitutions of over 130 countries across every region of the world,[4] and has been described as "the most comprehensive of rights and the right most valued by civilized men".[5]

More than ever, the right to privacy—and other vital civil liberties reinforced by it, including the freedom of expression and opinion, freedom of association and peaceful assembly, and right to be free from discrimination—are increasingly exercised online and through information and communication technologies, not least so because parts of our lives now permanently reside online. However, while technology facilitates the exercise of the right to privacy, and has become an indispensable part of global economic, cultural, political, and social realities, it has also enhanced the capacity of governments to conduct invasive and aggressive surveillance,

[1] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) (UDHR)

[2] The UDHR, together with the International Covenant on Civil and Political Rights, ICCPR (n 171) and the International Covenant on Economic, Social and Cultural Rights (16 December 1966, entered into force 3 January 1976) 993 UNTS 1966, form the so-called International Bill of Human Rights.

[3] From Abkhaz to Zulu, and available in more than 370 languages, the Universal Declaration of Human Rights is the most translated document in the world. See: UN Human Rights Office of the High Commissioner, 'New record: Translations of Universal Declaration of Human Rights pass 500' (*OHCHR Official Website*, 2 November 2016) <https://www.ohchr.org/en/human-rights/universal-declaration/new-record-translations-universal-declaration-human-rights-pass-500> accessed 13 July 2022. For a full list of translations, see: UN Human Rights Office of the High Commissioner, 'UDHR Translations' (*OHCHR Official Website*) <https://www.ohchr.org/en/search?f[0]=event_type_taxonomy_term_name%3AUniversal%20Declaration%20of%20Human%20Rights> accessed 13 July 2022.

[4] Privacy International, 'What Is Privacy' (*Privacy International*, 23 October 2017) <https://privacyinternational.org/explainer/56/what-privacy> accessed 10 May 2022

[5] *Olmstead v. United States*, 277 U.S. 438, 470 (1928) (Brandeis, J., dissenting).

including foreign surveillance, i.e., surveillance on people who are non-residents and who are non-nationals of a state.

Yet surveillance—whether domestic or foreign—threatens privacy. In fact, due partly to advancements in technology, states' growing surveillance capabilities, and actual or probable harm to privacy, it is not surprising to note that "[t]hroughout the past quarter century, no other fundamental right in the arena of public policy has generated such turbulence and controversy"[6] as the right to privacy. However, while no attempt is being made to remove states' surveillance powers, considerable legal, policy, and academic efforts are going into finding a balance, such that states can conduct surveillance without violating the right to privacy. Finding a balance is especially crucial to protect foreigners—for whom there appears to be inadequate protection under current international law and towards whom increased states' surveillance activities are directed.

Unravelling the question of where to draw the line has become a central political and policy focus since the 2013 Snowden revelations about the National Security Agency's foreign surveillance activities.[7] Until that question is answered, and in the absence of effective safeguards imposed and implemented on a global scale, there can be no way to ensure that states will curtail their current tendencies to carry out foreign surveillance, including on a mass scale. Yet for all that has been done so far—including certain regional arrangements (particularly in Europe) and soft law resolutions passed by the United Nations (UN)—no definitive or comprehensive global charter on surveillance and privacy is in place yet.[8]

Therefore, it is hoped that this thesis will, at the least, settle some of the current questions on (foreign) surveillance and the idea of a global right to privacy. Without discounting the utility of state surveillance in all its forms, this thesis will analyze the impacts of state surveillance activities on the right to privacy, consider the major international legal instruments protecting privacy, evaluate the major challenges with those laws, and offer some insight into what a concrete international instrument on surveillance and privacy could look like.

When discussing state surveillance in this thesis, major focus is placed on foreign and mass surveillance. Emphasizing the two categories of foreign and mass surveillance provides

[6] Simon Davies, 'Private virtue: At what point does your business become the legitimate concern of others?' (*The Guardian UK*, 7 September 2002*)* <https://www.theguardian.com/uk/2002/sep/07/privacy2> accessed 11 May 2022.
[7] See generally: Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded' (*The Guardian*, 1 November 2013 <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> accessed 11 May 2022.
[8] Kinfe Michael Yilma, 'Digital Privacy and Virtues of Multilateral Digital Constitutionalism - Preliminary Thoughts' (2017) 25 IJLIT 115.

strategic viewpoints to address the main question of this thesis: i.e., the (in)adequacy of current international legal instruments on privacy and surveillance and why we may need a new international instrument.

Again, the focus on these two areas is justified because domestic surveillance activities are attended, in many states, by clear legislative safeguards—these safeguards are usually embedded in national intelligence/defence laws, cybercrimes and criminal laws, or even dedicated surveillance laws, many of which are directly influenced directly by international law. Foreign surveillance, on the other hand, is not clearly regulated by international law, thereby creating room for states to dent the essence of the supposedly global privacy right granted under international law by granting lesser privacy guarantees to foreigners. In the same vein, the focus on mass surveillance is warranted not only because there is now an increasingly blurry line between targeted and mass surveillance, but because mass surveillance poses arguably the greater threat to the right to privacy, and especially to the privacy of foreigners. A dangerous and hard-to-govern phenomenon, mass surveillance operates, on the international stage, outside the bounds and confines of existing and decades-old rules that are "now woefully insufficient".[9]

In terms of definitions, the word 'foreigners' is used throughout to mean those individuals who are both non-nationals *and* non-residents of a state.[10] This means that the concept of 'foreign surveillance', as used this thesis, would not cover an instance where a state surveils the activities of one of its nationals who is also resident within its territory; one of its nationals who is resident in another state; or a resident who is not a national. On a related note, 'mass surveillance' denotes the intrusion by states of the privacy of a group of individuals usually through the interception of their communications. Both the individuals involved and the communication intercepted are often designated too broadly or not sufficiently defined. The term 'mass surveillance' does not cover activities by non-state entities such as technology companies.

[9] Bruce Schneier, *Data And Goliath: The Hidden Battles to Collect Your Data and Control Your World*, (W.W Norton & Company 2015) 12.

[10] Residents are within the territorial jurisdiction of states, and are not, therefore, categorized as foreigners. Likewise, nationals who are outside a state's jurisdiction are also not considered as foreigners, since "[s]tates may assert jurisdiction over the acts of their nationals, wherever the act might take place." See: Steve Coughlan, Robert J. Currie, Hugh M. Kindred, Teresa Scassa, *Law Beyond Borders. Extraterritorial Jurisdiction in an Age of Globalization* (Irwin Law Inc 2014) 37.

It is also important to note here that this work is focused solely on state surveillance, to the exclusion of related issues such as espionage or spying,[11] which are generally considered to be extra-legal in nature. Whereas state surveillance is legitimate and allowed under international law, the core of espionage is treachery and deceit and is contrary to the principles of international law,[12] which is founded on decency and common humanity.[13] Other works have considered the legal status of espionage and issues surrounding its use in peacetime and during armed conflicts.[14]

Chapter 1 of this thesis shows how privacy is currently being invaded by state actors and offers perspectives into the technological means enabling the invasion. The chapter is divided into two parts: the first part discusses the nature and extent of state surveillance. Using the Snowden disclosure as an instance, the section explores states' surveillance capabilities, with particular focus on the US and other members of the Five Eyes. The section also considers the immediate and lasting impacts of Snowden's disclosures, which include particularly a renewed focus on the importance of privacy on both national and international stages. It is noted, however, that despite all the efforts that have been made so far, not a lot has changed in terms of legislative/substantive and procedural/practical developments.

The second part of chapter 1 examines common state surveillance techniques. The chapter helps to understand the true extent of state surveillance capabilities and provides insight into how surveillance activities are carried out in practice, by offering a glimpse into some of the

[11] The concepts of surveillance and espionage are similar in many ways and the distinction between them is often imprecise and unclear, leading some authors to use the concepts fluidly and interchangeably. (See William C. Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66 ELJ) However, by way of offering some distinction, it is worthy to note that while surveillance often entails the continuous monitoring and collection of information for legitimate purposes (national security, economic advantage, population control, and more recently to curb the pandemic), espionage is often a deeply covert and illegal operation used to gain military or political advantage.

[12] This sentiment has conferred on espionage the cloak of illegitimacy. Interestingly, "[e]ven the law of diplomacy (a major area of spying activities) touches only very briefly and opaquely on questions of espionage, choosing instead to circle around the problem without ever tackling it directly." See A. John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28(3) MJIL 596. On a related note, the argument that because espionage is so widespread it has earned recognition under customary international law has been rejected. See, for example, Inaki Navarrete & Russell Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 Cornell Int'l LJ 897

[13] Radsan (n 12)

[14] See generally Geoffrey B. Demarest, 'Espionage in International Law' (1996) 24 Denv J Int'l L & Pol'y 321; Russell Buchan, 'Taking Care of Business: Industrial Espionage and International Law' (2019) 26 Brown J World Aff 143; Kathryn Jane Browne, 'The Paradox of Peacetime Espionage in International Law: From State Practice to First Principles' (2017) 23 Austl Int'l LJ 109; Patrick C. R. Terry, '"The Riddle of the Sands" - Peacetime Espionage and Public International Law' (2020) 51 Geo J Int'l L 377; Juan Pablo Hernández, 'The legality of espionage in international law' (The Treaty Examiner: Online Journal of International Law April 2020) https://treatyexaminer.com/espionage-legality/ accessed 19 November 2022; Veronika Prochko, 'The International Legal View of Espionage' (E-International Relations 2018) https://www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/ accessed 19 November 2022

most common techniques that states employ—from systems hacking and facial recognition technology to fibre optic cables tapping and the circumvention of online encryption.

Chapter 2 is also divided into two parts. The first part revolves around two of the most popular justifications for why states conduct surveillance: the value of security (and states' fundamental duty to protect everyone in the society) and the "nothing to hide" argument (prevalent on its own but also complementing and strengthening the security argument by seeking to relegate the value of privacy as a human right). Alternative views are offered in this section to balance the reader's perception of the facts and stimulate a reassessment of the cogency of the aforementioned bases for surveillance.

The second part—on the implications of state surveillance for privacy—explores how state surveillance activities affect privacy. To understand what aspect of privacy we are mostly concerned with here, a brief but useful explanation of what privacy means in the context of the thesis is provided, and the thesis settles on its own conception of privacy: (i.e., informational or data, communications, and individual privacy), which is necessary because privacy is such a multi-dimensional concept.

By providing some insights into the rationalizations that states and individuals employ to validate and promote surveillance agenda, this chapter offers key context into the factors that have fuelled—and continue to fuel—the growth of state surveillance. The chapter also delineates the scope of privacy under consideration, which is important as the discourse sharply progresses into a distinct focus on the interplay between privacy, surveillance, and law.

Chapter 3 of this thesis is on privacy, state surveillance, and international law. Here, key international instruments guaranteeing the right to privacy are considered. It is noted in this chapter that since privacy guarantees are not absolute, they can be curtailed in certain circumstances, including where states have to conduct surveillance for legitimate purposes. However, when conducting surveillance, certain principles have evolved to guide how states can go about their surveillance activities without jeopardizing privacy. In this chapter, we get a sense of how privacy is currently protected under current international law and the limitations that apply to the right.

Chapter 4 analyses the major problems with current international law on privacy: it suggests that states' surveillance practices, as they have evolved over the years, have become irreconcilable with current international law. Not only has international law failed to regulate foreign surveillance (thereby leaving room for states to make privacy-defeating foreign

surveillance laws), there are controversies regarding the scope of application of privacy obligations in international instruments. Also, mass surveillance is not regulated and there is little clarity on what the 'right to privacy' actually entails. This chapter exposes the doctrinal gaps and lacunas in current international law, and shows how states have exploited those lacunas, further weakening the right to privacy.

Based on the problems with the current international law on privacy explored above, chapter 5 concludes that existing international instruments are no longer adequate and proposes that we start exploring the idea of making a new, comprehensive, and modern international instrument to guide (especially foreign) surveillance activities and ensure real protection of a truly universal right to privacy. The section then highlights key elements to be considered as part of the new instrument.

It is important to note that while other scholars and prominent authors have proposed that the solution to excessive and unwarranted state surveillance is a new international instrument,[15] the major contribution of this thesis is its critical examination of the ills of state surveillance, the essence of privacy in a modern society and why it deserves protection; its evaluation of doctrinal gaps in current international law; and its proposition of concrete considerations in the making of a new international instrument. Put differently, this thesis is important because it investigates the doctrinal holes or problems that beset current international law on privacy—problems tangible enough to necessitate a serious consideration of a new instrument—and then analyses what the new instrument should look like in terms of specific provisions. That said, this thesis is not intended to be an exhaustive legal analysis, but only to investigate and stimulate further conversations about the constantly evolving nature of surveillance and privacy, and the role of international law.

[15] Cole David and Fabbrini Federico, 'Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders' (2016) 14(1) IJCL < https://doi.org/10.1093/icon/mow012> accessed 15 May 2022 (Although writing in the context of the US-EU transatlantic relationship, David Cole and Federico Fabbrini have also advocated the making of some sort of transatlantic compact, which ensures on a reciprocal basis that one state will not unwarrantedly carry out surveillance activities on citizens of other states); Frédéric Gilles Sourgens, 'The Privacy Principle' (2017) 42 YJIL 345, 349 (Whilst discussing the problematic application of existing international law approaches to the protection of privacy, Sourgens proposes in his essay on *The Privacy Principle*, that "privacy protections enshrined in human rights treaties could be extended by reliance upon another source of international law…"); Yilma (n 8) (Here, Yilma proposed the formulation of "a UN Declaration of Internet Rights as a pragmatic approach for upholding digital privacy rights [and serving] as an important supplement to the present international privacy norms that predate modern means of digital communication."); Asaf Lubin, 'We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance' (2018) 18 CJIL 502, 503 (Writing mainly from the foreign surveillance context, Asaf Lubin argues that it is time we stepped outside the "bounded thinking of one-size-fits-all human rights standards for all surveillance practices, and begin a much needed conversation on what a uniquely tailored human rights regime might look like").

1.2 On the Nature and Extent of State Surveillance

> "Publicity is the fittest law for securing the public confidence, and causing it constantly to advance towards the end of its institution… Without publicity, no good is permanent: under the auspices of publicity, no evil can continue. Conversely, 'secresy [sic] is an instrument of conspiracy; it ought not, therefore, to be the system of a regular government." -- Jeremy Bentham.[16]

Throughout history, governments across the world have carried out surveillance activities. Although those activities were not always 'foreign or 'mass' in nature, many states have maintained—especially since the beginning of the 19th century—intelligence offices, with personnel and units whose sole function is gathering, analyzing, and disseminating critical information on key political individuals, criminals, suspected enemies of states, and other governments' visiting officials.[17]

Due mainly to advancements in technology and the resulting growth of surveillance techniques and tools, state surveillance has changed profoundly from what it used to be: in the early to mid '80s, a number of dedicated law enforcement officers would have to work in concert, and usually round the clock, to tail a single suspect's movement. Even when wiretapping became a tool in the late '80s and early '90s, it still cost a lot of resources to listen in on the conversations of persons of interest. Consequently, "[t]he effort needed to collect [information through these tedious means] meant that governments would engage in surveillance only rarely, and only for compelling reasons… ".[18]

Today, everything has changed: "new technologies, from surveillance cameras and web bugs to thermal scanners and GPS transponders, have increased the ability to track, observe, and monitor, [and] [t]he scope and variety of the types of surveillance that are possible today are unprecedented in human history".[19] Indeed, things have changed so radically that now, only a few people are required to operate systems that can spy on an entire population. Not only have advancements in technology made it so that information gathering is now easy, technology has also enable the combination, aggregation, and analysis of information using powerful supercomputers that can find the needle in a haystack. Meanwhile, "[d]eclining costs of

[16] Jeremy Bentham, *The Collected Works of Jeremy Bentham: Political Tactics* (Clarendon Press 1999) 29 and 37.
[17] See generally: Carl Nyst, 'Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy Which Fortifies Them – An Activist's Account' (2018) 7 State Crime Journal 8.
[18] Jonathan Weinberg, 'The Real Costs of Cheap Surveillance' (*The Conversation*, 18 July 2017) <https://www.scientificamerican.com/article/the-real-costs-of-cheap-surveillance/> accessed 5 May 2022.
[19] Neil M. Richards, 'The Dangers of Surveillance' (2013) 126 HLR 1934, 1936.

technology and data storage have [also] eradicated financial or practical disincentives to conducting surveillance".[20]

What all of these mean is that states now have greater capabilities now, more than any other time in recorded history, to "conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."[21] Yet, states continue to build their capabilities. To get a sense of how states are pouring billions of dollars into developing surveillance and intelligence machines and apparatuses, consider the following observations of the US intelligence community by Tom Engelhardt:

> By 1964, the US Intelligence Community, or IC, had nine members, including the CIA, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA). [T]he IC of today, with seventeen official outfits, has, by the simplest of calculations, almost doubled. Take one outfit, now part of the IC, that didn't exist back in 1964, the National Geospatial-Intelligence Agency. With an annual budget of close to $5 billion, it recently built a gigantic $1.8 billion headquarters—"the third-largest structure in the Washington area, nearly rivaling the Pentagon in size"—for its sixteen thousand employees. It literally has its "eye" on the globe in a way that would have been left to sci-fi novels almost half a century ago…
>
> Or consider an outfit that did exist then: the National Security Agency, or NSA (once known jokingly as "No Such Agency" because of its deep cover). Like its geospatial cousin, it has been in a period of explosive growth, budgetary and otherwise, capped by the construction of that "heavily fortified" data center in Utah. According to NSA expert James Bamford, the center was built to "intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks."[22]

Thanks to works by journalists and whistle-blowers who continue to share with the public what states seek to keep hidden, we now have a good understanding of the nature of state surveillance. These works also offer us a glimpse into the extent of states' surveillance capabilities, even if only on a theoretical or notional note.

---

[20] UN Human Rights Office of the High Commissioner, 'A/HRC/27/37: The right to privacy in the digital age (focus on surveillance) - Report of the Office of the UN High Commissioner for Human Rights' (*OHCHR Official Website,* 30 June 2014) <OHC OHCHR | A/HRC/27/37: The right to privacy in the digital age (focus on surveillance) - Report of the Office of the United Nations High Commissioner for Human Rights> accessed 23 June 2022*;* UN General Assembly, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) 23rd Session A/HRC/23/40.

[21] Ibid.

[22] Tom Engelhardt, *Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World* (Haymarket Books 2014) 32 and 33.

Of the disclosures made so far, perhaps the most important is the publication of extensive and sensitive materials shared by Edward Snowden, a former intelligence contractor for the National Security Agency ("NSA") and once the most wanted man in the world.[23] Made a decade ago, Snowden's disclosures came as a shock to many people, governments, and intelligence communities across the globe.[24] The disclosures publicised global surveillance programmes[25] including the monitoring and collection by the US government and its foreign partners (particularly members of the Five Eyes Intelligence Alliance)[26] on a mass scale of information from phones, social media networks, laptops and other digital devices—information originating from or belonging to Americans and foreigners.[27] Although the other four members of the Five Eyes (Australia, Canada, Britain and New Zealand) with whom the US had no-spying arrangements were exempted from this pervasive monitoring, virtually every other country on earth, including even international organizations like the World Bank,

[23] James Bamford, 'The Most Wanted Man in the World' (*Wired*, 13 August 2014) <https://www.wired.com/2014/08/edward-snowden/> accessed 5 May 2022

[24] Although the NSA and the Foreign Intelligence Surveillance Act have been the centre of most of the attention directed at mass surveillance in the United States, it is worthy to note that as recently as February 2022, a declassified letter by U.S. Senator Ron Wyden, D-Ore., and Sen. Martin Heinrich, D-N.M reveals that the Central Intelligence Agency ("CIA") has been carrying out its own mass surveillance and warrantless collection of [American] data. According to the letter, the CIA has done all this "entirely outside the statutory framework that Congress and the public believe govern this collection, and without any of the judicial, congressional or even executive branch oversight that comes with FISA collection. This fact has been kept from the public and from Congress." See: Letter from Senator Ron Wyden, D-Ore., and Sen. Martin Heinrich, D-N.M to the Honorable Avril D. Haines and the Honorable William J. Burns (13 April 2021); Ron Wyden: United States Senator for Oregon, 'Wyden and Heinrich: Newly Declassified Documents Reveal Previously Secret CIA Bulk Collection, Problems With CIA Handling of Americans' Information' (2022) <https://www.wyden.senate.gov/news/press-releases/wyden-and-heinrich-newly-declassified-documents-reveal-previously-secret-cia-bulk-collection-problems-with-cia-handling-of-americans-information> accessed 23 May 2022.

[25] Apart from Snowden's disclosures, it is worthy to note that there have been other revelations regarding the existence and operation of mass surveillance programs, some of which clearly demonstrates states' growing technological capabilities and powers to hack into systems from anywhere in the world, sweep digital footprints of mass populations, and collect detailed information on persons of interest. For instance, in 2017, WikiLeaks, an international organization that publishes privileged information and classified media, released what it described as 'the largest ever publication of confidential documents on the [CIA]'. Codenamed Vault 7, the more than 8, 000 documents revealed the CIA's assembly of its own fleet of hackers, development of "more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware", capabilities to intercept communications before they are encrypted and use vulnerabilities in the operating systems of general-purpose computing devices to take full control of those devices. See: WikiLeaks, 'Vault 7: CIA Hacking Tools Revealed' (2017) <https://wikileaks.org/ciav7p1/> accessed 11 May 2022.

[26] The Five Eyes is an intelligence-sharing alliance consisting of the US, UK, Australia, Canada & New Zealand. The alliance was formed after the Second World War and is widely regarded as the world's most significant intelligence alliance in the world. See: J Vitor Tosinni, 'The Five Eyes – The Intelligence Alliance of the Anglosphere' (*UK Defence Journal*, 14 April 2020) <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/> accessed 17 May 2022.

[27] David E. Sanger and Eric Schmitt, 'Snowden Used Low-Cost Tool to Best N.S.A' (*The New York Times*, 8 February 2014) <https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html> accessed 17 May 2022. (Whilst thousands of the classified documents released by Snowden has been published, intelligence officials believe Snowden accessed roughly 1.7 million files); History, 'Edward Snowden discloses U.S. government operations' (*History*, 26 June 2018) <https://www.history.com/this-day-in-history/edward-snowden-discloses-u-s-government-operations> accessed 17 May 2022. (Snowden has since been "charged with theft of government property, unauthorized communication of national defense information and willful communication of classified communications intelligence…").

International Monetary Fund, and International Atomic Energy Agency, were swept up in this surveillance scheme.[28]

Referred to as "the most significant leak in US history"[29], Snowden's disclosures have prompted responses from high-ranking US government officials, sparked outrage from world leaders, including German Chancellor Angela Merkel and then-Israeli Prime Minister Benjamin Netanyahu.[30] The disclosures also validated long-standing suspicions by civil liberties organizations; led to raging debates on states' surveillance capabilities and arguments regarding the place of privacy in the face of national security;[31] and damaged the US' reputation as a liberties-protecting state.[32]

Contrary to the lines of arguments pursued by the US authorities—to the effect that they only conduct surveillance on persons of interests as opposed to common Americans—a four-month investigation by *The Washington Post* based on files provided by Snowden has revealed that besides persons of interest, innocent Americans and non-Americans alike were targeted. According to the *Post*, "[n]early half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents."[33] To make matters worse, information is collected not only on targets but also on virtually anyone who crosses the target's path. In one case, an NSA analyst wrote *'1 target, 38 others on there'* and collected data on them all. In an account on how files on

[28] Ellen Nakashima and Barton Gellman, 'Court gave NSA broad leeway in surveillance, documents show' (*The Washington Post*, 30 June 2014) <https://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html?hpid=z> accessed 17 May 2022.

[29] Jack Mirkinson, 'Daniel Ellsberg Calls Edward Snowden A 'Hero,' Says NSA Leak Was Most Important In American History' (*HuffPost*, 10 June 2013) <https://huffingtonpost.com/2013/06/10/edward-snowden-daniel-ellsberg-whistleblower-history_n_3413545.html> accessed 17 May 2022.

[30] James Ball and Nick Hopkins, 'GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief'(*The Guardian*, 20 December 2013) <https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner> accessed 17 May 2022.

[31] It is interesting to note that in one case at least, the then-US President, Barrack Obama acknowledged in a 2013 interview that security threats thwarted by NSA surveillance could well have been prevented through other means. See: Josh Gerstein, 'NSA: PRISM stopped NYSE attack' (*Politico*, 18 June 2013) <https://www.politico.com/story/2013/06/nsa-leak-keith-alexander-092971> accessed 17 May 2022. Besides the former President's admission, a White House review panel on NSA surveillance has also concluded that the NSA program was "not essential in preventing attacks", whilst finding that "there has been no instance in which NSA could say with confidence that the outcome [of a terror investigation] would have been any different" without the program. See: Michael Isikoff, 'NSA program stopped no terror attacks, says White House panel member' (*NBC News*, 20 December 2013) <https://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588> accessed 17 May 2022.

[32] Pew Research Center, 'Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image' (*Pew Research Center*, 14 July 2014) <https://www.pewresearch.org/global/2014/07/14/global-opposition-to-u-s-surveillance-and-drones-but-limited-harm-to-americas-image/> accessed 17 May 2022.

[33] Barton Gellman, Julie Tate and Ashkan Soltani, 'In NSA-intercepted data, those not targeted far outnumber the foreigners who are' (*The Washington Post*, 5 July 2014) <https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html> accessed 22 May 2022.

people other than targets—containing intimate and sensitive facts—were not only collected but also retained, the Post narrates that:

> Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless… Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risque poses in shorts and bikini tops.[34]

Just as the US authorities' arguments did not succeed in the court of public opinion, the basis for their action also failed in the court of law. In 2013, two notable, albeit contradictory, judicial decisions regarding the legality of the US surveillance programs were handed down in *Klayman v. Obama* and *ACLU v. Clapper*. In the former, Judge Richard Leon ruled that "the daily collection of virtually all Americans' phone records is almost certainly unconstitutional"[35] and in the latter, Judge William H. Pauley III—ruling only two weeks later—concluded "that the NSA's bulk telephone metadata spying program is "lawful" and represents the nation's "counter-punch" to terrorism".[36] Finally, in 2020, the US Court of Appeals for the Ninth Circuit handed down a definitive decision—the Court found that the NSA's warrantless mass surveillance activities were possibly unconstitutional and clearly illegal, seeing as they violated the Foreign Intelligence Surveillance Act.[37]

Meanwhile, Snowden's disclosures have also made lasting impressions and left huge impacts on the global stage.[38] They have raised awareness regarding the importance of encryption, enhanced the dissonance between European Union "EU" and the US on privacy and data protection, with some scholars even claiming that the EU "General Data Protection Regulation might never have happened without the Snowden revelations"[39]. The disclosures also created

---

[34] Ibid.
[35] Ellen Nakashima and Ann E. Marimow, 'Judge: NSA's collecting of phone records is probably unconstitutional' (*The Washington Post*, 16 December 2013) <https://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html> accessed 23 May 2022.
[36] David Kravets, 'Judge Rules NSA Bulk Telephone Metadata Spying Is Lawful' (*Wired*, 27 December 2013) <https://www.wired.com/2013/12/judge-upholds-nsa-spying/> accessed 24 June 2022.
[37] United States v Moalin (2021) 9th Circ. 10CR4246-JM.
[38] Patrice McDermott, 'Secrets and Lies—Exposed and Combatted: Warrantless Surveillance Under and Around the Law, 2001–2017' (2018) 2 Secrecy and Society 1.
[39] Nikhil Kalyanpur and Abraham Newman, 'Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened' (*The Washington Post*, 25 May 2018)

a spiral of events leading to the recommendation by the NSA in 2019 that the phone-surveillance program created following the 9/11 attacks be terminated.[40]

However, while some efforts have since been made to curtail warrantless mass surveillance and promote transparency, particularly by the US government, experts generally believe that there is still so much to be done. The common sentiment seems to be that "[f]rom a big-picture analysis, there's been a lot of developments without a whole lot of movement…"[41] or as American Civil Liberties Union's Ben Wizner puts it: "As far as the reforms themselves, they were, in the US, both historic and inadequate."[42]

To buttress the above observation, it is worthy to note that the US government still monitors, intercepts, and collects huge amount of information or data from foreigners and foreign entities without warrant or limits.[43] The collection of vast amount of data on innocent people continues despite the passage of the US *Freedom Act* in 2015. Unsurprisingly, the *Freedom Act* has been condemned as not going far enough in reforming US surveillance programs.[44] Speaking of which, the Office of the Director of National Intelligence has admitted that the Freedom Act allows the collection of "three times as much American telephone data… than before the law's enactment".[45] Finally, the monitoring of top foreign officials and the gathering of information from or on any person of interest has not stopped.[46]

While the US and the Five Eyes have acquired a bad reputation for their surveillance activities, it would be misleading to imply or think they are alone. As the UN Special Rapporteur on the Right to Privacy himself noted in 2017, "*a number of states have actually expanded large scale and extremely intrusive surveillance through new laws in the years since Snowden first brought*

<https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/> accessed 13 June 2022.

[40] Dustin Volz and Warren P. Strobel, 'NSA Recommends Dropping Phone-Surveillance Program' (*The Wall Street Journal*, 24 April 2019) <https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247> accessed 13 May 2022.

[41] Sarah Childress, 'How the NSA Spying Programs Have Changed Since Snowden' (*Frontline*, 9 February 2015) <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/> accessed 13 May 2022.

[42] Sean Gallagher, 'The Snowden Legacy, part one: What's changed, really?' (*Ars Technica*, 21 November 2018) <https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/> accessed 11 May 2022.

[43] Patrick Toomey, 'The NSA Continues to Violate Americans' Internet Privacy Rights' (*ACLU*, 22 August 2018) <https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy> accessed 11 May 2022.

[44] Bill Chappell, 'Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail' (*NPR*, 2 June 2015) <https://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act> accessed 11 May 2022.

[45] Patrick G. Eddington, 'The Snowden Effect, Six Years On' (*Just Security*, 6 June 2019) <*https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/*> accessed 11 May 2022

[46] Childress (n 41)

such practices to light."[47] The Special Rapporteur then goes on to reference the UK's "Investigatory Powers Act [which] authorizes mass surveillance and hacking and requires internet companies to store a record of every website their users visit"[48] and French laws "that enable sweeping surveillance with insufficient safeguards…".[49]

Many other countries, including well-known surveillance states like China, Bahrain, India, Russia, and North Korea are also heavily implicated.[50] And if precedent is anything to go by, one is justified to think that states will continue not only to invest heavily in their own surveillance capabilities, they will also continue to augment or upgrade their surveillance technologies by licensing from other states or private spyware vendors.[51] Speaking of private vendors' contribution to the growth of the surveillance state, vendors such as *Pegasus,*[52] *Candiru,*[53] and *Circles*[54] continue to spring up in what is clearly a lucrative market, and their activities—i.e., the commercialization and sale of surveillance technologies—have attracted attention on the international stage.[55]

---

[47] Human Rights Watch, 'Human Rights Council: Protect the right to privacy' (*Human Rights Watch*, 8 March 2017) <https://www.hrw.org/news/2017/03/08/human-rights-council-protect-right-privacy> accessed 13 May 2022. (emphasis added).

[48] Ibid.

[49] Ibid.

[50] I have written elsewhere about how even African governments, despite their limited resources, carry out mass surveillance on an unprecedented scale and through various means: from monitoring entire Internet traffic and filtering communications to restricting anonymous communications and the bulk collection of user data (See: Ademola Adeyoju, 'Africa and the State of Digital Privacy Protection' (forthcoming)); See also: Tony Roberts, et al., 'Surveillance Law in Africa: a review of six countries' (2021) Institute of Development Studies 1. In another instance, systems of mass surveillance, which entailed the almost total domination and control of online communications were also reportedly used by a couple of African governments in the lead-up to the Arab Spring. See: European Parliament, Directorate-General for External Policies, Policy Department, After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy (2012), pp. 9-10.

51 Speaking of private spyware vendors, only last year, when asking how state surveillance has reached the unprecedented level it has reached today, the UN High Commissioner for Human Rights, Michelle Bachelet, attributed the problem to the growth of a "surveillance technology market has dangerously flourished in the shadows, far from justice oversight and public scrutiny–both in authoritarian countries and in democracies"; UN Human Rights Office of the High Commissioner, 'Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe - Hearing on the implications of the Pegasus spyware' (*OHCHR Official Website*, 14 September 2021) <https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe> accessed 11 May 2022.

[52] The Citizen Lab, 'Pegasus' (*The Citizen Lab*, 2022) <https://citizenlab.ca/tag/pegasus/> accessed 15 May 2022.

[53] Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak and Ron Deibert, 'Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus' (*The Citizen Lab*, 15 July 2021) <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/> accessed 14 May 2022.

[54] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis and Ron Deibert, 'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles' (*The Citizen Lab*, 1 December 2020) < https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/> accessed 15 May 2022.

[55] In a Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, private entities that develop surveillance technologies have been enjoined to not only build into their technologies and systems robust safeguards (including human rights by design and "contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes," they are also required to promptly report evidence of misuse to relevant authorities or oversight bodies. See: UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (28 May 2019) 41st Session A/HRC/41/35. See also: UN General Assembly, 'Right to Privacy in the Digital Age' (13 October 2021) 48th Session A/HRC/RES/48/4.

Yet, continuing advances in technology and the ambition to build smart cities, the increased adoption of digital devices, constant access to the internet and the ever-growing desire by governments to carry out preventive law enforcement combine to depict a grim future for basic human rights, for democracy, and for the rule of law everywhere across the globe. One can almost visualize this grim future even in a place like Europe where the European Union ("EU") continues to establish itself as the global leader in digital privacy regulation and protection.

In what was an unusual twist of events, the same EU recently published a legislative proposal[56] that will see the institution headed in what the *Electronic Frontier Foundation* has described as "a dramatically different direction… [entailing] seeking state-controlled scanning of all messages."[57] The EU proposal, titled the 'Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse', has been described by Johns Hopkins University Professor Matthew Green as "the most terrifying thing [he's] ever seen"[58].

If passed into law, the proposal will establish a new international mass surveillance system that compels a broad range of entities to constantly access, search, and analyse private messages on behalf of states to discover cases of child sexual abuse. Reading through the proposal, it becomes obvious that this constant search is intended to be carried out on both "'public-facing' and 'private' services, including interpersonal communication services", which the proposal itself admits will "result in varying levels of intrusiveness in respect of the fundamental rights of users." Yet, to enable technology companies and other 'third-party entities' to search private communications is to render end-to-end encryption all but meaningless. This is a huge problem on its own. As the document notes:

On a related note, States are advised to refrain from using surveillance technologies in a way that infringes any human right and are urged to "take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations" (UN General Assembly (n 16) para 97). This duty of States to consider human rights when exporting surveillance technologies goes beyond its borders. It includes the duty to "have in place export control regimes applicable to surveillance technology, which provide for assessing the legal framework governing the use of the technology in the destination country, the human rights record of the proposed end user and the safeguards and oversight procedures in place for the use of surveillance powers." UN General Assembly, 'The right to privacy in the digital age' (3 August 2018) 39th Session A/HRC/39/29.

[56] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse' (*European Union Official Website*, 11 May 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472> accessed 15 May 2022.

[57] Joe Mullin, 'The EU Commission's New Proposal Would Undermine Encryption and Scan Our Messages' (*Electronic Frontier Foundation*, 11 May 2022) <https://www.eff.org/deeplinks/2022/05/eu-commissions-new-proposal-would-undermine-encryption-and-scan-our-messages> accessed 12 June 2022.

[58] Matthew Green (@matthew_d_green), 'This document is the most terrifying thing I've ever seen…' Twitter, 10 May 2022 <https://twitter.com/matthew_d_green/status/1524094474187644933> accessed 10 May 2022.

> … the detection process is generally speaking the most intrusive one for users (compared to the detection of the dissemination of known and new child sexual abuse material), since it requires automatically scanning through texts in interpersonal communications. It is important to bear in mind in this regard that such scanning is often the only possible way to detect it and that the technology used does not 'understand' the content of the communications but rather looks for known, pre-identified patterns that indicate potential grooming. Detection technologies have also already acquired a high degree of accuracy, although human oversight and review remain necessary…[59]

As strange as this proposal is, the EU has explained that the reason for putting it forward is really to aid efforts to "detect, report, block and remove child sexual abuse material… [and enable] improved detection, investigation and prosecution of offences… "[60] On the face of it, this sounds like a good reason, but it does not take much probing to discover that the proposal is going to mandate the building of backdoors into encrypted online communications and essentially eliminate online privacy. Indeed, the reason fronted by the EU and the incidental effect of the proposal reminds one of the ongoing war on encryption by the Five Eyes and other states' intelligence agencies[61], and brings into view a pattern showing how other governments have attempted to create communications backdoors through regulations made ostensibly[62] to combat child abuse.[63]

---

[59] European Commission (n 56)

[60] Ibid.

[61] Whitfield Diffie, 'The Encryption Wars Are Back but in Disguise' (*Scientific American*, 30 June 2020) <https://www.scientificamerican.com/article/the-encryption-wars-are-back-but-in-disguise/> accessed 19 May 2022; Mike Masnick, 'EU Proposes It's Own Version Of EARN IT: Effectively Mandates Full Surveillance Of All Messaging & No Encryption' (*Tech Dirt*, 12 May 2022) <https://www.techdirt.com/2022/05/12/eu-proposes-its-own-version-of-earn-it-effectively-mandates-full-surveillance-of-all-messaging-no-encryption/> accessed 23 May 2022.

[62] Many have argued—and I also believe—that these new legislation crafted in the name of protecting children from sexual abuse and sex trafficking are really meant to undermine end-to-end encryption, which is a core defence on the internet, allowing communications to flow from one end to the other securely and confidentially. As one writer puts it, "[t]he motivating factor here isn't an epidemic of kiddie porn. It's more of an organized effort among multiple governments to turn the public against anything that shields communications from prying eyes."; J.D. Tuccille, 'Invasion Of Privacy: Earn It Act Abuses Privacy in the Guise of Protecting Kids' (*Reason*, 16 February 2022) <https://reason.com/2022/02/16/earn-it-bill-abuses-privacy-in-the-guise-of-protecting-kids> accessed 5 May 2022; Dan Milmo, 'End-to-end encryption protects children, says UK information watchdog' (*The Guardian*, 21 January 2022) <https://www.theguardian.com/technology/2022/jan/21/end-to-end-encryption-protects-children-says-uk-information-watchdog> accessed 5 May 2022; Scott Shackford, 'The U.K. Government's Latest Encryption Fearmongering Relies on Child Sex-Trafficking Panics' (*Reason*, 18 January 2022) <https://reason.com/2022/01/18/the-u-k-governments-latest-encryption-fearmongering-relies-on-child-sex-trafficking-panics/> accessed 5 May 2022.

[63] Australian Border Force, 'Statement of Principles on Access to Evidence and Encryption' (*Australian Border Force*) <https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption> accessed 5 May 2022; Alfred NG, 'Why your privacy could be threatened by a bill to protect children' (*CNET*, 2 July 2020) <https://www.cnet.com/news/politics/why-your-privacy-could-be-threatened-by-a-bill-to-protect-children/> accessed 5 May 2022.

Unsurprisingly, the EU proposal has already faced staunch pushbacks from privacy activists and experts,[64] and the EU's largest member country, Germany, has tagged the proposal an attack on privacy and fundamental freedoms.[65]

1.3 Understanding Common State Surveillance Techniques

To conduct surveillance, states employ different techniques. These techniques range from systems hacking and facial recognition technology to fibre optic cables tapping and the circumvention of online encryption. Based on confidential documents on surveillance disclosed so far, government records, and publicly available information, we now have a sense of what technological capabilities states possess. Below, we will see some of the most common state surveillance techniques.

1.3.1 Internet Surveillance

Internet surveillance is perhaps the most common form of state surveillance, owing mainly to the global nature of the internet, the relative ease by which states' intelligence agencies can tap into the internet's network and infrastructure, and the incredible amount of data that can be gathered even with minimal effort. Starkly contrasting with the old, expensive, and ineffective human surveillance, internet surveillance is done remotely, automatically, and unobtrusively. It allows states to have both 'front-door' and 'back-door' access to communications transmitted over internet or network infrastructures and to monitor the activities of an individual or an entire population.

Front-door access allows states to have direct, unrestricted access to social media queries, emails, financial records, files transfers, internet surfing habits, etc., either by tapping fibre optic cables through which all this data is sent or by requesting/compelling internet companies—through which most of these communications pass—to hand over the data. The once-secret US PRISM program, which enables real-time, "direct access to servers of firms including Google, Apple, and Facebook"[66] affords a good instance.

Back-door access, on the hand, enables states to secretly break into major communications links or servers, and intercept data without the knowledge of the servers' owners or individual

[64] Mullin (n 57)
[65] Clothilde Goujard and Louis Westendarp, 'Germany forces EU into damage control over encryption fears' (*Politico*, 10 June 2022) <https://www.politico.eu/article/germany-eu-damage-control-encryption-abuse-online/> accessed 19 June 2022.
[66] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' (*The Guardian*, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 22 May 2022; Zack Whittacker, 'PRISM: Here's how the NSA wiretapped the Internet' (*ZDNET*, 7 June 2013) <https://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/> accessed 22 May 2022.

data subjects. The joint NSA and United Kingdom Government Communications Headquarters ("GCHQ")'s Muscular (which scoops internet traffic passing through private networks, bypasses encryption used on public networks, and decodes proprietary data formats) and Tempora (through which Britain's spy agency "analyses torrents of the world's internet data"[67] and exploited global telecommunications networks)[68] are prime examples.

1.3.2 Telephone Surveillance

Closely related to internet surveillance, telephone surveillance allows states to intercept, make copies, review, and analyse telephone data: text messages, fax messages, movement from one cell tower to another, and voice traffic. Indeed, "[e]vidence that the NSA was secretly building a vast database of U.S. telephone records—the who, the how, the when, and the where of millions of mobile calls—was the first and arguably the most explosive of the Snowden revelations".[69]

Telephone surveillance is so effective that it can be used to spy on entire populations, "collecting 'pretty much everything it can' rather than merely storing the communications of existing surveillance targets".[70] For example, the NSA and GCHQ covert global surveillance collection system, codenamed *DishFire*, carried out an untargeted global communications sweep.[71] *DishFire* collected on a daily basis details of 1.6 million border crossings based on the interception of network roaming alerts; the geolocation data of more than 76,000 text messages and other travel information; over 800,000 financial transactions that are either gathered from text-to-text payments or from linking credit cards to phone users; and about 200 million text messages from around the world.[72]

[67] Kadhim Shubber, 'A simple guide to GCHQ's internet surveillance programme Tempora' (*Wired*, 24 June 2013) <https://www.wired.co.uk/article/gchq-tempora-101> accessed 22 May 2022.
[68] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 22 May 2022.
[69] Raphael Satter, 'U.S. Court: Mass surveillance program exposed by Snowden was illegal' (*Reuters*, 2 Sepetember 2020) <https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK> accessed 22 May 2022.
[70] Committee on Legal Affairs and Human Rights, Council of Europe, *Draft Resolution on Mass Surveillance* (AS/Jur(2015) 01) 7.
[71] It is worthy to note that the Supreme Court has recently ruled in Carpentar v. United States (2018) 585 US that there is a reasonable expectation to privacy and that the encyclopaedic, exhaustic, and extensive chronicle of data collected and stored by telephone networks—which "give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers" contravenes that expectation.
[72] Dishfire, 'Overview' (*Dishfire*, 11 November 2018) <https://ldapwiki.com/wiki/DISHFIRE> accessed 2 May 2022; James Ball, 'NSA collects millions of text messages daily in 'untargeted' global sweep' (*The Guardian*, 16 January 2014) <https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep> accessed 2 May 2022.

1.3.3 Metadata Collection/Analysis

Metadata is data about data: it is the set of information that describes the qualities of a key piece of information: it excludes actual content and covers mainly the information that describes the actual content. For example, an actual content (e.g., an email) might include metadata, i.e., data about the time the email was sent, the network on which it was carried, the names of the sender(s) and recipient(s), the location from which it was sent, the computer model and IP address from which it was sent, and the language in which it was sent. Another easily comprehensible instance is when a file is created on a digital device. The file is the actual data but the timestamp (for the creation/modification of the file), ownership, file path in the data system, and file permissions (read, right, execute) are metadata about the file.

Incidental to and supplementing other surveillance methods (especially telephone surveillance), metadata surveillance can reveal the most intimate detail about the lives and livelihood of entire populations or persons of interest, especially because they are so detailed. In 2017 alone, the NSA declared in his transparency report[73] that it collected a staggering 534,396,285 call detail records (or telephone calls metadata), a form of surveillance that may now end in the US with the potential passage of the Safeguarding American's Private Records Act of 2020, which would effectively end the mass surveillance of communications metadata.[74]

1.3.4 Government Hacking

Potentially the most intrusive form of mass surveillance, hacking is the means of gaining unauthorized access to digital systems without consent. As a surveillance technique, it enables states—through their own armies of hackers or contractors—to remotely penetrate or access the digital devices. It also allows them to "manipulate data on [those] devices, by deleting, corrupting or planting data; recovering data that has been deleted; or adding or editing code to alter or add capabilities, all while erasing any trace of the intrusion".[75]

---

[73] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities* (Office of the Director of National Intelligence 2017).

[74] Human Rights Watch, 'US: End Bulk Data Collection Program' (*Human Rights Watch*, 5 March 2020) <https://www.hrw.org/news/2020/03/05/us-end-bulk-data-collection-program> accessed 22 May 2022; Jake Laperruque, 'The History and Future of Mass Metadata Surveillance' (*Pogo*, 11 June 2019) <https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/> accessed 24 May 2022; Jake Laperruque, 'It's Time to End the NSA's Metadata Collection Program' (*Wired*, 3 April 2019) <https://www.wired.com/story/wired-opinion-nsa-metadata-collection-program/> accessed 24 May 2022.

[75] Privacy International, 'Government Hacking' (*Privacy International)* <https://privacyinternational.org/learn/government-hacking> accessed 13 May 2022.

By targeting computers, smart TVs, self-driving cars, and the operating systems of mobile phones, states can "conduct novel forms of real-time surveillance, by covertly turning on a device's microphone, camera, or GPS-based locator technology, or by capturing continuous screenshots or seeing anything input into and output from the device".[76]

Government hacking is often carried out through the weakening or cracking of encryption (the technology that helps keep the confidentiality,[77] zero-knowledge,[78] and integrity proof properties of communications[79]); gaining access to and monitoring data sent through communication channels; and endpoint compromise (which facilitate ongoing surveillance through the use of malicious software, human engineering, and known systems exploits).[80] As complicated as all of this sounds, it is astounding to note what capabilities states have developed in this regard. The US affords a classic instance—when WikiLeaks disclosed the government's hacking capabilities in 2017, it noted that "the CIA's hacking division… had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other 'weaponized' malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook."[81]

1.3.5 Facial Recognition Technology ("FRT")

FRT is another extremely intrusive and dangerous technology. Enabling both overt and covert remote identification and categorization of persons of interest or entire groups without warrant or consent, FRT can be used to mine, retrieve, enhance, and analyse millions, possibly billions, of images. These images are usually collected from the World Wide Web, government databases, or airborne surveillance systems that facilitate mass geo-location tracking of pedestrians and vehicles' movement and enables the creation of a pattern-of-life data.

---

[76] Ibid.

[77] Encryption ensures that when a message is transmitted through a network, such as the internet, only the intended recipient of the message gets it. Encryption technology works by taking plain text, such an email, and turns it into what is essentially unreadable gibberish, such that even if that communication were to be intercepted by a third party, that third party would not be able to discover the actual content or meaning of the message.

[78] Zero-knowledge proof is a mathematical or encryption techniques that allows one party (the prover) to verify to another party (the verifier) that a statement is true without having to reveal any other information including the prover's identity. Zero-knowledge works because the prover must convince the verifier that the prover definitely has the answer by having to do something that can only be done by someone who definitely has the key to the answer.

[79] Integrity proof is an aspect of information security triage that is guaranteed by encryption technology. This works by ensuring and proving that a communication or data sent over a network has not been changed or altered in any way during the transmission process.

[80] Amie Stepanovich et al, 'A Human Rights Response to Government Hacking' (September 2016) Access Now <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf> accessed 23 June 2022

[81] WikiLeaks (n 25)

Through Snowden's disclosures, we now know that the NSA through its surveillance program, *Wellspring*, "exploit[ed] the flood of images included in emails, text messages, social media, videoconferences and other communications".[82] The very nature of covert surveillance means that it is difficult, if not impossible, to determine how many people could have been caught up in the NSA effort, but "[g]iven the N.S.A.'s foreign intelligence mission, much of the imagery would involve people overseas whose data was scooped up through cable taps, Internet hubs and satellite transmissions."[83]

Considering their surveillance capabilities and impact on basic human rights, especially when used indiscriminately or without appropriate safeguards, FRTs have always been a thing of interest for private companies who now invest billions of dollars into developing them. Consider, for instance, Clearview AI, a private software company that has come under increasing scrutiny and continues to face legal battles for its business model, which is built around scraping, without authorizations, publicly available web pages. Data collected by Clearview AI include billions of images, which are used to build and enhance the company's powerful facial recognition system/software, which software it then sells to governments and law enforcement agencies around the world.[84]

This chapter has depicted how privacy is currently being invaded by states and has offered insights into the technological means enabling the invasion. Through the Snowden disclosures and the examination of common state surveillance techniques, we have seen the nature and extent of state surveillance practices, many of which are yet to be adequately addressed under international law in a bid to ensure the relevance of the fundamental right to privacy in an era of constant surveillance.

[82] James Risen and Laura Poitras, 'N.S.A. Collecting Millions of Faces From Web Images' (*The New York Times,* 31 May 2014) <https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html> accessed 19 June 2022.
[83] Ibid.
[84] Ian Carlos Campbell, 'Clearview AI hit with sweeping legal complaints over controversial face scraping in Europe' (*The Verge,* 27 May 2021) <https://www.theverge.com/2021/5/27/22455446/clearview-ai-legal-privacy-complaint-privacy-international-facial-recognition-eu> accessed 21 May 2022; Office of the Privacy Commissioner of Canada, 'From state surveillance to surveillance capitalism: The evolution of privacy and the case for law reform' (*Office of the Privacy Commissioner of Canada Official Website,* 16 June 2021) <https://www.priv.gc.ca/en/opc-news/speeches/2021/sp-d_20210616/> accessed 21 May 2022.

Chapter 2

> "Shorn of the cloak of privacy that protects him, an individual becomes transparent and therefore manipulable. A manipulable individual is at the mercy of those who control the information held about him, and his freedom, which is often relative at best, shrinks in direct proportion to the extent of the nature of the options and alternatives which are left open to him by those who control the information".—Joseph Cannataci.[85]

2.1 Introduction

This chapter examines the two major arguments for justifying state surveillance: the value of security and the nothing to hide argument. By providing some insights into the rationalizations that states and individuals employ to validate and promote surveillance agenda, this chapter offers key context into the factors that have fuelled—and continues to fuel—the growth of state surveillance. The chapter also delineates the scope of privacy under consideration, which is important as the discourse in the chapters that follow sharply progresses into a distinct focus on the interplay between privacy, surveillance, and law.

2.2 The Value of Security

For governments all over the world, the central argument for surveillance—whether domestic or foreign and whether targeted or mass in nature—has always revolved around the value of security. Foreign surveillance, in particular, has been justified on the basis that the boundaries between national and global security have become fluid, and that it would be difficult to achieve one without the other. As one author observes, states have experienced and continue to experience interconnectedness with one another that makes cooperation not just important but also necessary. Summarizing the impact of this interdependence and how it is used to justify cooperation among states, Segun Osisanya has concluded that, "the security concerns of states are deeply interconnected to the point that one state's security needs cannot be realistically considered without taking into consideration the security needs of the other states".[86]

---

[85] Joseph Cannataci, *Privacy & Data Protection Law* (Norwegian University Press 1986) 60.

[86] Segun Osisanya, 'National Security versus Global Security' (*UN)* <https://www.un.org/en/chronicle/article/national-security-versus-global-security> accessed 13 June 2022.

Whether in the context of domestic or foreign surveillance, the security argument usually proceeds as follows: states have the responsibility to protect citizens from inside and outside threats, further the general sense of safety that people enjoy in their daily lives, and protect the values of freedom and democracy.[87] More recently, the argument has been made to encompass states' efforts to curb a pandemic and secure public health.[88] Owing to these responsibilities, therefore, states claim that they are justified in making massive investment in surveillance technologies,[89] even if constant surveillance might entail some future, probable harm, and even though there is no concrete evidence that mass surveillance actually works to improve security.[90]

The above argument, also supported by many individuals,[91] is common even in liberal, democratic societies. Take the United States, for example, where the four coordinated attacks of 11 September 2001 (9/11 attacks) were the inflection point for unprecedented augmentation of mass surveillance capabilities.[92]

---

[87] Council of the European Union, *Internal Security Strategy for the EU, Towards a European Security Model* (March 2010) 12.

[88] Victoria Kim, 'Who's watching? How governments used the pandemic to normalize surveillance' (*Los Angeles Times*, 9 December 2021) <https://www.latimes.com/world-nation/story/2021-12-09/the-pandemic-brought-heightened-surveillance-to-save-lives-is-it-here-to-stay> accessed 24 June 2022.

[89] The courts have also validated this argument in a number of cases. For example, in Appl. No. 37138/14 Szabó and Vissy v. Hungary (2016) ECHR, the European Court of Human Rights "accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents." And in Klass and Others v. Germany (1979) 2 EHRR 214, the same court held that, "democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction…"

[90] Jennifer Stisa Granick, 'Mass Spying Isn't Just Intrusive---It's Ineffective' (*Wired*, 2 March 2017) <https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/> accessed 4 May 2022. One may ask what the standard of success in this regard would be. While that is beyond the scope of this thesis, one may argue that some verifiable metrics of crimes averted or harms reduced through bulk surveillance might be something to show that resources and money invested have not gone to waste. As seen in Klayman v Obama (2015) No. 14-5004 D.C. Cir. below, it has been hard to promote any meaningful evidence in favour of bulk surveillance.

[91] Comments made by Gerald Walpin, who served as inspector general under President George W. Bush, captures the sentiment expressed by many individuals. Walpin once argued that, "[t]he NSA program is logical… Wouldn't you want our intelligence services to know who in the United States called those numbers and area codes and to examine the information to determine whether those calls were innocent or not? I certainly would" Walpin, G., 'We need NSA surveillance' (*National Review*, 16 August 2013). <http://www.nationalreview.com/article/355959/we-need-nsa-surveillancegerald-walpin> accessed 9 May 2022. Walpin even goes on to suggest that there would be no point in constraining the NSA's activities through civil or administrative oversight.

See also: James Stacey Taylor, 'In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance' (2005) 19 PAQ 227, 227 (From the same lens, James Stacey Taylor has argued that "rather than opposing [the expanding use of surveillance technology], its use should be *encouraged*—and not only in the public realm. Indeed, the State should place all of its citizens under surveillance at all times and in all places, including their offices, classrooms, shops—and even their bedrooms").

[92] Perhaps the most consequential of the measures taken following the 9/11 attacks was the hasty passing of the Patriot Act (An Act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes 2001), which among other things, expanded the US government's authority to collect unprecedented surveillance on both Americans and foreigners anywhere in the world.

Justifying the US' surveillance activities on the basis of the security argument, the former president of the United States, George W. Bush, once said, "first and foremost that he believes it was authorized by the Constitution under provisions of the Constitution that say that the chief executive has an obligation to protect the citizens of the United States".[93] According to the former president, in order to "effectively detect enemies hiding in our midst and prevent them from striking us again . . . we must be able to act fast and to detect conversations [made by individuals linked to al Qaeda] so we can prevent new attacks."[94] As the former president emphasized, "a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives."[95]

Echoing President Bush's sentiment almost a decade later, the former head of the NSA and CIA, Michael Hayden, noted during the Munk Debate of May 2014 that if the NSA had had the surveillance capabilities it now has, it would have been able to prevent or at least disrupt the 9/11 attacks. In his words, "… if we'd have had this program in place we would have known that Nawaf al-Hazmi and Khalid al-Mihdhar, two of the muscle guys on the plane planning to hit the Pentagon, were in San Diego".[96] And, perhaps most interestingly, a judge on the U.S. Court of Appeals for the 7th Circuit has lamented that the US must do better in terms of mass surveillance in the name of national security—"[t]he terrorist menace", Judge Richard Posner noted, "… grows every day. This is not only because al Qaeda likes to space its attacks, often by many years, but also because weapons of mass destruction are becoming ever more accessible to terrorist groups and individuals."[97]

Across the Atlantic, in the United Kingdom, the former Director of the Government Communication Headquarters ("GCHQ"), Sir Iain Robert Lobban, has described how mass surveillance carried out by the GCHQ has helped to enhance the detection of terrorist

---

[93] Renee Montagne, 'Bush Defends Surveillance Without Warrant' (*NPR*, 19 December 2005) <https://www.npr.org/templates/story/story.php?storyId=5061250> accessed 25 June 2022.

[94] See: Requesting the President and Directing the Secretary of Defense to Transmit to the House of Representatives All Information in the Possession of the President Or the Secretary of Defense Relating to the Collection of Intelligence Information Pertaining to Persons Inside the United States Without Obtaining Court-ordered Warrants Authorizing the Collection of Such Information and Relating to the Policy of the United States with Respect to the Gathering of Counterterrorism Intelligence Within the United States: Adverse Report of the Committee on Armed Services, House of Representatives, on H. Res. 645, United States. Congress. House. Committee on Armed Services, Washington: U.S. G.P.O. [For sale by the Supt. of Docs., U.S. G.P.O., Congressional Sales Office], 2006, 11. See also: US Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Department of Justice 2006).

[95] Ibid.

[96] Peter Munk, *Does State Spying Make us Safer: The Munk Debate on Mass Surveillance* (House of Anansi Press Inc 2014) 8.

[97] Richard A. Posner, 'Our Domestic Intelligence Crisis' (*The Washington Post*, 21 December 2005) <https://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html> accessed 21 May 2022.

communications, the thwarting of crimes, and the saving of lives.[98] In his words, "[t]here is a complex [mosaic] of strategic capabilities that allow [the GCHQ] to discover, process, investigate and then to take action. That uncovers terrorist cells. It reveals people shipping secrets, expertise or materials to do with chemical, biological and nuclear [sic] around the world…".[99]

2.2.1 Debunking the Security Argument

Many courts, experts, and policy makers have criticized the security argument. They claim that instead of guaranteeing or promoting security, state surveillance, particularly mass surveillance, actually damages security. For instance, the American cryptographer, Bruce Schneier has claimed that "... [i]n the years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obliged to investigate all the tips."[100] According to Schneier, state surveillance, especially of an untargeted or mass nature, produce many false positives, however well calibrated. Each alert requires a lengthy investigation, time and money is taken away; and intelligence officers are prevented from doing actual, productive, crime-prevention work. As Schneier aptly puts it, "when you're watching everything, you're not seeing anything."[101]

William Binney, a whistleblower and intelligence official who used to specialize in enabling government intelligence gathering—first as a Russia specialist during the Cold War, and later as co-founder/leader of the NSA SIGINT Automation Research Center—has echoed the same sentiment as Schneier. Binney thinks "[t]he bulk collection approach produces up to hundreds of thousands of false positives, burdens analysts, and distracts from the real and critical threats that need prioritising. The problem with bulk collection… is that it makes intelligence analysts dysfunctional by drowning them in data".[102] Rebutting the security argument and claiming that state surveillance technologies may actually jeopardize the very security they are built to

[98] David Irvine, the former Head of the Australian Security Intelligence Organisation ("ASIO") has also been quoted as saying regarding his push for broader surveillance powers for ASIO that, "[w]ithout our ability to access telecommunications call data and intercept communications [we] cannot guarantee the level of safety assurance that people expect…" Cited in Daniel Hurst, 'ASIO Spy Chief Defends Surveillance Network and Argues for Broader Powers' (*The Guardian*, 21 July 2014) <https://www.theguardian.com/world/2014/jul/21/asiospy-chief-defends-surveillence-network> accessed 2 July 2022.
[99] Intelligence and Security Committee of Parliament, *Uncorrected Transcript of Evidence: Given by Sir Iain Lobban, Director, Government Communication Headquarters; Mr Andrew Parker, Director General, Security Service; Sir John Sawers, Chief, Secret Intelligence Service* (Intelligence and Security Committee of Parliament 2013).
[100] Schneier (n 9) 161.
[101] Ibid.
[102] Joint Committee on the Draft Investigatory Powers Bill: Written Evidence (2015) 180.

enhance, Binney has also noted that state surveillance, especially mass or untargeted surveillance, "undermines security and has consistently resulted in loss of life in my country and elsewhere, from the 9/11 attacks to date. The net effect… is that people die first, even if historic records sometimes can provide additional information about the killers (who may be deceased by that time)."[103]

Apart from the fact that it sometimes produces the exact opposite effect intended, state surveillance, especially mass surveillance, is also difficult to support on the basis of security given its poor record of actually achieving its purpose. Put in other words, there is scant evidence that state surveillance actually helps to prevent crime and ensures safety, and judicial notice has been taken of this. In *Klayman v Obama*, for instance, the Court noted that, "To date, the [US] [g]overnment has still not cited a single instance in which telephone metadata analysis actually stopped an imminent attack, or otherwise aided the Government in achieving any time-sensitive objective". Buttressing their frustration regarding the government's inability to adduce any concrete evidence in favour of their surveillance programs, and their consequent inability to make a finding for the necessity of the programs in place, the Court mentioned further that "providing… examples of the [p]rogram's success would certainly [have] strengthen[ed] the [g]overnment's argument regarding the [p]rogram's efficacy."[104]

Even if one were to argue that state surveillance is worth operating because it might help prevent or respond to at least one security incidence, the problem is that the far-reaching consequences of state surveillance far outweigh any immediate benefits. Warning against the potential harm of states increasing surveillance activities, US Supreme Court Justice William O. Douglas once said,

> … The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the

[103] Ibid.
[104] (2015) DDC 13-851 RJL.

> safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.[105]

With the present level of state surveillance going on, it seems as though we are slowly getting to the world described by Justice Douglas above.

2.3 The Nothing to Hide Argument

For some states and individuals, the central justification of state surveillance is expressed mainly through sentiments captured in the now-popular nothing to hide argument. To express the argument, some reason that if one has done nothing wrong—and so, have nothing to hide—it does not really matter if one's activities are constantly monitored or if the government indiscriminately collects data about one, because the government will not find anything incriminating anyway. And because the government will not find anything, one has nothing to fear.

In its more compelling variants, the nothing to hide argument is made in a more general sense: it is recast to advance the view that those who engage in unlawful or illicit activities, and therefore, have things to hide, have no legitimate claim to secrecy. On the other hand, those who abide by the law should have nothing to hide and should, therefore, not mind being under constant surveillance.[106] In any case, "[t]he vast majority of citizens go through their daily lives believing that surveillance processes are not directed at them, but at the miscreants and wrongdoers [and] [f]or all the evidence that the monitoring of individual behaviour has become routine and everyday, the dominant orientation is that mechanisms of surveillance are directed at others."[107]

In its most compelling form, the nothing to hide argument bears deep relationship with the security argument examined above. The argument balances the value of secrecy, of being left alone by the state, with the state's wildly important interest in maintaining security. Professor Daniel Solove restates the most compelling version of the argument thus:

> … the nothing to hide argument proceeds as follows: The NSA surveillance, data mining, or other government information-gathering programs will result in the disclosure of particular pieces of information to a few government officials, or perhaps only to

[105] Osborn v. United States (1966) 385 U.S. 323.
[106] See generally: Daniel J. Solove, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 44 SDLR 745 (Yale University Press 2007); Timothy Casey, 'The Value of Deviance: Understanding Contextual Privacy' (2019) 51 LUCLJ 65.
[107] Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance*, (The MIT Press 2008) 97 and 98.

> government computers. This very limited disclosure of the particular information involved is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information. Although there may be some cases in which the information might be sensitive or embarrassing to law-abiding citizens, the limited disclosure lessens the threat to privacy. Moreover, the security interest in detecting, investigating, and preventing terrorist attacks is very high and outweighs whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information. Cast in this manner, the nothing to hide argument is a formidable one. It balances the degree to which an individual's privacy is compromised by the limited disclosure of certain information against potent national security interests. Under such a balancing scheme, it is quite difficult for privacy to prevail.[108]

2.3.1 Debunking the Nothing to Hide Argument

Experts have also exposed the inadequacies in the reasoning forming the basis of this argument. Perhaps one of the most famous retorts to the nothing to hide argument was made by Snowden himself when he noted that the driving force behind the nothing to hide argument is a lack of understanding of how human rights work. According to Snowden, "[a]rguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say". Snowden argues that even if a significant segment of the population do not understand or care about their fundamental human rights, that does not constitute a license to give away other people's rights: in other words, "the majority cannot vote away the natural rights of the minority."[109]

In his paper, *"I've Got Nothing to Hide and Other Misunderstandings of Privacy",* Daniel Solove, law professor at George Washington University, has also attempted to debunk the nothing to hide argument. In doing this, Solove first acknowledges the power and formidability of the nothing to hide argument, introduces the various formulations of the argument in their strongest forms, and tries to (re)conceptualise privacy.[110] According to Solove, the underlying issue with the argument is its conception of privacy as secrecy, as having wrongs to hide.[111] This is a myopic view that does not take into consideration the plurality of related interests and

---

[108] Solove (n 106)

[109] Sophie Kleeman, 'In One Quote, Snowden Just Destroyed the Biggest Myth About Privacy' (*Mic,* 29 May 2015) <https://www.mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for> accessed 24 May 2022.

[110] Unfortunately, despite Solove's best effort, the nothing to hide argument remains a common refrain. Part of the problem, as Solove explained, is that privacy concerns remain hidden, and it is difficult to protect or even define something that is obscured— Solove (n 106)

[111] Solove (n 106)

concerns that privacy addresses.[112] Crucially, the argument misses the point that privacy is about control and values and the balancing of interests; it is about accountability and the responsible use of power and privilege.[113]

But even if we were to admit that privacy is about secrecy, and that one does not care about secrecy, the question is whether one's thinking would remain unchanged even in instances where one's life—as a soldier in a battlefield, a child used as a sex slave, or a journalist uncovering a sensitive story—depends on the ability to send encrypted communications in a situation of grave danger where one's assailant might be listening on what one is saying or trying to say?

On a different note, the nothing to hide argument also draws undue strength from a poor understanding and description of the relationship between privacy and security—i.e., the argument gives the security of many an upper hand over the privacy of each. Yet, the value of protecting the individual is a social one;[114] and privacy, therefore, is a social interest. As paradoxical as it sounds, one might even claim that one of the things that makes a society work is the right to retreat into oneself and one's space, and avoid unwanted intrusiveness from time to time. As Solove puts it, "a society without privacy protection would be suffocating, and it might not be a place in which most would want to live. Thus, even when it protects the individual, privacy does so for the sake of society."[115] Solove concludes his arguments on the baselessness of the nothing to hide claim by noting that:

> When the nothing to hide argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the debate to its terms, then draws power from its unfair advantage… The nothing to hide argument speaks to some problems but not to others. It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised with government security measures. When engaged directly, the nothing to hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing to hide argument, in the end, has nothing to say.[116]

[112] Ibid.
[113] Ibid.
[114] Of course, the value of protecting the majority is a social one as well. However, we already take this for granted, hence the emphasis here on the individual.
[115] Solove (n 106).
[116] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press 2011) 32.

Finally, in Timothy Casey's *"The Value of Deviance: Understanding Contextual Privacy"*, Casey takes a somewhat different approach. He attempts to rebut the nothing to hide argument by defining 'privacy concerns' in a non-binary, contextual way, where the key emphases revolve around the fact that we shape our identities through a contextual disclosure of our data (or information about our lives) and we desire to have some control over the way those disclosures are made. In other words, "[we] gain value in self-preservation and self-promotion through a nuanced and contextual disclosure of personal information", and without the choice to shape our identities, our humanity is deeply impacted and we cannot be free to be ourselves. As one scholar writes:

> Everyone needs some room to break social norms, to engage in small "permissible deviations" that help define a person's individuality. People need to be able to think outrageous thoughts, make scandalous statements and pick their noses once in a while. They need to be able to behave in ways that are not dictated to them by the surrounding society. If every appearance, action, word and thought of theirs is captured and posted on a social network visible to the rest of the world, they lose that freedom to be themselves… This ability to develop one's unique individuality is especially important in a democracy, which values and depends on creativity, nonconformism and the free interchange of diverse ideas.[117]

2.4 On the Implications of State Surveillance for Privacy

Surveillance can have damaging effects on privacy. Of course, surveillance affects a host of other rights too, and the focus on privacy in this section is not intended to take away from that fact. Noting this from the outset is important because one runs the risk of making the general, multi-phenomenal impacts of "… surveillance seem less significant than they are and hence set the criteria upon which it is decided whether surveillance is appropriate or legitimate, too low"[118] by focusing only on privacy. As leading historian, Quentin Skinner once said: "[t]he

[117] Michael McFarland S.J., 'Why We Care about Privacy' (Markkula Center for Applied Ethics, 1 June 2012) <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/> accessed 6 July 2022. See also: Ruth Coustick-Deal, 'Responding To "Nothing To Hide, Nothing To Fear"' (*Open Rights Group (ORG)*, 4 December 2015) <https://www.openrightsgroup.org/blog/responding-to-nothing-to-hide-nothing-to-fear/> accessed 6 July 2022; Adam Kingsmith, 'Data Privacy Day 2014: Think you have nothing to hide? Think again' (*Canadian Journalists for Free Expression (CJFE)*, 27 January 2014) <https://www.cjfe.org/resources/features/data-privacy-day-2014> accessed 6 July 2022

[118] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate' (2016) JCP 252

response of those who are worried about surveillance has so far been too much couched, it seems to me, in terms of the violation of the right to privacy".[119]

While Skinner is right to argue that the very existence of surveillance powers endangers liberty itself,[120]the reason many analyses, including the present one, focus on privacy when assessing state surveillance impact is "partly because privacy underpins [many] other rights… and partly because of the nature of the internet and how we now use it".[121]

This thesis also focuses on privacy because of its centrality of privacy in the human rights system.[122] As commonly conceptualized, privacy is necessarily connected to other civil liberties, and, where privacy is lost, we lose a host of other rights including the freedoms of association, expression, thought, conscience, and religion.[123] Suddenly, it becomes difficult or impossible for us to join groups, movements, or assemblies;[124] and our abilities to form independent opinions, to refuse to conform, or to develop radical thoughts are also deeply impacted. After all, "*[t]o lose control of one's personal information is in some measure to lose control of one's life and one's dignity*."[125]

To truly understand how state surveillance affects privacy, we must necessarily agree on what we mean by privacy, since privacy is a constantly evolving concept that means different things to different people and in different contexts. Understanding what we mean by privacy also helps comprehend the scope of other discussion in this thesis, including especially the limitations of current international law discussed in chapter 4.

2.4.1 Our Present Conception of Privacy

---

[119] Richard Marshall and Quentin Skinner, 'Liberty, Liberalism and Surveillance: a historic overview' *(OpenDemocracy*, 26 July 2013) <https://www.opendemocracy.net/en/opendemocracyuk/liberty-liberalism-and-surveillance-historic-overview/> accessed 3 July 2022.

[120] Ibid.

[121] Bernal (n 118) 252

[122] In fact, privacy is so important to other human rights that the UN has recognized that privacy enable[s] the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life…" UN General Assembly, 'The right to privacy in the digital age' (7 April 2017) 34th Session A/HRC/RES/34/7. See also: Office of the Privacy Commissioner of Canada, 'International privacy guardians urge legislators to reaffirm commitment to privacy as a right and value in itself' (*Office of the Privacy Commissioner of Canada Official Website*, 28 October 2019) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191028/> accessed 13 July 2022. (emphasis added).

[123] For an excellent analysis on how surveillance affects privacy and other human rights, see generally: Bernal (n 114).

[124] In China, the identities of people attending religious assemblies or houses of worship are recorded through surveillance cameras in order to repress certain religious beliefs and "authorities have also collected biometric information—including blood samples, voice recordings, and fingerprints—from religious and faith communities, often without their consent"—Dominic J. Nardi, 'Religious Freedom in China's High-Tech Surveillance State' (*United States Commission on International Religious Freedom Official Website*, September 2019) <https://www.uscirf.gov/countries/china/religious-freedom-chinas-high-tech-surveillance-state> accessed 29 July 2022.

[125] McFarland (n 117). (emphasis added). See also: Dr Ilia Siatitsa, 'Digital Rights are Human Rights' (*Digital Freedom Fund)* <https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/> accessed 12 July 2022.

As we now understand it, privacy is a relatively modern invention that continues to prove elusive in terms of both definition and description. Just about everyone—lawyers, legislators, business leaders, and scholars across disciplines—who has devoted some time to its study or analysis agrees that privacy is difficult to define. As a concept, it suffers from a great deal of indeterminateness, being "a highly subjective notion, whose interpretation changes over time and space."[126] Scholars like Daniel Solove even asserts that nobody can articulate the meaning of privacy.[127] According to him, privacy is "a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[128]

Professor Daniel Solove is not alone. Philosopher of law, Judith Jarvis Thomson once wrote about the right to privacy that, "the most striking thing about [it] is that nobody seems to have any very clear idea what it is."[129] Legal theorist Robert Post has observed that: "[p]rivacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[130] And American professor, lawyer, and philosopher, Kenneth Einar Himma has written that, "[w]hat exactly privacy is, what interests it encompasses, and why it deserves legal protection, are three of the most contentious issues in theorizing about information ethics and legal theory".[131] In her celebrated work on privacy, Helen Nissenbaum, professor of information science at Cornell Tech echoes the same sentiments as Judith Jarvis and Robert Post. According to her:

> Almost as many who have taken up the subject of privacy… have declared it deeply problematic, referring not only to questions and disagreements about its value, benefits, and harms but to its conceptual morass. Attempts to define it have been notoriously controversial and have been accused of vagueness and internal inconsistency-of being overly inclusive, excessively narrow, or insufficiently distinct from other value concepts… [132]

[126] Colin J Bennett, *Regulating Privacy* (Cornell University Press 1992) 13.
[127] Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008) 1.
[128] Ibid.
[129] Judith Jarvis Thomson, 'The Right to Privacy' (1975) 4 PPA 295, 295.
[130] Robert C. Post, 'Three Concepts of Privacy' (2001) 89 GLJ 2087, 2087.
[131] Kenneth Einar Himma, 'Privacy Versus Security: Why Privacy is Not an Absolute Value or Right' (2007) 44 SDLR 857, 860.
[132] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009).

Despite the obvious challenge of defining the wide and multidimensional field of privacy, some scholars have undertaken the difficult task of (re)conceptualizing privacy in order to help bring some contexts, clarity, and colour to it. From William Prosser, Alan Westin and Daniel Solove to Jerry Kang and Ken Gormley, attempts have been made to develop taxonomies of privacy that are quite useful and instructive.[133] To offer some insight, I shall briefly discuss three of these taxonomies.

In 1960, US scholar, William L. Prosser identified four different privacy interests: the intrusion upon a person's solitude or seclusion; the appropriation, for commercial purposes, of a person's name, likeness, or personality; the public disclosure of embarrassing private facts about a person; and the publicity that places a person in a false light in the public eye. However, because Prosser focused solely on privacy tort in common law, his taxonomy has been heavily criticized by Edward Bloustein for reducing the right to privacy to "a mere shell of what it has pretended to be".[134] According to Bloustein: "If Dean Prosser is correct, there is no 'new tort' of invasion of privacy, there are rather only new ways of committing 'old torts.' And, if he is right, the social value… we call privacy is not an independent one, but is only a composite of the value our society places on protecting mental tranquillity, reputation and intangible forms of property".[135]

In *Privacy and Freedom*, published in 1967 following a formal inquiry into the question of privacy and computerization in the US, Alan Westin identified four categories of privacy: (1) solitude; (2) intimacy; (3) anonymity; and (4) reserve ("the creation of a psychological barrier against unwanted intrusion").[136]. Unfortunately, while his "account of privacy placed information at its very core"[137] and his definition was clearly "conceived in light of the advent of computerisation",[138] Westin's classification "focus [sic] mostly on spatial distance and separateness; they fail to capture the many different dimensions of informational privacy".[139]

More recently, in the early 2000's, Daniel Solove also attempted a classification of privacy in a journal article published in 2006 and made popular in his 2008 book: *Understanding*

[133] As will be seen, these taxonomies have been criticized, by proponent themselves and other scholars, as stretching the scope of privacy beyond any graspable, comprehensible form.
[134] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 NYULR 962
[135] Ibid.
[136] Alan F. Westin, *Privacy and Freedom* (IG Publishing 1970).
[137] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Science & Business 2014) 31.
[138] Ibid.
[139] Westin (n 136).

Privacy[140]. According to him, privacy (concerns) can be categorized into (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion. However, Solove's taxonomy also suffers from incomprehensiveness: his attempt exempts matters and activities that are culturally contextual. In his own words, "all taxonomies are generalizations based upon a particular focus, and they are valuable only insofar as they are useful."[141] As such, Solove concludes that "the entire 'privacy equation' must be worked out in each particular case… ".[142]

The thing with taxonomies is: while they make it easier to grasp the scope of privacy and to discuss it in a meaningful way, they are also limited in certain respects, and, thus, cannot aid the establishment of a comprehensive, all-inclusive meaning of privacy. Despite the work already done by theorists such as Alan Westin and William L. Prosser, Solove was probably right, when he observed that "the quest for a singular essence of privacy leads to a dead end"[143]. Given this context, one also understands Solove's resignation when he declared what is now intuitively clear: "[t]here is no overarching conception of privacy".[144]

However, while it may be difficult to truly capture the essence of privacy both as a concept and as a fundamental human right, nothing impedes one from addressing crucial and substantive questions regarding privacy as long as it is possible to carve out relevant aspect or aspects of it. To be sure, it has become common for scholars and experts who do not want to commit the proper-meaning fallacy to define, in their own words, only a dimension of privacy relevant to their immediate scope of enquiry, as opposed to attempting a natural meaning or all-encompassing overview of the term.

The most useful way to address privacy and to sidestep unreachable precisions, normative assumptions, and definitional exactness, therefore, seems to be to settle on those key contextual concerns that relate to one's immediate analysis by understanding what, in given contexts, constitute privacy concerns, since privacy is context- and fact-dependent.[145] Based on that understanding, it is important to note that this thesis is concerned only with digital privacy; and

[140] Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 UPLR 477.
[141] Ibid.
[142] Ibid.
[143] Ibid.
[144] Ibid.
[145] See for example: Ken Gormley, 'One Hundred Years of Privacy' (1992) 5 WLR 1335; Jerry Kang, 'Information Privacy in Cyberspace Transactions' (2004) 50 SLR 1193. See generally also: Gareth Crossman et al., *Overlooked: Surveillance and Personal Privacy in Modern Britain* (The Nuffield Foundation 2007).

throughout the rest of this thesis, unless otherwise indicated, the word 'privacy' is used interchangeably with 'digital privacy'.

By digital privacy, I mean the distinct but related sub-categories of information (or informational or data) privacy, communications privacy, and individual privacy. Together, these form the 'taxonomy' within which boundaries the rest of this thesis proceeds. For the purpose of clarity, information privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[146] Communications privacy is about the right of individuals to communicate digital data or information securely, and without interruption by a third party. In other words, communications privacy entails the confidentiality of mail, telephones, e-mail and other forms of communication. And individual privacy is the right of individuals to access the internet[147], transfer or receive digital information anonymously, without the information being tracked or surveilled. In other words, individual privacy is about the use of tools to ensure anonymity and the use of encryption technology, such that no one can track one's digital footprint, and even where one's information is somehow intercepted, such interception effort would be fruitless as the interceptor would be unable to decipher the information.

2.4.2 How State Surveillance Affects Privacy

Whenever we post on social media, shop online, subscribe to a newsletter, or use digital navigation services, we make ourselves visible. We are also constantly leaving a digital record of ourselves; a trail of information about us, which, when put together, can reveal a detailed diary of our lives when we perform daily, routine activities and interact with the world around us. Even when we are deeply asleep, we are still on the radar, as our mobile phones and devices constantly communicate with the nearest communication towers, and broadcast our location to anyone that is listening. And when our mobile devices are not trying to communicate with cell tower—which is really never—the mobile applications we use share our location anyway, with some broadcasting "as many as 200 individually time-stamped location data points within a

[146] Westin (n 135).
[147] Express Web Desk, 'Right to access internet is part of RTE and right to privacy: Kerala High Court' (*Indian Express*, 19 September 2019) <https://indianexpress.com/article/india/right-to-access-internet-part-of-rte-right-to-privacy-kerala-high-court-6011227/> accessed 23 August 2022.

12-hour interval."[148] This perpetual broadcast is happening even when our devices' locations are turned off.[149]

Especially when combined with other categories of data, such as our telephone and internet communications, browsing records and preferences, our mobility data "reveal habits, preferences and tastes – and can uncover, to a reasonable probability, religion, sexual preferences, political leanings and more. It can dig deep into personal lives."[150] Not only can data about us reveal facts about us, it can also offer acute glimpses into our tendencies, as the aggregation and analysis of our data with massive data sets can expose our inclinations with almost mathematical exactness.[151]

As intrusive as all of this can get, what is really terrifying is that data about us are readily accessible to law enforcement or intelligence agencies in many countries either through direct bulk collection or through data retention laws that mandate companies to retain bulk data and grant access to the state when required. Once accessed, these data can be processed or analysed using highly sophisticated surveillance systems.

When we lose our privacy this way, we lose a part of ourselves. We lose what makes us human, because when we feel as though we are no longer able to lead private lives, we tend to inhibit our agency and adjust our behaviour: we are less likely to speak freely, engage fearlessly, express dissent, or volunteer unpopular opinions.

The effect of state surveillance activities on privacy is as potent even when it is only felt, as opposed to being real;[152] i.e., when we merely perceive that we are being watched or monitored.[153] Yet because most forms of state surveillance are often carried out in secret, we can never know when we are being watched, and so we must live our lives under the assumption that we are constantly being watched: this way, we become a ruler of ourselves for the sake of

[148] Judge Herbert B. Dixon Jr. (Ret.), 'Your Cell Phone Is a Spy!' (*American Bar Association*, 29 July 2020) <https://www.americanbar.org/groups/judicial/publications/judges_journal/2020/summer/your-cell-phone-a-spy/#3> accessed 19 August 2022. See also: Stuart A. Thompson and Charlie Warzel, 'Twelve Million Phones, One Dataset, Zero Privacy' (*The New York Times*, 19 December 2019) <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> accessed 19 August 2022.

[149] Josh Lake, 'How your mobile phone tracks you (even when switched off)' (*Comparitech*, 25 November 2020) <https://www.comparitech.com/blog/vpn-privacy/stop-mobile-phone-tracking/> accessed 3 August 2022.

[150] Bernal (n 118) 253.

[151] Ibid.

[152] This is known as the 'Panopticon Effect', and is now used to describe a situation in which surveillance has become a central watchtower from which states may or may not be monitoring our activities in the real and digital world.

[153] UN General Assembly, 'The right to privacy in the digital age' (30 June 2014) 27th Session A/HRC/27/37.

another; we become the lord of our own enslavement.[154] As George Orwell described the situation in *Nineteen Eighty-Four*:

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[155]

Orwell's frightening vision seems to have become reality. Consider the US, for instance, where the Muslim society has faced profound backlash and surveillance since the 9/11 attacks.[156] Research shows that, due to real or perceived acts of state surveillance, many Muslims feel as if they have lost their privacy; many have also "modified aspects of their daily lives to avoid harassment or suspicion".[157] And although it has been two decades since the 9/11 attacks and some of the surveillance programs that were built immediately after the attacks have been dismantled following the Snowden revelations, the chilling effects of surveillance on US Muslims' exercise of basic rights still remain till today.[158]

For a comprehensive understanding of state surveillance impact on privacy, we must move beyond evaluations that limit their analyses to communications/correspondence surveillance only,[159] and consider the fact that state surveillance affects other aspects of privacy captured in our digital privacy taxonomy: i.e., individual, communications, and data/informational privacy.

---

[154] As counterintuitive as it would sound, one may even argue that it is not even the secret nature of surveillance, per se, that makes it so bad; it is the secret nature of laws enabling and governing surveillance and the secret interpretation of those laws. Secret laws and secret interpretations often entails the risk of inadequate oversight and responsibility. A classic instance is afforded by a 2019 investigation by the US Justice Department Inspector General Michael Horowitz, which "documented 17 significant inaccuracies and omissions in the [FBI's] applications to the [secretive Foreign Intelligence Surveillance Court, before whom there is no adversarial process] to wiretap [Carter] Page", a former aide to the former US President Donald Trump. Commenting on the investigation report, Elizabeth Goitein, the co-director of the Liberty and National Security program at the Brennan Center for Justice has said that, "[w]hat we have to worry about is that the system is so secretive and so one-sided — where the FISA Court hears only from the government — that these kinds of distortions can go undetected" (See: Ryan Lucas, 'Scathing Report Puts Secret FISA Court Into The Spotlight. Will Congress Act?' (*NPR*, 22 December 2019) <https://www.npr.org/2019/12/22/790281142/scathing-report-puts-secret-fisa-court-into-the-spotlight-will-congress-act> accessed 12 June 2022.

[155] George Orwell, *Nineteen Eighty-Four* (London: Penguin 2008) 4-5.

[156] Dawinder S. Sidhu, 'The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans' (2007) 7 University of Maryland Law Journal of Race, Religion, Gender and Class 375.

[157] Ibid.

[158] Lisa Lambert, 'Polling calls to U.S. Muslims raise surveillance fears' (*Reuters*, 24 November 2016) <https://www.reuters.com/article/us-usa-muslims-idUSKBN13I2PK> accessed 9 June 2022.

[159] See, for example, Eliza Watt, 'The right to privacy and the future of mass surveillance' (2017) 21 IJHR 773; Lubin (n 11); Monika Zalnieriute, 'An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance' (2015) 0 IJLIT 1. Also, see: UN General Assembly (n 20); UN General Assembly (n 153).

Regarding individual privacy, for instance, many states have monitored or shown the tendency to monitor individuals' activities on the internet. Measures put in place to monitor online activities extend from mere surveillance of citizens' communications to using social media to promote states' agenda and application-level or content censorship. Despite the devastating consequences[160] of these actions, states across different regions of the world engage in them anyway. In fact, since 2016, there have been "at least 768 government-ordered internet disruptions in more than 60 countries."[161]

In a different, but somewhat related way, individual (and communications) privacy can also be jeopardized by state surveillance when states seek to gain access to encrypted correspondence, restricts anonymous communications, and collect users' data. To achieve this goal, many states have engaged in disturbing campaigns to misinform the public.[162] In a bid to end encryption states have passed laws or prepared draft legislation allowing them to break down encryption. Thus, in 2018, Australia passed the first anti-encryption law in the world. The law allows the state, through its enforcement/intelligence agencies, to access users' information and data on any digital device. The legislation has drawn "fierce opposition from privacy experts and tech industry players, who warned that undermining encryption could compromise the privacy and security of millions of people worldwide".[163]

Also, in December 2020, an omnibus bill was signed into law in Kenya. Known as *The Statute Law Miscellaneous Amendment Act*, this law empowers the Cabinet Secretary of Interior and Coordination of National Security to access data from any phone or computer.[164] Anyone who refuses to comply with the new law risks a one-year prison term, a fine of one million shillings,

[160] UN General Assembly, 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights' (13 May 2022) 50th Session A/HRC/50/55.
[161] UN, 'Internet shutdowns now 'entrenched' in certain regions, rights council hears' (*UN Official Website*, 1 July 2021) <https://news.un.org/en/story/2021/07/1095142> accessed 7 June 2022.
[162] Joe Mullin, 'The U.K. Paid $724,000 For A Creepy Campaign To Convince People That Encryption is Bad. It Won't Work' (*Electronic Frontier Foundation*, 21 January 2022) <https://www.eff.org/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work> accessed 25 June 2022.
[163] John Power, 'Australia's early plans for 'dangerous' encryption law revealed' (*Aljazeera*, 5 April 2022) <https://www.aljazeera.com/news/2022/4/5/australias-dangerous-encryption-law-in-works-in-2015-document#:~:text=Australia%20in%202018%20passed%20world,a%20target's%20computer%20or%20phone> accessed 16 June 2022.
[164] The Statute Law (Miscellaneous Amendments) Bill, 2020, Kenya Gazette Supplement No. 89 (National Assembly Bills No. 15), Parliament of Kenya, http://www.parliament.go.ke/index.php/node/12423; Emmanuel Paul, 'Kenyan government takes another shot at infringing privacy and digital rights' (*Techpoint Africa*, 17 December 2020) <https://techpoint.africa/2020/12/17/kenya-private-data/> accessed 16 June 2022.

or both.[165] Commentators have called this legislation constitute a "sneak attack on the right to privacy".[166]

Information privacy can also be negatively impacted where state surveillance affects people's choice to determine when, how, and to whom they want to make their information available. One of the most striking manifestation of this can be seen in states' tendency to create and maintain massive digital databanks where personal and often sensitive data about citizens are stored. In 2005, the Thailand Cabinet approved a smart card initiative designed to hold information such as the card holder's name, date of birth, health conditions, social security, insurance, and taxation data, biometric images (fingerprints, face and iris), etc. Also in Nigeria, mass data collection remains a major threat, with at least "six government agencies maintain[ing] different biometric data points on citizens and residents at federal and state level".[167]

This tendency to build digital databases has become more obvious during the COVID-19 pandemic as governments across the world scramble to curb the spread of the virus. In Argentina, for example, people were required, during the height of the pandemic, to use a mobile health application in which they entered personal information like their national identification numbers and email addresses. The Colombian app asks people to provide their data and answer questions about participation at protests and ethnicity."[168] And in South Africa, anxieties around mass collection of personal and sensitive data through contact tracing applications and lack of adequate security measures,[169] have also been highlighted.[170]

The problem with the creation of massive databanks is that it makes both targeted and mass surveillance really easy and tempting. Consider, for example, how in January 2022, news broke that the Public Health Agency of Canada had secretly accessed location data from 33 million

---

[165] Bridget Andere, 'Kenya's sneak attack on privacy: changes to the law allow government access to phone and computer data' (*AccessNow*, 27 January 2021) <https://www.accessnow.org/kenya-right-to-privacy/> accessed 19 June 2022.
[166] Ibid.
[167] Ridwan Oloyede, 'Surveillance Law in Africa: A review of six countries (Nigeria Country Report)' Institute of Development Studies 102, 104.
[168] Privacy International, 'Apps and COVID 19' (*Privacy International)* <https://privacyinternational.org/examples/apps-and-covid-19> accessed 4 July 2022.
[169] Speaking of adequate security measures, a study of 17 Android mobile contact tracing apps from 17 different countries has found that most government-sponsored contact tracing apps are insecure and risk exposing users' privacy and data. See: Privacy International, 'Most contact tracing apps fail at privacy and security' (*Privacy International*, 25 June 2020*)* <https://privacyinternational.org/examples/4229/most-contact-tracing-apps-fail-privacy-and-security> accessed 4 July 2022.
[170] See e.g., Amanda Manyame, 'Data protection in the age of technology-based disease surveillance' (*African Internet Rights)* <https://africaninternetrights.org/sites/default/files/Amanda_Manyame-1_1.pdf> accessed 5 July 2022. See also: Gabriella Razzano, 'Privacy and the pandemic: An African response' surveillance' (*African Internet Rights)* <https://africaninternetrights.org/sites/default/files/Gabriella_Razzano_1.pdf> accessed 6 July 2022.

mobile devices to monitor people's movement during lockdown.[171] Commenting on the issue, David Lyon, author of *Pandemic Surveillance* and former director of the Surveillance Studies Centre at Queen's University, believes that "[t]he pandemic has created opportunities for a massive surveillance surge on many levels [and] [e]vidence is coming in from many sources, from countries around the world, that what was seen as a huge surveillance surge—post 9/11—is now completely upstaged by pandemic surveillance".[172] It will be interesting to see how things play out, particularly in terms of how the pandemic changes the face of state surveillance.

[171] Bryan Short, 'How the federal government failed to protect our mobility data' (*Open Media*, 2 May 2022) <https://openmedia.org/article/item/how-the-federal-government-failed-to-protect-our-mobility-data> accessed 6 July 2022.
[172] Swikar Oli, 'Canada's public health agency admits it tracked 33 million mobile devices during lockdown' (*National Post,* 24 December 2021) <https://nationalpost.com/news/canada/canadas-public-health-agency-admits-it-tracked-33-million-mobile-devices-during-lockdown> accessed 7 July 2022.

Chapter 3

3.1 Introduction

In this chapter, key international instruments guaranteeing the right to privacy are considered. It is noted here that since privacy guarantees are not absolute, they can be curtailed in certain circumstances, including where states have to conduct surveillance for legitimate purposes. However, when conducting surveillance, certain principles have evolved to guide how states can go about their surveillance activities without jeopardizing privacy. In this chapter, we get a sense of how privacy is currently protected under current international law and the limitations that apply to the right.

3.2 Privacy, State Surveillance, and International Law

The establishment of the UN in 1945 marked the beginning of the modern international regime to protect human rights, including the right to privacy. Before 1945, however, many states protected aspects of privacy, whether explicitly in their constitutions or implicitly by courts reading the existence of the right to privacy into relevant provisions.[173] I say 'aspects' of privacy because no state constitution, national legislation, or code protected privacy as a unitary right and it was international law that first protected the general, unitary right to privacy.[174]

[173] To buttress this assertion, consider, for example, the early developments in the United States of privacy jurisprudence, which is reflected in key judicial decisions, where the Courts found that, although the Constitution does not explicitly guarantee the right to privacy, the Constitution does provide for a right to privacy in its First, Third, Fourth, and Fifth amendments. Thus, in Griswold v. Connecticut (1965) 381 U.S. 479, the United States' Supreme Court first recognized the right to privacy, albeit construed, narrowly, as one for married couples, and only with regard to the right to purchase contraceptives. In Eisenstadt v Baird (1972) 405 U.S. 438, the Supreme Court decided to extend the right to possess contraception to unmarried couples on the same basis as married couples. And then in Roe v Wade (1973) 410 U.S. 113, the Supreme Court used the right to privacy, as derived from the Fourteenth Amendment, to extend the concept of privacy to encompass a woman's right to have an abortion. (Roe v Wade has now been overturned, in an unpopular decision that has been criticised all over the world for taking human rights back to the Stone Age, and sparked protests across the United States. See: Maureen Chowdhury, Mike Hayes and Amir Vera, 'Roe v. Wade news' (*CNN*, 26 June 2022) <https://www.cnn.com/politics/live-news/abortion-roe-wade-supreme-court-06-26-22/index.html> accessed 7 July 2022.

Consider also the situation in Canada where although there is no explicit guarantee in the Constitution, privacy has been elevated to a quasi-constitutional status as the courts have interpreted Sections 2b, 7, and 8 of the Canadian Charter of Rights and Freedoms (on freedom of expression; right to life, liberty, and security of the person; and freedom from unreasonable search or seizure respectively) as protecting the right to privacy. For a comprehensive discussion, see generally: Barbara von Tigerstrom, *Information and Privacy Law in Canada* (Irwin Law Inc, 2020).

[174] Oliver Diggelmann and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 HRLR 441.

And so, as we will see below, many of the key international instruments simply choose to protect people against "arbitrary interference with [their] privacy".[175]

While evidence suggests that protecting privacy as a unitary concept was not done on purpose,[176] a unitary right has nevertheless proven to be a generally helpful thing as it "supplies a highly abstract framework, one with deep philosophical elements, around which a complete… cosmology of… [different privacy concerns] has been constructed".[177] Indeed, the recognition of privacy as a unitary right has allowed for the broad and boundless application of privacy provisions in international human rights instruments and permitted people to bring a wide range of relevant claims under the right privacy. Examples include the monitoring of employees' computer use,[178] and the recording of suspects' voices at a police station,[179] to a soldier's inability to access their health record even though they had been made to participate in mustard and nerve gas tests conducted under the auspices of the British Armed Forces.[180]

However, the creation of privacy as a unitary right also creates unique problems. One major and immediately obvious one is that by covering everything, privacy as a unitary right covers nothing in particular. And while it was wise to offer an umbrella protection decades ago when the idea of privacy itself was not fully formulated and technology had not introduced peculiar and new privacy challenges, it has become outdated to draft privacy legislation based on a unitary concept. Clarity and specificity now trump generality. This point will be discussed in more detail in chapter 4 where we consider the limitations of current privacy laws. For now, it suffices to note that because privacy is such a general right, there are uncertainties around the existence of particular, specific rights to privacy.

[175] See, for example, Article 17 of the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) 1966.
[176] There is evidence that the privacy provision in the Covenant, for instance, was haphazardly created and "[t]he *travaux préparatoires* of the UDHR, the ICCPR, and the European Convention on Human Rights indicate that the right to privacy was included in all three instruments as an afterthought" (See: Krishnamurthy V., *A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy* (AJIL Unbound 2020). Also, Oliver Diggelmann and Maria Nicole Cleis conclude that their "… analysis of the drafting history of the right to privacy in the UDHR, ICCPR and the ECHR has shown, however, that there was no conscious decision to create an integral guarantee—neither on the global nor on the European level…". According to them, "the creators of the UDHR, the ICCPR and the ECHR did something new when they decided to include an umbrella term in the provisions on privacy, but they made this step without being aware of the potential implications of such a guarantee." (See: Diggelmann and Cleis (n 170) 457).
[177] Paul M. Schwartz and Karl-Nikolaus Peifer, 'Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?' (2010) 98 CLR 1925, 1929.
[178] See: Appl. No. 61496/08 Bărbulescu v. Romania (2017) ECHR 268.
[179] Appl. No. 44787/98 P.G. and J.H. v. the United Kingdom (2001) ECHR.
[180] Appli. No. 32555/96 Roche v. the United Kingdom (2005) ECHR.

That said, when it comes to the protection of privacy on the global stage, the UN has, without any doubt, been the torchbearer. Apart from creating the most important instruments on privacy on the international stage, the UN has also created specialized bodies or institutions to monitor and encourage the implementation and enforcement of the provisions on the right to privacy specifically and other fundamental human rights generally.

There are two types of specialized bodies: the charter bodies and the treaty bodies, both of which are supported by the leading UN entity on human rights: the Office of the High Commissioner for Human Rights ("OHCHR").[181] The charter bodies are created by the UN Charter itself and comprise the General Assembly, the Economic and Social Council, the Security Council, the International Court of Justice, the Secretariat (Secretary-General), and the Trusteeship Council.[182] The treaty bodies, on the other hand, are part-time bodies with a wide range of functions, usually consisting of independent human rights expert acting in their individual capacity and not as representatives of their Governments. These bodies are established under the respective UN human rights treaties.[183] While their focus and working mechanisms differ somewhat, treaty bodies generally "consider States parties' reports; consider individual complaints; conduct country inquiries; adopt general comments and organize thematic discussions to interpret the provisions of their treaty or treaties; attend the annual meeting of Chairpersons; and contribute to the treaty body strengthening process."[184]

While an extensive discussion of the functions and powers of both the charter and treaty bodies is beyond our scope, for the current purposes emphasis will be placed on two main bodies—one charter based and the other treaty based. The charter-based body is the key political human rights organ known as the Human Rights Council ("Council"), which replaced the now-defunct Commission on Human Rights. To enable its performance, the Council uses a number of general human rights mechanisms available to its predecessor. These mechanisms include the Universal Periodic Review, involving the assessment of each State's human rights performance; the Special Procedures System, a central UN human rights machinery, tasked with reporting and advising on human rights both from a country-specific and thematic

[181] In charge of achieving the human rights efforts of the UN, the OHCHR works in three core areas: supporting human rights standard setting; human rights monitoring; and supporting human rights implementation at the country level.
[182] The operations of the Trusteeship Council has since been suspended following the independence of Palau, the last remaining UN trust territory.
[183] UN Human Rights Committee, for example, is set up under Article 28 of the ICCPR (n 175).
[184] UN Human Rights Office of the High Commissioner, 'What the treaty bodies do' (*OHCHR Official Website*) <https://www.ohchr.org/en/treaty-bodies/what-treaty-bodies-do> accessed 13 July 2022.

perspectives; and the Independent Investigations, used to respond to serious violations of international humanitarian law and international human rights law.[185]

The treaty-based organ is known as the Human Rights Committee ("HRC"), which is created to monitor the implementation of the International Covenant on Civil and Political Rights and its optional protocols. Among other things, the HRC can consider inter-state complaints (although this has never been used),[186] examine individual complaints (which decisions are not generally considered binding),[187] and issue very useful, albeit merely persuasive, jurisprudential material known as General Comments, which are documents containing expanded interpretations or clarifying aspects of right(s) set out in a relevant treaty.

Bearing in mind that the two major international instruments on the right to privacy are the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, we will now carry out a quick survey of international human rights provisions on privacy. Emphasis is placed on globally applicable instruments. It is important to note that focus is placed here on treaties and other instruments. Customary international law is not discussed in any serious detail because there are uncertainties regarding the status of the right to privacy and there are arguments on whether the right has become part and parcel of customary international law, despite its recognition in important international treaties and its protection in the majority of legal systems. To provide some context, authors like Alexandra Rengel has argued that the very fact that the right to privacy is protected in a number of international instruments and has gained global recognition means that the right has earned customary international law status. [188] Arvind Pillai and Raghav Kohli have taken essentially the same position.[189]

---

[185] Ibid.

[186] Sarah Louise Joseph and Adam McBeth, *Research Handbook on International Human Rights Law* (Edward Elgar Publishing 2010).

[187] International Justice Resource Center, 'UN Human Rights Treaty Bodies' (*International Justice Resource Center*) <https://ijrcenter.org/un-treaty bodies/#:~:text=The%20committee%20issues%20a%20decision,agreed%20to%20be%20legally%20bound> accessed 15 July 2022.

[188] Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) 2(2) GroJIL 33, 42. See also See Alexandra Rengel, *Privacy in the 21st Century* (Martinus Nijhof Publishers, Leiden, 2013), 205–255.

[189] Arvind Pillai and Raghav Kohli, 'A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice' (Oxford University Comparative Law Forum) https://ouclf.law.ox.ac.uk/a-case-for-a-customary-right-to-privacy-of-an-individual-a-comparative-study-on-indian-and-other-state-practice/#3-B accessed 19 November 2022. (It is important to add that the authors note in their work that while the general right to privacy may be considered customary international law, data privacy cannot be said to have earned the same status as "it has not enjoyed sufficient time to crystallise into customary international law.")

However, other authors, including myself, take a differing view of the matter and opine that the fact that privacy has gained and continues to gain such incredible momentum globally serves only as evidence that the right is *crystallizing* into customary international law.[190] As Dr Eliza Watt puts it, "online privacy cannot be said to have yet become such a rule [of customary international law], but that it is an emergent right. Consequently, the only source is that derived from international human rights treaties stipulating for the right to privacy…"[191] Therefore, while it seems to reasonable to characterise the right to privacy as lex ferendi or an emerging norm, it is debatable that the right has met all the core criteria for a right to qualify as customary international law. In any case, the analysis of relevant treaties and other international instruments seems to be a more useful approach in addressing the key questions raised in this thesis.

3.2.1 Global Instruments on the Right to Privacy

3.2.1.1. Universal Declaration of Human Rights, 1948 ("UDHR")

A foundational text in the history of human and civil rights, the UDHR was accepted by the UN General Assembly on 10 December 1948. For the first time in human history, a list of common rights were inscribed in a document and common standard of achievements for all people and nations was set. In its Article 12, the UDHR records that: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*."[192]

As it is merely a proclamation of rights, the UDHR does not constitute a legally binding document. Thus, its provisions, including the above-cited Article 12 on the right to privacy are not legally enforceable. Its lack of legal status regardless, the UDHR is recognized internationally to have paved the way for further developments of the human right idea, and is reputed to have inspired hundreds of documents, including the International Covenant on Civil and Political Rights. Indeed, some have argued that "whatever the intention of its authors may have been, the [UDHR] is now part of the customary law of nations and therefore is binding

[190] Scott J. Shackelford 'Should Cybersecurity Be A Human Right? Exploring The 'Shared Responsibility' Of Cyber Peace' (2019) 55(2) SJIL. See also Eliza Watt, *State Sponsored Cyber Surveillance: The right to online privacy as a customary international law rule* (Edward Elgar Publishing, 2021) 93-121
[191] See: Watt (n 159).
[192] The United Nations, 1948.

on all states".[193] Of course, there are counter arguments capturing the sentiment that while "some UDHR rights may satisfy the tests of customary international law (State practice and *opinio juris*), such as the right to be free from torture, it is optimistic to ascribe such a status to the full slate of UDHR rights."[194]

3.2.1.2. International Covenant on Civil and Political Rights, 1966[195]

Unlike the UDHR, the International Covenant on Civil and Political Rights ("ICCPR" or "Covenant") is a legally binding treaty. Adopted on 16 December 1966 and becoming effective on 23 March 1976,[196] the Covenant is arguably the most important global treaty protecting the right to privacy. The Covenant contains comparable provisions on the right to privacy as that contained in the UDHR. Particularly, Article 17 of the ICCPR provides that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Through these provisions, the ICCPR not only guarantees the right to privacy, it also vests states with the obligation to ensure that the right is protected from interferences or attacks emanating both from state actors and natural or legal persons.[197] According to the General Comment No. 16, States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.

According to the interpretation of the Covenant's provision on privacy, it has been noted that the right to privacy covers, by implication, the protection of communication, inviolability of the body, dignity of the person, and data protection.[198] Especially in the context of digital privacy, the HRC has noted that:

---

[193] John Humphrey, 'The International Bill of Rights: Scope and Implementation' (1976) 17 WMLR 527, 529. A later work by Humphrey emphasizes the point that the Declaration is now "binding on all states, including the states that did not vote for it in 1948" (John Humphrey, 'No Distant Millennium: The International Law of Human Rights' (1989) UNESCO/SHS/230).
[194] Joseph and McBeth (n 186).
[195] ICCPR (n 175).
[196] There are two Optional Protocols to the ICCPR. The First Optional Protocol establishes an individual complaints mechanism. The Second Optional Protocol abolishes the death penalty.
[197] UN Human Rights Committee, 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1998) 32nd Session (UN Human Rights Committee, General Comment No. 16 on the Right to Privacy).
[198] Ibid.

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law… In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[199]

3.2.1.3. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families[200]

The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families ("Migrant Workers Convention") came into force on 1 July 2003 after years of discussion of migrants' rights since the early 1970s within the international community. A Working Group, established in 1980, finalised the Convention in 1990. Article 14 of the Migrant Workers Convention provides that:

> *No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.*

According to the Migrant Workers Convention, migrant workers and members of their families are divided into two groups: those migrant workers and members of their families who are documented or are in a regular situation and those migrant workers and members of their families who are undocumented or are in an irregular situation. It is interesting to note that the right to privacy is one right that applies to migrants, regardless of whether they are documented (regular) or undocumented (irregular).

3.2.1.4. Convention on the Rights of the Child, 1989[201]

Widely accepted as the foundational document on children's rights, the Convention on the Rights of the Child ("CRC") has been adopted by every country in the world, save for the

[199] Ibid.
[200] International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (adopted 18 December 1990, entered into force 1 July 2003) 1990.
[201] Convention on the Right of the Child (adopted 20 November 1989, entered into force on 2 September 1990) (CRC) 1989.

United States. In a language similar to the ICCPR's, Article 16 of the Convention provides that:

> *1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks.*

Also, Article 40 (2)(b)(vii) guarantees that every child alleged or accused of having infringed a penal law shall have his or her privacy fully respected at all stages of the proceedings in which the child is tried.

In their General Comment No. 25 (2021),[202] the Committee on the Rights of the Child indicated their views on many aspects of a child's right to privacy. Among other things, they noted that interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child, and must not conflict with the provisions, aims or objectives of the Convention. They also noted any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy.

3.2.1.5. Convention on the Rights of Persons with Disabilities, 2006[203]

Article 22 of the Convention on the Rights of Persons with Disabilities ("CRPD") protects personal and family privacy and reputation. The Article states that:

> *1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.*

[202] UN Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment' (2 March 2021) CRC/C/GC/25.
[203] UN General Assembly, 'Convention on the Rights of Persons with Disabilities' (24 January 2007) 61st Session A/RES/61/106.

2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.

This Article closely resembles those found in other international human rights document above considered. However, it goes further than the other documents—by ensuring that the privacy of health-related information is protected, the CRPD reflect the special concerns that people with disabling conditions are uniquely at risk of discrimination when their health data disclosed without authority.

3.2.2 Regional Instruments on the Right to Privacy

Almost all geographic regions of the world have their own general-purpose human rights instruments. Many of these instruments protect the right to privacy.

In Europe, there is the European Convention on Human Rights[204] ("ECHR") (*formally the Convention for the Protection of Human Rights and Fundamental Freedoms*), which provides in its Article 8 that: *Everyone has the right to respect for his private and family life, his home and his correspondence."* And there is the European Union Charter of Fundamental Rights[205] (the "Charter"), which alongside the ECHR, forms the second system to ensure the protection of fundamental and human rights in Europe. Proclaimed by the EU in 2000,[206] Article 7 of the Charter protects the right to privacy[207] by stating, "*Everyone has the right to respect for his or her private and family life, home and communications*".

In the Americas, the American Declaration of the Rights and Duties of Man, 1948[208] (the "Declaration") protects the right to privacy when it states that, "*Every person has the right to the protection of the law against abusive attacks upon his honour, his reputation, and his private and family life*". There is also the American Convention on Human Rights, 1969[209] ("ACHR"). Negotiated at San Jose, Costa Rica in 1969, the ACHR is an international human rights document that operates within the framework of the Organization of American States ("OAS"). Together with the Charter of the Organization of American States Charter and the

[204] European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 1950.
[205] Charter of Fundamental Rights of the European Union (CFR) 2012/C 326/02.
[206] Nine years after the Charter was first proclaimed, it earned the same status as other EU treaties and became legally binding following the entry of the Lisbon Treaty in 2009.
[207] The Charter then goes further to recognize—more like, create from nothing—the right to data protection in Article 8. The Charter represents the first supranational-level instrument to separate and establish side by side the twin rights to privacy and data protection.
[208] American Declaration of the Rights & Duties of Man. Organization of American States. 1948.
[209] American Convention on Human Rights, "Pact of San Jose, Costa Rica" (adopted 22 November 1969, entered into force 18 July 1978) 1969.

American Declaration of the Rights and Duties of Man, the ACHR form the trifecta of sources of the human rights system within the OAS. Article 11 of the ACHR also guarantees and protects the right to privacy by providing that: *No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.*

In Africa,[210] the Declaration of Principles on Freedom of Expression and Access to Information in Africa (the "Declaration")[211] protects the right to digital privacy in its Principle 40 by providing that: "*Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information*".[212] The Declaration even protects the right to "*communicate anonymously or use pseudonyms on the Internet and to secure the confidentiality of… communications and personal information from access by third parties through the aid of digital technologies.*"[213] The Declaration even goes further[214] to forbid States from adopting measures "*prohibiting or weakening encryption, including backdoors, key escrows and data localisation requirements, unless such measures are justifiable and compatible with international human rights law and standards.*"[215]

In South Asia, the Association of Southeast Asian Nations Human Rights Declaration, 2012[216] ("AHRD") was adopted on 18 November 2012.[217] In some respect, the AHRD is an adaptation of the UDHR, declaring a commitment to "all the economic, social and cultural rights in the Universal Declaration". Principle 21 of the AHRD states that: *Every person has the right to be*

[210] There is also the African Declaration on Internet Rights and Freedoms (which states in its Article 8 that "Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet and to use appropriate technology to ensure secure, private and anonymous communication"; the African Charter on the Rights and Welfare of the Child (came into force 29 November, 1999) (which protects a child's right to privacy in its Article 10); and the African Union Convention on Cybersecurity and Personal Data Protection, 2014, (which devotes 16 articles to issues ranging from States' obligations to establish legal frameworks strengthening the protection of privacy and punishing instances of its violation, to the establishment of independent national data protection authorities, and the rights of data subjects.)

[211] The Declaration has little or no practical force, being only a soft law instrument. However, this is not to deny the influence of the Declaration. As Michelle Barnard once argued, it is misleading to relegate the status of an instrument or law only because it is 'soft'. See: Michelle Barnard, 'Legal Reception in the AU against the Backdrop of the Monist/Dualist Dichotomy' (2015) 48 CILJSA 144,149.

[212] Principle 40 (1), the Declaration of Principles on Freedom of Expression and Access to Information in Africa.

[213] Principle 40 (2), the Declaration of Principles on Freedom of Expression and Access to Information in Africa.

[214] Principle 41 of the Declaration on privacy and communication surveillance is equally important and deserves mention. Among other things, the Principle 41 puts a positive obligation on States to: ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy. (See: Principle 41(3), Declaration of Principles on Freedom of Expression and Access to Information in Africa.

[215] Principle 40 (3), the Declaration of Principles on Freedom of Expression and Access to Information in Africa.

[216] Association of Southeast Asian Nations (ASEAN), ASEAN Human Rights Declaration (adopted and came into force 18 November 2012) (AHRD) 2012.

[217] The AHRD has been widely condemned as grossly ineffective, promoting cultural relativism (by suggesting or promoting the idea that the UDHR does not apply everywhere), introduces new limit to human rights, and uses language that suggest that domestic state laws can trump universal human rights.

free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.

Finally, the Council of the League of Arab States has also adopted the Arab Charter on Human Rights,[218] ("Arab Charter") during the 16th Ordinary Session of the Arab Summit, which was held on 23 May 2004 in Tunis. The Arab Charter reaffirms, in its preamble, the principles of the UN Charter, the UDHR, the provisions of the two UN International Covenants, on Civil and Political Rights and on Economic, Social and Cultural Rights, and the Cairo Declaration on Human Rights in Islam.[219] Article 17 of the Arab Charter protects the right to privacy by providing that: *Private life is sacred, and violation of that sanctity is a crime…*

3.3 Limitations on the Right to Privacy

The right to privacy can be limited in certain circumstances. It is, therefore, not an absolute right.[220] In fact, many of the international law provisions on the right to privacy themselves limit the scope of the right by recognizing that the certain legitimate events or legislation may curtail its application.[221] Thus, by using words like 'arbitrary' and 'unlawful', international law contemplates that the right to privacy can be limited in circumstances where limiting it is neither unlawful nor arbitrary. In their General Comment 16 on the right to privacy as expressed in Article 17 of the ICCPR, the UN HRC has explained that, "[t]he term "unlawful" means that no interference can take place except in cases envisaged by the law. And interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the [ICCPR]".[222]

Also, international instruments sometimes allow the suspension or suppression of rights under certain circumstances. For instance, the ICCPR contains a limitation provision for the right to privacy by allowing for the right to privacy, among other rights, to be derogated "[i]n times of public emergency which threatens the life of the nation and the existence of which is officially

[218] Arab Charter on Human Rights (adopted 22 May 2004, came into force 15 March 2008) 2004.
[219] The Charter has been severely criticized as incompatible with the UN's understanding of universal human rights, including with respect to women's rights and capital punishment for children, in addition to other provisions in the Charter.
[220] While it is inaccurate, the idea of privacy right as an absolute right has been promoted by some. For example, Patrick J. Murphy, an American politician and attorney once said "The equal protection clause of the constitution is absolute. The right to privacy is absolute. The right to assemble is absolute" See: Above Average Jane, 'Interview with Patrick Murphy' (*Above Average Jane)* <http://aboveavgjane.blogspot.com/2005/12/interviewwith-patrick-murphy.html> accessed 5 July 2022.
[221] See for example: Universal Declaration of Human Rights; International Covenant on Civil and Political Rights; Convention on the Right of the Child; International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families.
[222] UN Human Rights Committee, General Comment No. 16 on the Right to Privacy (n 197).

proclaimed".[223] To prevent abuse of this possibility of derogation, the ICCPR clearly states that any derogation measures taken must not conflict with "other obligations under international law and [must] not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin".[224] Of course, before any emergency can be used to justify the suppression of rights, such emergency must actually threaten the life of the state concerned; the emergency must have been officially declared, and notification of the emergency and measures taken must have been made to other states parties to the ICCPR.[225]

Apart from limitation provisions stipulated in many of the international instruments considered above, courts and other judicial bodies have also noted instances where the right to privacy can be limited. For example, in *Huvig*[226] and *Kruslin*[227]the European Court of Human Rights ("EctHR"), interpreting the ECHR, identified four questions, which provide a test for deciding if any given interference with a specific right, or rights, has been "legal": i.e., Does the domestic legal system sanction the infraction? Is the relevant legal provision accessible to the citizen? Is the legal provision sufficiently precise to enable the citizen reasonably to foresee the consequences, which a given action may entail? Does the law provide adequate safeguards against arbitrary interference with the respective substantive rights?[228]

Applying the tests in *Huvig* and *Kruslin*, the EctHR and other courts have decided that the right to privacy does not cover activities, "which are of an essentially public nature;"[229] and complaint of personal, social, psychological and economic suffering which is a foreseeable consequence of one's own actions. This includes, for example, the commission of a criminal offence or similar misconduct.[230] Courts have also held that the right to privacy may be restricted "for the promotion of health or morals;"[231] in cases involving the regulation of various aspects of prison life;[232] compulsory psychiatric examination;[233] the secret surveillance

[223] Article 4(1), ICCPR.
[224] Ibid.
[225] UN Human Rights Committee, 'CCPR General Comment No. 5: Article 4 (Derogations)' (31 July 1981) 13th Session.
[226] Appl. No. 11105/84 Huvig v. France (1990) ECHR A/176-B.
[227] Appl. No. Kruslin v. France (1990) ECHR.
[228] Besides these tests, two broad categories of restrictions of the right to privacy, as most other human rights, have been noted to include: those which concern "public interests", that is, the general interests of State and society; and those which concern "private interests", in the sense that they are capable of benefiting distinct groups or individuals. See: Steven Greer, *Human Rights File No 15: The exceptions to Articles 8 to 11 of the European Convention on Human Rights* (Council of Europe Publishing 1997).
[229] See: Appl. No. 10090/16 Centre for Democracy and the Rule of Law v. Ukraine (2020) ECHR.
[230] Appl. No. 76639/11 Denisov v. Ukraine (2018) ECHR; Appl. No. 17895/14 Evers v. Germany (2020) ECHR.
[231] Appl. No. 7215/75 X v. The United Kingdom (1978) ECHR.
[232] Ibid.
[233] Appl. No. 8355/78 X v. the Federal Republic of Germany (unpublished).

of criminal suspects;[234] searches for evidence of crime;[235] prohibition on consensual homosexual conduct within the armed forces;[236] the recording of journalists' telephone conversations with a lawyer suspected of involvement in terrorism;[237] and the arrest and brief detention of two protesters at a military parade in Vienna[238].

3.4 Principles Governing State Surveillance

International and regional authorities recognize that states may sometimes have to resort to surveillance in the name of national security, the economic well-being of the country, territorial integrity, the maintenance of public safety, the protection of health or morals, or the prevention of disorder or crime. Indeed, the OHCHR has said that, "surveillance… may constitute a necessary and effective measure for intelligence and/or law enforcement entities when conducted in compliance with international and domestic law."[239]

Thus, despite the centrality and importance of the right to privacy and the understanding that surveillance threatens it, there is no intention to prohibit states completely from carrying out surveillance activities. However, UN instruments state that any surveillance activity conducted by states must comply with international human rights laws, particularly those safeguarding the right to privacy.[240] In the interpretations of relevant laws by various bodies, certain (surveillance) principles have emerged over the years and are used to evaluate when limits on privacy are permissible. These can be found, for example, in court decisions and in documents such as the 1984 *Siracusa Principles* (developed to guide and limit states' restriction of rights during emergencies) or the 2014 International Principles on the Application of Human Rights to Communications Surveillance.[241] These principles help states to determine when they can

[234] R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67
[235] Appl. No. 5488/72, X v. Belgium, Yearbook XVII (1974) 222.
[236] Appl. No. 9237/81, B v. the United Kingdom, DR 34 (1983) 68.
[237] Appl. No. 8290/78, A, B, C and D v. the Federal Republic of Germany, DR 18 (1980) 176.
[238] Appl. No. 13308/87 Chorherr v. Austria (1993) ECHR.
[239] UN General Assembly (n 160) Para. 24.
[240] See generally: UN General Assembly, 'The right to privacy in the digital age' (28 December 2020) 75th Session A/RES/75/176; United Nations General Assembly (n 51); United Nations General Assembly, 'Terrorism and Human Rights' (16 January 2020) 74th Session A/RES/74/147; UN General Assembly, 'The right to privacy in the digital age' (7 October 2019) 42nd Session A/HRC/RES/42/15.
[241] The International Principles on the Application of Human Rights to Communications Surveillance (the "Principles") was issued to clarify how international human rights law applies in the current digital environment, and in what environment can those rights be limited. Conceived and drafted with the participation of the United Nations Special Rapporteur and international human rights organizations, the Principles include legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communication and systems, safeguards for international cooperation, and safeguards against illegitimate access and right to effective remedy as preconditions to surveillance activities. (See: A Project of the Electronic Frontier Foundation and a coalition of NGOs, 'Necessary and Proportionate on the Application of Human Rights to Communications Surveillance' (*Electronic Frontier Foundation*, May 2014) <https://necessaryandproportionate.org/principles/#top> accessed 28 July 2022.

legitimately conduct surveillance and they include the principles of legality, necessity, proportionality, and appropriate safeguards. In many ways, these principles are interlinked and operate in synchronization to infuse some reasonableness into state surveillance operations.

3.4.1 The Principle of Legality

Essentially, this principle states that any surveillance activity that will interfere with the right to privacy must have a legal basis in national legislation. Such legislation must be properly enacted, legitimate, and have the qualities of law; otherwise any surveillance activities carried out on the basis of such legislation will in turn be invalid and unlawful.[242] In other words, for surveillance to be lawful, it must be backed by a legitimate legislation. As the UN notes in a 2017 Report, "to satisfy the principle of legality, surveillance powers must be contained in public legislation… However, publicly available *primary legislation is not, in itself, sufficient* to ensure the compatibility of those regimes with international human rights law".[243] Thus, where a piece of legislation permits surveillance, but that legislation does not meet the qualities of law requirement, it may be struck down by the court. Accordingly, in *Ekimdzhiev and Others v. Bulgaria*[244], the EctHR held that there had been a violation of the ECHR because the Bulgarian laws on secret surveillance "*did not meet the 'quality-of-law requirement of the Convention*"[245] and was unable to keep surveillance to only that which was necessary".[246]

Speaking of the qualities that surveillance laws must have, major ones are that the laws must be easily accessible to the public and must contain precise conditions for initiating and conducting surveillance. In other words, "secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law"".[247] Again, the law

[242] For an excellent discussion on the principle of legality, see: Antonella Galetta, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance' (2014) 10 ULR 55. Although written from the perspective of the ECHR, it is still an excellent resource. See also: the Siracusa Principles, developed to guide and limit states' right of restriction. According to the Siracusa Principles, restrictions of rights can only be justified when those restrictions are provided for by law, strictly necessary, proportionate, of limited duration, and subject to review against abusive applications (UN Commission on Human Rights, 'The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (28 September 1984) 41st Session E/CN.4/1985/4).

[243] United Nations General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (21 February 2017) 34th Session A/HRC/34/61. (emphasis added).

[244] Appl. No. 70078/12 (2022) ECHR 1.

[245] Ibid. (emphasis added).

[246] See: Ekimdzhiev and Others v. Bulgaria (n 244); European Court of Human Rights, *Factsheet – Mass surveillance* (European Court of Human Rights 2022).

[247]United Nations General Assembly (n 153) Para 29; Appl. No. 58361/12;25592/16;27176/16 Zoltán Varga v Slovakia (2021) ECHR.

must be "sufficiently precise [and] [d]iscretion granted to the executive or a judge and how such discretion may be exercised must be circumscribed with reasonable clarity".[248]

The UN has issued several reports discussing in part the principle of legality and the nature of laws sanctioning such legality, and there are also several international decisions. In a 2021 report, the Council noted that the "… surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory".[249] In another report, the UN observed that, "… all types of surveillance activities and interference with privacy, including online surveillance, interception of communications and communications data (metadata) and retrieval of data, are governed by appropriate legislation that is in full conformity with the Covenant… ".[250] Lastly, in the 2021 case of Big Brother Watch v The United Kingdom, the Court held that, "[a]ny interference with an individual's Article 8 rights can only be justified… if it is in accordance with the law, pursues one or more of the legitimate aims… and is necessary in a democratic society in order to achieve any such aim".[251]

3.4.2. The Principle of Proportionality

This principle mandates complete abstinence from the thinking that the end always justifies the means and stresses that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[252] According to this principle, states must always consider whether surveillance—the form and level of surveillance and the sensitivity of information gathered—is proportional to the interest sought to be secured or the objective(s) hoped to be accomplished.[253] It is about carrying out a cost-benefit analysis and

[248] United Nations General Assembly, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism' (23 September 2014) 69th Session A/69/397.
[249] United Nations General Assembly (n 51); United Nations General Assembly (n 160).
[250] UN Human Rights Committee: Concluding Observations on the Third Periodic Report of Tajikistan' (22 August 2019) CCPR/C/TJK/CO/3.
[251] Appl. No. 58170/13;62322/14;24960/15 Big Brother Watch and 15 Others v The United Kingdom (2021) ECHR. See also: Appl. No. 27057/06 Gorlov and Others v Russia (2019) ECHR; Appl. No. 59589/10 Konstantin Moskalev v Russia (2017) ECHR; Appl. No. 43514/15 Catt v The United Kingdom (2019) ECHR.
[252] UN Human Rights Committee, 'Toonen v Australia, Communication No 488/1992, U.N. Doc CCPR/C/50/D/488/1992' (1994) 50th Session CCPR/C/WG/44/D/488/1992;CCPR/C/46/D/488/1992. See also: (Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) (2014) The Grand Chamber C-293/12 and C-594/12.
[253] Antonio Troncoso Reigada, 'The Principle Of Proportionality And The Fundamental Right To Personal Data Protection: The Biometric Data Processing' (2012) 17 Lex Electronica. See also: Jonida Milaj, 'Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance' (2015) 30 IRLCT 115-130.

balancing the state's aim with the possible implication of infringing on fundamental rights, including especially the right to privacy. Put in other words, the principle of proportionality would have been complied with where surveillance measure(s) adopted brings an advantage that outweighs any harm or restriction to democratic values and rights.

In assessing proportionality, the UN has proposed that "there must be a rational connection between the means employed and the aim sought to be achieved… [and] the measure chosen [must] be "the least intrusive instrument among those which might achieve the desired result".[254] Based on that context, therefore "[a] high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high".[255]

Referencing the HRC's General Comments and the 1984 *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, the UN has also stated that any limitation sought to be imposed on the right to privacy "… must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal."[256] In the same breath, the UN noted further that "any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination…"[257]

3.4.3. The Principle of Necessity

This principle states that any interference with the right to privacy on the basis of state surveillance must be necessary. States must, therefore, be able at all times to show that surveillance is necessary in particular circumstances because other means would not have achieved intended objectives.[258]

[254] United Nations General Assembly (n 248).
[255] United Nations General Assembly, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (22 May 2015) 29th Session A/HRC/29/32.
[256] United Nations General Assembly (n 156).
[257] Ibid.
[258] Appl. No. 54934/00 Weber and Saravia v Germany (2006) ECHR.

Thus, in *Toonen v Australia*,[259] the Committee held that, [...] any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case." Also in *Liblik and Others v Estonia*, the Committee held that, "… powers to instruct secret surveillance of citizens are only tolerated… to the extent that they are strictly necessary for safeguarding democratic institutions."[260] To determine necessity, surveillance can only be considered legitimate if it is strictly necessary to address a "pressing social need" in a democratic society.[261] This was also the Court's decision in Szabó and Vissy v Hungary[262]where:

> the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the ECHR only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance, which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse.

3.4.4 The Principle of Adequate Safeguards

This principle serves to ensure that all other principles are observed. It ensures not only that surveillance is legal, necessary, and proportionate but that an assessment and implementation of appropriate limitations on access, processing, storage, and sharing is done. The principle of adequate safeguards goes even further to also prevent arbitrariness. It does this by mandating transparency in surveillance operations, demanding that states obtain authorization from an independent judicial or quasi-judicial body, and requiring the establishment of a process that enables the review of surveillance activities even after they have been terminated.

By analysing the current international law on privacy, this chapter provides the background for examinations in the next chapter showing how current international law fails to protect privacy, especially in light of sophisticated state surveillance practices.

[259] UN Human Rights Committee (n 252).
[260] Appl. No. 173/15 (2019) ECHR 383.
[261] Appl. No. 37717/05 Dudchenko v Russia (2017) ECHR 965.
[262] Appl. No. 37138/14 (2016) ECHR.

Chapter 4

> "Unfettered international surveillance creates an array of issues, from invading intellectual privacy to distorting power relationships between state and citizen to accelerating discrimination and human rights abuses. The surveillance state is ubiquitous and increasingly transnational, so the realm of international law presents an opportunity to build a theoretical framework for at least protecting the human rights and privacy of non-citizens from foreign surveillance."—Will Schrepferman[263]

4.1 Introduction

Chapter 4 analyses the major problems with current international law on privacy and concludes that states' surveillance practices, as they have evolved over the years, have become irreconcilable with current international law. Not only has international law failed to regulate foreign surveillance (thereby leaving room for states to make privacy-defeating foreign surveillance laws), there are controversies regarding the scope of application of privacy obligations in international instruments. Also, mass surveillance is not regulated and there is little clarity on what the 'right to privacy' actually entails. This chapter exposes the doctrinal gaps and lacunas in current international law, and shows how states have exploited those lacunas, further weakening the right to privacy.

4.2 The Problems with Current International Law

International law and its implementation mechanisms have largely succeeded in establishing and promoting the right to privacy and providing guidance to states on complicated issues affecting privacy, including surveillance, artificial intelligence, and the use of health-related data. However, as international law has remained relatively static over the past several decades in the face of incredible and daily technological advancements, the evolution of new privacy concerns, and changes in states dynamics, current practices of states when it comes to surveillance practices have become irreconcilable with current international law.

[263] Will Schrepferman, 'Supervising Surveillance: Applying International Law to the Global Surveillance State' (*Harvard International Review*, 11 November 2020) <https://hir.harvard.edu/global-surveillance-state/> accessed 19 August 2022.

At the heart of the problem is international law's failure to evolve to regulate foreign surveillance—i.e., surveillance conducted on non-residents/non-nationals of a state—which has grown to become the new normal since the periods after the Cold War.[264] Therefore, whilst directly influencing states' protection of individuals' privacy right when conducting domestic surveillance,[265] international legal instruments and principles on privacy and surveillance encounter serious difficulty when dealing with the "murkier problem of states surveilling non-citizens"[266] outside their territories. This has created room for states to dent the essence of the supposedly global privacy right granted under international law by granting lesser privacy guarantees to foreigners.

A second, different but related problem revolves around claims by some states that privacy obligations under international law do not apply to them when they conduct foreign surveillance, particularly through technology that allows them to surveil foreigners without ever leaving their territories.[267]

Yet a third problem with current international law concerns the issue of mass surveillance, especially when conducted on foreigners. The analyses of current international laws and principles on privacy and surveillance seem to suggest that mass surveillance is unjustifiable or illegitimate. That said, there have been conflicting views, especially on the international stage, regarding the legitimacy of mass surveillance. Unfortunately, international law does not clearly regulate mass surveillance, even though it has become a standard feature of many states' surveillance programs.

Fourth, there is the issue of privacy's scope—it is unclear what 'privacy' as it appears in many international instruments actually covers. Does it include data protection, which is a subset of privacy? Does it cover metadata, which is a subclass of data? Does it protect such things as

---

[264] Von Laura Poitras, Marcel Rosenbach and Holger Stark, 'How America Spies on Europe and the UN' (*Spiegel International*, 26 August 2013) <https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> accessed 18 August 2022.

[265] At least when it comes to domestic surveillance, states usually have some legislative safeguards—usually embedded in national intelligence/defence laws, cybercrimes and criminal laws, or even dedicated surveillance laws—guaranteeing the right to privacy and dictating the circumstances under which surveillance is permissible. For example, in Belgium, the Law of 30 November 1998 Organizing the Intelligence and Security Services and Law on electronic communications regulate domestic surveillance activities. In Germany, the domestic intelligence legislative framework includes the Act on the Federal Office for the Protection of the Constitution, the Act on the Military Counter-Intelligence Service, the Act on the Federal Intelligence Service, and the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications (Article 10 Act). And in Canada, the National Security and Intelligence Review Agency Act (NSIRA Act); the Intelligence Commissioner Act (IC Act); the Communications Security Establishment Act (CSE Act); the Privacy Act, Charter of Rights and Freedoms, Criminal Code, and the National Defence Act, all contain provisions stipulating when and how state surveillance can be conducted.

[266] Schrepferman (n 263).

[267] Yet another scenario raised beyond the scope of this thesis involves a situation where state A carries out surveillance on the people in state B while actually present in the territory of state B.

encryption and anonymity, which are subsets of communications privacy? As noted earlier in this thesis, while it was wise to offer an umbrella protection decades ago when the idea of privacy itself was not fully formulated and technology had not introduced peculiar and new privacy challenges, it has now become outdated and impracticable to continue to use privacy instruments based on a unitary concept.

4.2.1 Unequal Legislative Guarantees to Citizens/Residents and Foreigners

When conducting domestic surveillance, states often work within the confines of laws intended to protect the privacy of individuals who are citizens and/or residents. These laws give some indication on permissible/impermissible surveillance activities; usually contain some form of administrative/judicial safeguards to prevent abuse; and often arm interested persons with the right to seek redress through the local courts where they perceive that their right have been infringed.

On that last point, consider, for examples, the cases of: (a) *Hassan v City of New York*,[268] concerning the New York Police Department's baseless surveillance of Muslims residing in New Jersey; (b) *Clavir v Levi*,[269] concerning the FBI's illegal surveillance of political activists: Judy Clavir and Stew Albert; and (c) *Mohamud v United States*,[270] challenging the constitutionality of the *Foreign Intelligence Surveillance Act*.[271] In the EU, there are the cases[272] of *Association pour l'intégration européenne and les droits de l'homme and Ekimdzhiev v. Bulgaria*,[273] *Oleynik v. Russia*,[274] *Liberty and Others v. the United Kingdom*,[275]; and *Rotaru v. Romania*[276]; in all of which the EctHR found violations of Article 8 of the ECHR (on the right to privacy). Several other examples abound still.[277]

[268] (2015) 804 F.3d 277.
[269] (1979) 84 F.R.D. 612.
[270] (2016) 843 F.3d 420.
[271] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 ("FISA Amendment Act") 1978.
[272] See for examples, CCR v. Obama (formerly CCR v. Bush) (2006) 3:07-cv-01115 U.S District Court for the Northern District of California; Kinoy v. Mitchell [(1971) 331 F. Supp. 379]; and Haasev Webster [(1985) 608 F. Supp. 1227].
[273] Appl. No. 62540/00 (2007) ECHR.
[274] Appl. No. 23559/07 (2016) ECHR 553.
[275] Appl. No. 58243/00 (2008) ECHR.
[276] Appl. No. 8341/95 (2000) ECHR.
[277] See also Dombrowski v Eastland [(1967) 387 U.S. 82]; Association "21 December 1989" and Others v. Romania [Appl. No. 33810/07 (2011) ECHR]; Roman Zakharov v. Russia [Appl. No. 47143/06 (2015) GC]; Shimovolos v. Russia [Appl. No. 30194/09 (2011) ECHR 987]; Valašinas v. Lithuania [Appl. No. 4558/98 (2001) ECHR]; Silver and Others v. the United Kingdom [Appl. No. . 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 (1983) ECHR]; Labita v. Italy [Appl. No. 26772-95 (2000) ECHR; Niedbała v. Poland [Appl. No. 27915/95 (2000) ECHR; Messina v. Italy (no. 2) [Appl. No. 25498/94 (2000) ECHR; Ekinci and Akalın v. Turkey [Appl. No. 40365/09 (2012) ECHR 246]; Campbell v. the United Kingdom [Appl. No. 12244/86; 12245/86; 12383/86 (1990) ECHR; A.B. v. the Netherlands [Appl. No. 37328/97 (2002) ECHR 9; Peers v. Greece [Appl. No. 28524/95 (2001) ECHR]; and Szuluk v. the United Kingdom [Appl. No. 36936/05 (2009) ECHR).

Foreign surveillance, on the other hand, faces peculiar challenges. The OHCHR has recognized this problem when it observed that: "*[s]everal legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection.*"[278] To see how dissimilar privacy guarantees are offered to citizens/residents and foreigners, let us briefly consider the surveillance laws in Canada, the US, and the EU.[279]

When it comes to foreign surveillance in Canada, the Communications Security Establishment ("CSE") is the agency primarily responsible for foreign surveillance. The agency is mandated by law "to acquire, covertly or otherwise information from or through the global information infrastructure… and to use, analyse and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities."[280] By authorizing the collection of 'unselected' information[281] (information that is not tied to any criteria or keyword) and by enabling the collection of publicly available information, the law—i.e., An Act Respecting National Security Matters, 2019 ("National Security Act")[282]—empowers the CSE to carry out mass surveillance on foreigners.

The *National Security Act* even prescribes that the CSE may be authorized to "[gain] access to a portion of the global information infrastructure; [acquire] information on or through the global information infrastructure…; [install, maintain, copy, distribute, search, modify, disrupt, delete or intercept] anything on or through the global information infrastructure.[283] Furthermore, the law "gives the CSE new powers to use cyber-attacks against foreign individuals, states, organizations or terrorist groups. This would include hacking, deploying malware, and "disinformation campaigns".[284]

Throughout the National Security Act, emphasis is placed on protecting the privacy of Canadians and persons in Canada, especially concerning communications sent or received

[278] United Nations General Assembly (n 156) Para. 35. (emphasis added).
[279] It is worthy to note that the ECtHR has also suggested in at least two cases that the same privacy standards do not apply to domestic and foreign surveillance. See: Appl. No. 35252/08 Centrum for Rattvisa v. Sweden (2018) GC; Big Brother Watch and Others v The United Kingdom For a comprehensive analysis of the ECtHR's position, see: Asaf Lubin, 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights' (*Just Security*, 2 August 2018) <https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/> accessed 15 August 2022.
[280] An Act Respecting National Security Act Matters 2019 (AARNSAM 2019) s 16.
[281] Ibid. s 26 (2) (b).
[282] Ibid.
[283] Ibid. s 26 (1) and (2).
[284] Lawyers' Rights Watch, 'Canada: Civil Society Statement Regarding Bill C-59, An Act Respecting National Security Matters | Joint Letter' (Lawyers' Rights Watch, 27 March 2018) < Canada: Civil Society Statement Regarding Bill C-59, An Act Respecting National Security Matters | Joint Letter — Lawyers' Rights Watch Canada (lrwc.org)> accessed

abroad, with foreigners left with few guarantees and no remedies.[285] This sentiment is clearly expressly in Section 22(1) of the law,[286] which provides that the surveillance activities of the CSE "must not be directed at a Canadian or at any person in Canada and must not infringe the *Canadian Charter of Rights and Freedoms*."[287]

CSE has a 'sister' agency with which it is often confused—the Canadian Security Intelligence Service ("CSIS"). The CSIS's chief role is to investigate and report activities that may constitute threats to Canada's security. Unlike the CSE whose main focus is collecting foreign intelligence and monitoring threats from abroad, the CSIS looks for threats inside Canada. Interestingly, the law establishing the CSIS also empowers the CSIS to conduct foreign surveillance relating to the capabilities, intentions or activities of foreigners but offers wide protection to artificial entities and natural persons who are citizens of or permanent residents in Canada.[288]

The situation is the same in the US where the position has always been that foreigners are not entitled to the same level of privacy protection as that offered to US citizens. As Professor David Cole has excellently summarized the sentiment, law, and policy in the US towards foreign surveillance:

> American law and politics have long taken the view that our constitutional and statutory privacy protections are limited to persons within the United States, and US citizens outside our borders. The Supreme Court has ruled that the Fourth Amendment does not apply to searches of foreigners' homes overseas. The Foreign Intelligence Surveillance Act is focused on protecting U.S. citizens and persons, and offers no protection for foreign citizens outside our borders – even though they are just as vulnerable to wiretaps and other forms of electronic monitoring as are US citizens. And in the substantial public debate that Snowden's disclosures have prompted here, virtually all the concern voiced here has focused on NSA monitoring of U.S. citizens' communications.[289]

[285] See generally: AARNSAM 2019.
[286] Ibid, s 24(a) and (b), which provides that the CSE "must ensure that measures are in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of (a) information related to them acquired in the course of the furtherance of the foreign intelligence and cybersecurity and information assurance aspects of the [CSE's] mandate; or (b) publicly available information related to them…". See also: ibid s, 22(3) and (4).
[287] Ibid, s 22(1).
[288] Canadian Security Intelligence Service Act 1985 s 11, 12(3), and 16.
[289] David Cole, 'We Are All Foreigners: NSA Spying and the Rights of Others' (*Just Security*, 29 October 2013) <https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/> accessed 18 August 2018.

Indeed, foreign surveillance programs in the US are justified by citing key provisions, including Section 215 of the Patriot Act;[290] Executive Order 12333[291] and Section 702 of the FISA Amendments Act of 2008,[292] all of which authorize foreign surveillance, including on a mass scale. Section 702 of the FISA Amendments Act of 2008, for instance, authorizes the gathering, analysis, and dissemination of electronic communications content; and whilst prohibiting the intentional targeting of people in the US, nothing in Section 702 requires foreign surveillance to be targeted or the primary purpose of the surveillance should be to obtain foreign intelligence information.[293] Then there was the US Patriot Act,[294] which expired in 2020, and which provisions have now been substantially restored and/or amended in the USA Freedom Act. Despite its innovations, the Freedom Act does little to protect foreigners' privacy. Not only does the Act fail to eliminate "dragnet collection under Section 215 of the Patriot Act, repeal Section 702 of the FISA Amendments Act, [or] require the administration to disclose the full scope of its mass surveillance";[295] the Act also fails to end mass surveillance under Executive Order 12333.[296]

One legal novelty intended to protect foreigners is the Presidential Policy Directive 28 ("PPD-28"),[297] introduced to affirm the "principles to guide why, whether, when and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes".[298] The PPD-28 was issued in January 2014. Prior to this time, there was no public commitment by the US to foreigner's privacy.

Now, while the PPD-28 declares that the US intelligence collection should respect the privacy interest of all persons, privacy protections offered under the PPD-28 are weak, insubstantial, and insufficient—none of the principles and requirements introduced by it change or deviate in any fundamental way from existing practice by the intelligence community. For one, while the PPD-28 stipulate that the collection of surveillance data shall be "authorized by statute or

[290] US Patriot Act 2001.
[291] Executive Order 12333 (appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200) 1981.
[292] FISA (n 271).
[293] Congressional Bills 110th Congress, Amendment to the Foreign Intelligence Surveillance Act of 1978 (FISA) to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes, 2008.
[294] US Patriot Act 2001.
[295] Natalie Butz, 'Congress Must Put Human Rights at the Center of Surveillance Reform' (*Amnesty International*, 7 May 2014) <https://www.amnestyusa.org/press-releases/congress-must-put-human-rights-at-the-center-of-surveillance-reform/> accessed 17 August 2022.
[296] Human Rights Watch, 'US: Modest Step by Congress on NSA Reform' (*Human Rights Watch*, 8 May 2014) <https://www.hrw.org/news/2014/05/08/us-modest-step-congress-nsa-reform> accessed 8 August 2022.
[297] Office of the Director of National Intelligence, *Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28* (Leading Intelligence Integration 2014).
[298] Ibid.

Executive Order, proclamation, or other Presidential directive…" this principle effects no radical change to the status quo but only "formalize[s]" current practice… since all signals intelligence activities are conducted either pursuant to executive order or statute."[299]

On a related note, the PPD-28 also requires that "SIGINT[300] activities shall be as tailored as possible." As such, "[i]n determining whether to collect SIGINT, the United States shall consider the availability of other information… [s]uch appropriate and feasible alternatives to SIGINT should be prioritized."[301] Again, while this principle sounds innovative, it only describes the efficiency with which the intelligence community must ordinarily work even when conducting surveillance on a mass scale. As such, 'tailored' surveillance does not stop strategic mass surveillance, and it does not guarantee the conduct of surveillance using the "least intrusive means"—a principle that must be observed when determining the proportionality of a surveillance measure.[302]

The above observations have led one author to comment that, "while PPD-28 may create some changes at the margins by adding internal government procedures and coordination, in practice the [PPD-28's] aspirational language still allows the [intelligence community] to maintain the status quo".[303] As such, billions of people outside the US continue to live in a world where they cannot feel safe communicating online. As Daniel Severson puts it:

> In sum, other than the requirements that information collected meet foreign intelligence needs and the general oversight provided by the inspectors general and through reporting to Congress, non-U.S. persons have virtually no privacy protections under programs conducted pursuant to Executive Order 12333. Section 702 of FISA is unique among U.S. intelligence programs in that it provides at least nominal judicial review for non-U.S. persons. Yet the FISC does not review individual targeting decisions, and the minimization procedures do not apply to non-U.S. persons. *Overall, persons with U.S. person status enjoy greater privacy protections under programs conducted pursuant to both Executive Order 12333 and FISA Section 702*.[304]

[299] Daniel Severson, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change' (2015) 56 HILJ 465, 481.
[300] 'SIGINT' is an abbreviation—or more accurately a shortening—of the word 'signal intelligence'. As the name implies, SIGINT or signal intelligence refers to the gathering of intelligence that usually involves complex technical characteristics from communications, electronic, and foreign instrumentation signals or systems.
[301] Office of the Director of National Intelligence (n 297).
[302] United Nations General Assembly (n 248).
[303] Severson (n 299) 486.
[304] Severson (n 299) (emphasis added).

Things are no different in the EU where their surveillance laws also treat domestic and foreign surveillance differently. To offer a glimpse into the differences, consider, for instance, that "no [member states in the EU] explicitly provides for minimisation procedures or remedies for non-citizens and there is a lack of detail regarding the nature, scale, purposes and oversight mechanisms of foreign intelligence gathering by European intelligence agencies."[305] Much more than that, EU member states' laws tend to allow the carrying out of foreign surveillance for a wide variety of purposes ranging from "external military threats, the prevention or detection of serious crimes… and often include the collection of data 'relevant' to a country's foreign policy or economic interests."[306]

Consider France,[307] for instance, where the 2015 *Intelligence Act*, as amended in July 2021,[308] regulates France's intelligence agencies. For domestic surveillance to be conducted in France, it must be targeted, approved, and retained for very limited period (i.e., 30 days for voice communications; 4 years for metadata; and up to 6 years for encrypted data). However, when it comes to surveillance of non-nationals conducted within France, broad authorizations lasting four months but which can be renewed indefinitely can be issued to carry out foreign surveillance on entire countries, organizations, or geographic regions.

In addition to the above, under the French law, whereas voice communications and encrypted data collected under domestic surveillance could be stored for only 30 days and 6 years respectively; voice communications and encrypted data collected under foreign surveillance conducted within France could be stored for 1 year and up to 8 years respectively.[309] But perhaps the most unusual thing about the French law is its failure to impose any restrictions on surveillance activities conducted by French agencies *outside* of France.[310]

Besides Canada, the US, and the member countries of the EU, many other states also create a dichotomy between the level of oversight, safeguards, and privacy protection afforded to citizens and foreigners when conducting surveillance. As Professor Lubin succinctly writes,

---

[305] Ian Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, 'Towards Multilateral Standards for Surveillance Reform' (2015) 1, 10.
[306] Ibid.
[307] For an excellent analysis of the French Intelligence Act, see: Felix Treguer, Overview of France's Intelligence Legal Framework' (2021) HAL Open Science <https://halshs.archives-ouvertes.fr/halshs-01399548/document> accessed 10 August 2022.
[308] See Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement (codified in the Code of Internal Security, Book VIII "On Intelligence" (article L. 801-L. 898-1)).
[309] Internal Security Code [(Legislative part (Articles L111-1 to L898-1) Amended by Ordinance No. 2018-1125 of 12 December 2018 - art. 22].
[310] Electrospaces, 'A look at the latest French laws on intelligence collection' (*Electrospace.net*, 26 February 2016) <https://www.electrospaces.net/2016/02/a-look-at-latest-french-laws-on.html> accessed 14 August 2022.

"[f]rom the U.S to Russia, from Germany to the United Kingdom, from Canada to Australia, internal legislation seems to denote two separate legal regimes, one for those within the borders of the country, and another for foreigners."[311] Indeed, many states do not even have actual, publicly accessible legislation governing their foreign surveillance activities. These states often resort to the use of "confidential executive orders and secret internal guidelines, naturally allowing for even greater flexibility and leniency".[312]

One major reason why unequal legislative guarantees have become prevalent and largely unchallenged is that international law has failed to clearly regulate foreign surveillance, thereby creating room for states to make privacy-defeating foreign surveillance laws. This lacuna in international law is not exactly astounding, considering that foreign surveillance is a relatively new form of surveillance that has emerged as dominant thanks to technological advancement of the past couple of decades.

4.2.2 Controversies around the Universality of Privacy and States' Obligations to States when Conducting Foreign Surveillance

Another problem with current international law revolves around the lingering question of states' responsibilities when they conduct surveillance on foreigners. The question has been framed variously as whether international human right treaties such as the ICCPR have extraterritorial application or apply to foreign surveillance activities; and whether privacy is a universal right to which all people everywhere can lay claim against any state. The UN, itself, has acknowledged the problem when they noted that "[w]hereas it is clear that certain aspects of… surveillance programmes, for instance, will trigger the territorial obligations of States conducting surveillance… concerns have been expressed in relation to extraterritorial surveillance and the interception of communications."[313]

Although the "question of extraterritorial application of treaties has been riddled with inconsistencies and has evolved on a case-by-case basis rather than following a principled approach",[314] the popular sentiment seems to be that international law offers equal privacy protections to everyone.[315] Reinforcing this view, the UN also cited Articles 31 and 32 of the

[311] Lubin (n 15) 513.
[312] Lubin (n 15) 514.
[313] United Nations General Assembly (n 149) Para. 31.
[314] *R. (Smith) v. Secretary of State for Defence* (2010) UKSC 29*;* Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 HILJ 81, 102.
[315] Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2014) 82 FLR 2137; Ilina Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 UJIEL 104. Also see: Appl. No. 55721/07 Al-Skeini v. United

Vienna Convention on the Law of Treaties (on general and supplementary rules of interpretation, respectively), and noted the views of the International Court of Justice, affirming that states are bound by the ICCPR "in the exercise of [their] jurisdiction[s] outside [their] own territory."[316] Furthermore, the HRC has noted that "[t[here shall be no discrimination between aliens and citizens…"[317] and that a "State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking at home".[318]

These conclusions are based mainly on Article 2 of the ICCPR which binds states to respect all the rights protected in the ICCPR, including the right to privacy, when dealing with "all individuals within its territory *and* subject to its jurisdiction".[319] In other words, a state must respect its privacy obligations when surveilling individuals (nationals or non-nationals) who are within its territory or on foreigners who are outside its territory but subject to its jurisdiction. Regarding the latter, the idea is that states' jurisdictions extend to those places or spheres where they exercise their powers or 'effective control'—after all, "[i]n international human rights courts and treaty bodies, whether a state exercises 'effective control' over a territory or a person today operates as the main test for settling the threshold issue of jurisdiction."[320]

Summarizing the popular interpretation of Article 2 of the ICCPR, Francesca Bignami & Giorgio Resta notes that,

> … the majority opinion asserts a broader interpretation of Article 2 of the ICCPR, downplaying its literal wording, namely the use of the conjunctive "and," and holding that any state party must respect and ensure the rights guaranteed by the ICCPR *both* within its territory *and* whenever it has "jurisdiction" over either foreign territory or a person. In particular, the Human Rights Committee, in its case law and its General Comment, Number 31, has firmly taken the position that '*a State Party must respect and ensure the rights laid*

Kingdom (2011) GC; see also Thomas Buergenthal, *To respect and to ensure: state obligations and permissible* (Louis Henkin ed., 1981).

[316] International Court of Justice (ICJ) Advisory Opinion, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory' (9 July 2004) ICJ Reports. See also: Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (2005) ICJ.

[317] UN Human Rights Committee, 'CCPR General Comment No. 15: The Position of Aliens Under the Covenant' (11 April 1986) 27th Session Para. 7.

[318] See: Official Records of the General Assembly, 36th Session (see footnote 27), Annex XIX, Paras. 12.2-12.3, and Annex XX, Para. 10.3.

[319] International Covenant on Civil and Political Rights (n 175).

[320] Francesca Bignami and Giorgio Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance' (2017) 67 GWU Law School Public Law and GWU Legal Studies 1, 5.

down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.'"[321]

Finally, the Committee has held in the *Lopez Burgos* case (dealing with the question of whether a state was liable under the ICCPR for violations perpetrated by its agents outside its territory) that states cannot be permitted to "perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory."[322] This, according to the Committee, would be an unconscionable thing for states to do.

Supporting the argument that international law applies globally and to everyone, including especially those protecting the right to privacy, some academics and privacy scholars have also argued that the extraterritorial application of international law is a given; and that nothing in the *travaux* of the ICCPR, for instance, signals that the ICCPR is not meant to apply extraterritorially.[323] In this regard, Professor Milanovic has observed that, "human rights treaties do apply to all or the vast majority of foreign surveillance activities… The appeal of human rights as a regulatory framework lies precisely in the fact that surveillance measures are now deployed against masses of ordinary people both at home and abroad…"[324]

While the view described above seems reasonable and popular, it has not been accepted by many states, including notably the US and the UK,[325] both of which countries seem to have valid reasons for their non-acceptance of extraterritorial application of their obligations under

[321] Ibid.
[322] UN Human Rights Committee, '*Delia Saldias de Lopez v. Uruguay'* (29 July 1981) 13th Session CCPR/C/13/D/52/1979 Para. 12.3.
[323] See for examples: Michael J. Dennis, 'Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation' (2005) 99 AJIL 119; Noam Lubell, *Extraterritorial Use of Force Against Non-State Actors* (Oxford University Press 2010); Margulies (n 308); Nigel Rodley, 'The Extraterritorial Reach and Applicability in Armed Conflict of the International Covenant on Civil and Political Rights' (2009) 5 EHRLR 628; Margaret Satterthwaite, 'Rendered Meaningless: Extraordinary Rendition and the Rule of Law' (2007) 75 GWLR 1333; Beth Van Schaack, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations' (2014) 90 ILS 20.
[324] Milanovic (n 314) 140.
[325] That the UK and US, particularly, have taken this view is rather unfortunate, considering their combined surveillance capabilities, occasioned especially by their relatively easy access to much of world's internet. See: James Ball, Julian Borger and Glenn Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security' (*The Guardian*, 6 February 2013) <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> accessed 10 August 2022; Olga Khazan, 'The Creepy, Long-Standing Practice of Undersea Cable Tapping: The newest NSA leaks reveal that governments are probing "the Internet's backbone." How does that work?' (*The Atlantic*, 16 July 2013) <https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/> accessed 10 August 2022.

international law.[326] First, the US has argued consistently[327] that their obligations under the ICCPR, especially as provided under Article 2, apply only to individuals who are both *within* the state's territory *and* subject to the state's jurisdiction. Essentially, this means "… communications involving individuals abroad, which are the focus of many NSA programs, are not covered by the 'international right to privacy'."[328]

Although the US' interpretation of Article 2 of the ICCPR is considered a restrictive version, it is an interpretation that is as valid as the HRC's: after all, "[t]he treaty's negotiating history confirms [the US'] interpretation. Anxious about the ICCPR applying to foreign persons under U.S. occupation after World War II, the United States suggested adding the phrase 'within its territory.' The language was adopted, and subsequent efforts to remove the phrase failed".[329]

Other states have followed the US' perspective on the matter. In their replies to the HRC's observations regarding their interpretation of the ICCPR, the Government of Netherlands claimed that: "Article 2 of the Covenant clearly states that each State party undertakes to respect and to ensure to all individuals 'within its territory and subject to its jurisdiction' the rights recognized in the Covenant . . . . It goes without saying that the citizens of Srebrenica, vis-à-vis the Netherlands do not come within the scope of that provision."[330] The State of Israel has also maintained the same stance, as can be gleaned from the HRC observation in their 2014 *Concluding Observations on the Fourth Periodic Report of Israel*. According to the HRC, Israel "continues to maintain its position on the non-applicability of the Covenant to the Occupied Territories, by claiming that the Covenant is a territorially bound treaty and does not apply with respect to individuals under its jurisdiction but outside its territory".[331] Things are no different in the UK—and indeed potentially all of EU—where, despite the privacy provisions in the ECHR and other international instruments, the EctHR's recent judgments in

[326] Arguing in favour of states like the US and the UK, Professor Orin Kerr has also posited that "the US government's obligation to respect the privacy of its citizens and those within its territory stems from a social contract not present with everyone else in the world." See: Benjamin Wittes, 'A Global Human Right to Privacy?' (*Lawfare*, 11 November 2013) <https://www.lawfareblog.com/global-human-right-privacy> accessed 10 August 2022 (And scholars like Benjamin Wittes has questioned the practicality of a global right to privacy, which would necessarily entail reciprocal treatments by and among democratic and non-democratic states).
[327] For a critical analysis of the traditional U.S. position, see Beth Van Schaak, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change' (2014) 90 ILS 20.
[328] Bignami and Resta (n 320) 4.
[329] Daniel Severson citing Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Privacy and Civil Liberties Oversight Board 2014).
[330] UN Human Rights Committee, 'Information in Pursuance of Paragraph 27 of the Concluding Observations of the Human Rights Committee: Netherlands' (29 April 2003) CCPR/CO/72/NET/Add.1 para 7.
[331] United Nations Committee on Economic, Social and Cultural Rights, 'Concluding observations on the 4th periodic report of Israel: Committee on Economic, Social and Cultural Rights' (12 November 2019) 66th Session E/C.12/ISR/CO/4.

Centrum För Rättvisa v. Sweden and Big Brother Watch v The United Kingdom[332] clearly show "a surprising willingness by the [C]ourt to re-tailor its human rights standards to meet the "collect it all" and "master the internet" agendas of western SIGINT agencies".[333]

In any case, for a person to be considered as being under a state's jurisdiction and for the ICCPR's extraterritorial application to kick in, a state must be exercising 'effective control' over that person, per the HRC's own interpretation.[334] Unfortunately, the notion of 'effective control' in the context of state surveillance and right to privacy continues to prove very tricky, as the notion was more useful in an era where to assume effective control, a state would have to have physical or actual control over an individual. But now that states can observe and reach individuals from almost anywhere in the world, the notion no longer makes sense, especially considering the fact that "[i]nterference with correspondence hardly amounts to effective control of a person in the same manner as physical detention… [and] [i]t is far from obvious that intercepting an individual's communications would render her subject to the jurisdiction of the state conducting surveillance."[335] Given all of these, Professor Lubin was probably right when he concluded that currently, there is no universal right to privacy and that we should probably begin to think of ways to develop tailored regulation of states foreign surveillance activities from a human rights perspective.[336]

To summarize the competing views above, the UN and relevant international bodies, human rights organizations, and privacy activists argue that international instruments, particularly those protecting the right to privacy, apply globally, because each state not only owes privacy obligations to those in their territories but also to those outside their territories when they exercise effective control on them. In other words, where a state seeks to curtail a foreigner's right to privacy through surveillance, the state must observe certain obligations because it would be exercising jurisdiction, triggered by its exercise of power or effective control on the person being surveilled. On the other hand, some states and privacy scholars reject the effective control and 'extended jurisdiction' argument and argue that they owe no (privacy) obligations

[332] Centrum För Rättvisa v. Sweden (n 279); Big Brother Watch and Others v The United Kingdom (n 251).
[333] Lubin (n 279).
[334] UN Human Rights Committee, 'General Comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant' (26 May 2016) 80th Session CCPR/C/21/Rev.1/Add. 13 (UN Human Rights Committee, General Comment no. 31).
[335] Severson (n 299) 498.
[336] Lubin, (n 15) 509.

in respect of individuals who are not both *within* their territories *and* subject to their jurisdiction.

Whichever side of the debate one decides to lean, the fact remains that there is some controversy regarding the application of international law when states act outside their territory.[337] This is a key issue that needs to be addressed with finality on the international stage.

4.2.3 The Problem of Mass (Foreign) Surveillance

In itself, mass surveillance has always been a huge problem in a world still trying to ensure minimum privacy guarantees.[338] Schneier put it best in his book, *Data and Goliath: the hidden battles to collect your data and control your world*:

> Mass surveillance is dangerous. It enables discrimination based on almost any criteria: race, religion, class, political beliefs. It is being used to control what we see, what we can do, and, ultimately, what we say. It is being done without offering citizens recourse or any real ability to opt out, and without any meaningful checks and balances. It makes us less safe. It makes us less free. The rules we had established to protect us from these dangers under earlier technological regimes are now woefully insufficient; they are not working. We need to fix that, and we need to do it very soon.[339]

When targeted at foreigners, mass surveillance constitutes an even bigger problem, as it has earned some form of legitimacy in many countries. As Professor Lubin notes, "When called out about any of these [mass surveillance] programs, policymakers would often respond to their constituencies with a shrug and a smile: *we only apply these programs to foreigners; you have nothing to worry about*", thus making obvious the insinuation that mass surveillance on foreigners is acceptable.[340] Clearly, this way of thinking has gained ground, as mass foreign surveillance has become a routine, largely unchallenged activity in many states. States like Canada[341] and the US,[342] have even explicitly written mass foreign surveillance into their laws,

[337] Wittes (n 326).
[338] Peter Königs excellently captures three key ways privacy is adversely impacted by mass surveillance: (a) the very act of mass surveillance or bulk collection of data diminishes privacy, however the data or information gathered is used; (b) data collected through mass surveillance can be accessed, thereby causing a breach of privacy on a different level; and (c) beyond mere access, data collected through mass surveillance can be used for objectionable purposes, for instance, where the data is leaked or someone with access uses the data to pursue personal, potentially detrimental interests. See: Peter Königs, 'Government Surveillance, Privacy, and Legitimacy' (2022) PT 1.
[339] Schneier (n 9) 4–5
[340] Lubin (n 15) 508.
[341] AARNSM 2019 s, 26 (1) and (2).
[342] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 s, 702.

displacing in some way the principles of legality, necessity, proportionality, and appropriate safeguards.

One reason mass foreign surveillance has become a common feature of many states' surveillance programs is because states consider that they have many options to investigate or prevent a crime if committed or intended to be committed within their borders. Meanwhile, the same plethora of means is not available where a criminal or someone with criminal intent is acting from outside a state's jurisdiction. As one author describes the situation:

> [a state's security service] can, amongst other things, examine a target's information against internal data sets, conduct certain inquires and issue certain subpoenas with a local police station, compel the disclosure of information from service providers… interview witnesses and acquaintances, analyze the feeds from closed-circuit television (CCTV) cameras, deploy visual surveillance against the person's address or place of work, and if necessary issue warrants for the seizure of assets and property and the arrest of persons. *Given the myriad options available to a state in conducting domestic investigations, the need to rely on covert communications interception, let alone in bulk form, is innately reduced.* There are simply less intrusive means available to the state to achieve the same legitimate aim.[343]

As of now, there are uncertainties as to whether mass foreign surveillance can be legitimate under any circumstance, or whether by its nature, it is impossible for it to be conferred with the cloak of legitimacy. Put differently, there is currently no consensus on the international stage on whether mass foreign surveillance violates privacy by default or whether it can be legitimate if it follows general surveillance principles.

Of course, by definition, mass surveillance cannot be legitimate as it would encounter many legal challenges, with the core challenge being that the use of mass surveillance techniques contradict and defeat the principles of legality, necessity, proportionality, and safeguards. Also, mass surveillance cannot survive scrutiny when viewed from the lens of the 'less intrusive means' principle, or as the UN puts it, "[m]ass data collection programmes appear to offend against the requirement that intelligence agencies must select the measure that is least intrusive on human rights".[344]

To reiterate, the problem with mass surveillance generally, or mass foreign surveillance particularly, is that it is indiscriminate surveillance, and there is simply no way to show that

[343] Lubin (n 15) 530.
[344] United Nations General Assembly (n 248).

indiscriminate surveillance is: necessary (especially considering the uncertainties regarding its ultimate effectiveness), used for limited purposes, proportionate, or reasonable.

Buttressing the above point, the UN had, in a 2014 report issued through the General Assembly, stated that "[t]he hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether."[345] A year before the above-cited report, the UN General Assembly had also issued another report analysing the impact of state surveillance activities on the rights to privacy, freedom of opinion and expression. In that report, the UN noted that mass surveillance upturns the traditional conception and means of surveillance and, therefore, cannot be reconciled with existing international laws on surveillance. According to the report "… [m]ass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception".[346]

On the other hand, the UN has sometimes seemed to suggest that mass surveillance can be legitimate in certain circumstances. For instance, consider that in its Resolution A/HRC/RES/34/7 of 2017, the UN called upon states "[t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, *including mass surveillance*", thereby hinting that mass surveillance might be permissible if certain safeguards are put in place.[347] And, in a 2014 report, Special Rapporteur Ben Emerson called "upon all States that currently operate mass digital surveillance technology to provide a detailed and evidence-based public justification for the systematic interference with the privacy rights of the online community by reference to the requirements of article 17 of the Covenant",[348] thereby implying again that mass surveillance could be legitimate. In the same report, the Special Rapportuer concluded that mass

[345] Ibid.
[346] United Nations General Assembly (n 20).
[347] This line of thinking is also reflected in the statement of Mr. Emmerson in the 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ben Emmerson : framework principles for securing the accountability of public officials for gross or systematic human rights violations committed in the course of States-sanctioned counter-terrorism initiatives'. Mr. Emmerson noted that, "[a]s an absolute minimum, article 17 requires States using mass surveillance technology to give a meaningful public account of the tangible benefits that accrue from its use. Without such a justification, there is simply no means to measure the compatibility of this emerging State practice with the requirements of the Covenant." Emmerson Ben and United Nations Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ben Emmerson: framework principles for securing the accountability of public officials for gross or systematic human rights violations committed in the course of States-sanctioned counter-terrorism initiatives' (17 April 2013) A/HRC/22/52 Para. 4; See also: United Nations General Assembly (n 248); United Nations General Assembly (n 55).
[348] United Nations General Assembly (n 248).

surveillance programs "*can be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people in any part of the world*".[349]

The problem should become clear at this point: not only is there no binding source of international law regulating mass (foreign) surveillance, resolutions and reports issued by the UN have taken somewhat contradictory and largely unhelpful positions. Perhaps this is the same issue that caused the UN to admit that "… *mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law*."[350]

Despite the above, it is interesting to note that the EU seems to have moved ahead of the UN by recognizing that mass surveillance, especially foreign, may "form a legitimate part of states' response to national security threats".[351] And at least one international body, the EctHR, has begun to "weigh in on a sweep of legislation passed, in recent years, that authorizes bulk interception of foreign communications in countries including France and the U.K."[352] Thus, in *Centrum För Rättvisa v. Sweden*[353] the EctHR upheld the Swedish legislation sanctioning mass surveillance in a case that laid down "a crucial precedent by drawing the lines of legality and illegality for intelligence agencies operating in the digital age".[354] Then, in the somewhat recent Big Brother case,[355] the EctHR all but legalized mass foreign surveillance in the EU. In that case, the Court explicitly held that "[o]wing to the proliferation of threats that [s]tates faced from networks of international actors… the Court considered that they [i.e. EU states] had a wide discretion ("margin of appreciation") in deciding what kind of surveillance scheme was necessary to protect national security."[356]

Based on the above foundation, the Court then went ahead to conclude that "[t]he decision to operate a bulk interception regime did not therefore *in and of itself* violate Article 8 [of the ECHR]."[357] Commenting on this case in her aptly titled paper, *Legalization of "Mass*

[349] Ibid. (emphasis added).
[350] Ibid.
[351] Daragh Murray, Pete Fussey, 'Lorna McGregor & Maurice Sunkin, 'Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective' (2021) 11 JNSLP 743, 744.
[352] Lubin (n 279).
[353] Appl. No. 35252/08 (2018) GC.
[354] Lubin (n 279).
[355] Big Brother Watch and Others v The United Kingdom (n 251) — The Big Brother Watch case is pending before the Grand Chamber of the European Court. It is possible, therefore, that certain conclusions as to the legitimacy of large-scale surveillance regimes, or aspects thereof, may be reconsidered.
[356] ibid
[357] Big Brother Watch and Others v The United Kingdom (n 251) Para. 3 (emphasis added).

Surveillance" by the European Court of Human Rights: What's Behind the Big Brother Watch and Others v. the United Kingdom Ruling?, Dr Vera Rusinova has argued that:

> Taking the approach that states enjoy a wide discretion in deciding whether to implement a mass interception regime… [the EctHR] thereby legalized the use of this measure by the member states of the Council of Europe. In assessing the content behind the EctHR's recognition of "mass surveillance" per se as not violating the Convention… the Court, acting both explicitly and implicitly, removed… the test of "lawfulness", "necessity in a democratic society" and "proportionality" and significantly lowered the bar for other components of the regime of mass interception of data.[358]

4.2.4 The Problem with Privacy Being a Unitary Right

International law provisions "are broad and vague".[359] Also, they "are very brief and they do not give detailed guidance on what privacy is or what aspects of privacy must be legally protected… "[360] As such, relevant international instruments, and their interpretation have left the scope of privacy—mainly conceived as a unitary right—undefined and unbounded.

Major reasons for privacy's vague nature have been attributed to ideological differences among states and fear that the UDHR or the ICCPR may not be adopted unless serious compromises were made. As Kinfe Michael puts it, "[r]ights—the right to privacy included—formulated in general phrases were thought to leave room for the technical details and exceptions to be determined by state parties, and hence limit the nature of state obligations."[361] While "compromise-induced deliberate vagueness but also—perhaps mainly—poor draftsmanship" ultimately led to the creation of a rather general and somewhat obscure right, the burden of interpreting the essence and scope of privacy right in the ICCPR and its limitation has fallen on the HRC. Unfortunately, while the HRC has defined other key components of Article 17 of the ICCPR, guaranteeing the right to privacy—including 'unlawful', 'arbitrary', and 'family life',[362] they have left the definition of privacy itself open.

The same open approach favoured by the UDHR and the ICCPR has been adopted by the ECtHR, which oversees the enforcement of the ECHR. The EctHR has admitted that the concept of private life, a term used interchangeably with privacy in the court's jurisprudence,

[358] Rusinova Vera, 'Legalization of "Mass Surveillance" by the European Court of Human Rights: What is Behind the Ruling in the Case of Big Brother Watch and Others v. the United Kingdom?' (2018) 4 IJ 1, 3 and 20.
[359] Milanovic (n 314) 83.
[360] Adrienn, Lukács, 'What is Privacy? The History and Definition of Privacy' (2016) LCS 256, 259.
[361] Yilma, (n 8) 129; Diggelmann and Cleis (n 174).
[362] UN Human Rights Committee, General Comment No. 16 on the Right to Privacy (n 197) para 6, 8, and 10.

is incapable of exhaustive definition.[363] Thus, in *Niemietz v. Germany*,[364] the Court flatly stated that a definition of private life was neither possible nor necessary. In *Costello-Roberts v. the United Kingdom*[365], the Court echoed the same sentiment, referencing *Niemietz v. Germany*, and reiterating that the concept of private life was not entirely suitable to be defined.

As I have noted elsewhere,[366] the undefined nature of privacy in international instruments is, in some way, a useful thing. Privacy's unbounded nature means that individuals can bring all sorts of claims under the right to privacy. However, as "strengths and weaknesses are two sides of the same coin"[367] , privacy's loose nature has also birthed arguments among states and privacy scholars on the exact scope of privacy rights that individuals enjoy under international law. In fact, until the UN General Assembly's Resolution 68/167, which addresses the right to privacy in the digital age,[368] it was not even clear whether privacy in human rights treaties applied to digital privacy.

Even now, there are still questions around such things as the status of metadata as "it has been suggested that the interception or collection of data about a communication [i.e., metadata], as opposed to the content of the communication, does not on its own constitute an interference with privacy."[369] And current international sources are unhelpful—while some UN documents have confirmed that metadata is critical and deserves equal protection as actual communication data in a number of UN resolutions—including Resolutions A/RES/75/176 of 28 December 2020[370] and A/HRC/RES/48/4 of 7 October 2021—[371] some states have not always accepted this interpretation. And so, in response to the Snowden disclosure and, particularly, the NSA's indiscriminate collection of phone records, the Obama administration retorted that nobody is collecting actual communication, just metadata. Yet, when it comes to surveillance, metadata is as important, if not more important, than actual content. As the Guardian put it: "in [the

[363] See: Niemietz v. Germany [Appl. No. 13710/88 (1992) ECHR]; Pretty v. the United Kingdom [Appl. No. 2346/02 (2002) ECHR]; Peck v. the United Kingdom [Appl. No. 44647/98 (2003) EHRR 287); Denisov v Ukraine (n 233); and Marper v The United Kingdom [Appl. Nos. 30562/04 and 30566/04 (2008) ECHR 1581].
[364] Ibid.
[365] App No 13134/87 (A/247-C)
[366] Ademola Adeyoju, 'Africa and the Protection of Digital Privacy: The State of Play' (2021) (Unpublished).
[367] Casey Lankow and Tim Johansson, 'Psychology at Work: Toward the Deepest Understanding of Strengths (It Depends)' (*Buzz Sprout*, 3 October 2019) <https://www.buzzsprout.com/342416/1785202> accessed 14 August 2022.
[368] United Nations General Assembly, 'The right to privacy in the digital age' (21 January 2014) 68th Session A/RES/68/167.
[369] United Nations General Assembly (n 153) Para. 20
[370] In this resolution, the UN General Assembly noted that: "… while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity." See United Nations General Assembly (n 237); United Nations General Assembly, 'The Right to Privacy in the Digital Age' (21 January 2019) 73rd Session A/RES/73/179; United Nations General Assembly, 'The Right to Privacy in the Digital Age' (10 February 2015) 69th Session A/RES/69/166.
[371] United Nations General Assembly (n 55); United Nations General Assembly (n 237).

surveillance] business at least, content isn't king. It's the metadata – the call logs showing who called whom, from which location and for how long – that you want. Why? Because that's the stuff that is machine-readable, and therefore searchable."[372]

The problem of privacy's scope has been noted by other scholars, including Professor Frédéric Gilles Sourgens, who once remarked as follows: "[t]he ICCPR poses significant interpretive challenges. It is not clear on its face what the ICCPR includes within the scope of privacy. It further does not provide concrete guidance as to what state conduct would be deemed unlawful. Finally, it does not clearly define exceptions to this general rule."[373] And in her 2019 paper on *Digital Privacy and Article 12 of the Universal Declaration of Human Rights*, Lorna Woods concludes that, "while in principle, privacy guarantees apply, there is still some uncertainty as to how. In this there are weaknesses in relation to the nature and intensity of intrusion… This, then, is the new challenge for article 12 UDHR, as well as the corresponding privacy rights in the ICCPR and regional instruments."[374]

To be sure, General Comments and Resolutions[375] have been issued and adopted to give some indications as to privacy's scope and states' obligations. Regarding the ICCPR particularly, the General Comment No. 16[376] states that the right to privacy has an extensive scope that covers the protection of communication, inviolability of the body, dignity of the person, and data protection.[377] More indications as to the scope of the right to privacy under the Covenant are offered when the HRC urged that to comply with Article 17 requires that the "integrity and confidentiality of correspondence should be guaranteed… surveillance should be prohibited… searches of a person's home should be restricted to a search for necessary evidence… [and] gathering of personal information on computers, data banks, and other devices must be regulated by law."[378]

On a related note, the General Comment No. 25[379] on children's rights in relation to the digital environment, issued in March 2021 by the Committee on the Rights of the Child ("CRC"),

[372] John Naughton, 'NSA surveillance: don't underestimate the extraordinary power of metadata' (*The Guardian*, 21 June 2013) <https://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama> accessed 14 August 2022.
[373] Sourgens (n 15) 13.
[374] Lorna Woods, 'Digital Privacy and Article 12 of the Universal Declaration of Human Rights' (2019) 90 The Political Quarterly 422, 429.
[375] United Nations General Assembly (n 122); United Nations General Assembly (n 237).
[376] All treaty bodies may issue General Comments, which address matters of relevance to all States parties to a particular treaty. Most General Comments contain expanded interpretations of particular rights in a relevant treaty
[377] See: UN Human Rights Committee, General Comment No. 16 on the Right to Privacy (n 197) para 6, 8, and 10.
[378] See generally: UN Human Rights Committee, General Comment No. 16 on the Right to Privacy (n 197).
[379] UN Committee on the Rights of the Child (n 195).

offers a roughly similar perspective on the right to privacy. The CRC acknowledges that the right entails protection of the children's agency, dignity, safety, and data, including information about "children's identities, activities, location, communication, emotions, health and relationships"[380]; and protection of the children against "automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance"[381]among other things.

Unfortunately, "international human rights instruments… do not grant the treaty bodies or any other entity the authority to issue legally binding views on the nature of state obligations under the treaties."[382] Thus, while General Comments and views on individual communications are recognized as being highly authoritative, being expert pronouncements on treaties issues, they are not legally binding.[383] In their work examining the standing, meaning, and effect of a CRC general comment, Paula Gerber et al. remarked that "… it remains accepted that *general comments do not legally bind states parties*. Furthermore, it would be overstating the standing of general comments to say that they have attained the status of a source of international law".[384]

Resolutions issued by the General Assembly are also not very helpful, as they are generally considered to be non-binding.[385] As one author has observed, "… the UN Charter refers to General Assembly resolutions as "recommendations", and the International Court of Justice has stressed the recommendatory nature of General Assembly resolutions repeatedly."[386]

Thankfully, EU jurisprudence provides some guidance. In a 2014 decision, the EctHR observed that, metadata "taken as a whole may allow very precise conclusions to be drawn concerning

[380] Ibid para 67.
[381] Ibid.
[382] Michael J. Dennis, 'Non-Application of Civil and Political Rights Treaties Extraterritorially During Times of International Armed Conflict' (2007) 40 ILR 453.
[383] See: Curtis A. Bradley & Jack L. Goldsmith, *Foreign Relations Law*: Cases *and Materials* (6th edn, Wolters Kluwer 2017) ("The HRC technically has no official power to issue binding legal interpretations of the ICCPR.").
[384] Paula Gerber, Joanna Kyriakakis and Katie O'byrne, 'General Comment 16 on State Obligations Regarding the Impact of the Business Sector on Children's Rights: What is its Standing, Meaning and Effect?' (2013) 14 MJIL 1. (emphasis added).
[385] It is worthy to note that the Security Council's resolution, on the other hand, are binding.
[386] Emma Finamore, 'Are UN resolutions legally enforceable?' (*All About Law*, 31 October 2018) <https://www.allaboutlaw.co.uk/commercial-awareness/commercial-insights/are-un-resolutions-legally-enforceable-> accessed 20 August 2022. See also Article 10 of the UN Charter (adopted 26 June 1945, enforced 24 October 1945) 1945 which defines the powers of the General Assembly thus: "The General Assembly may discuss any questions or any matters within the scope of the present Charter or relating to the powers and functions of any organs provided for in the present Charter, and,…*may make recommendations to the Members of the United Nations or the Security Council or to both on any such questions or matters*." (emphasis added).

the private lives of the persons whose data has been retained."[387] And in the landmark Big Brother case, the Grand Chamber of the EctHR addressed the issue of metadata—the court acknowledged that technology has evolved to the point where people's communication online is of "of a different nature and quality", and implied that privacy guarantees must cover metadata if they are to be meaningful.[388] According to the court,

> … greater volumes of communications data are currently available on an individual relative to content, since every piece of content is surrounded by multiple pieces of communications data. *While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted*.[389]

[387] Digital Rights Ireland and Seitlinger and others v Minister for Communications; Marine and Natural Resources and others (Joined cases C-293/12 and C-594/12) (2014) ECR I-238 Paras. 26-27, and 37. See also Executive Office of the President, *Big Data and Privacy: A Technological Perspective* (Executive Office of the President of the United States 2014) 19.
[388] Big Brother Watch and Others v The United Kingdom (n 251) Para. 341.
[389] Big Brother Watch and Others v The United Kingdom (n 251) Para. 342.

Chapter 5

> "Analysts have argued that a protected global right to privacy is urgent because the global surveillance state has itself become a reality… The rights of [foreigners] to privacy, in other words, extra-territorial rights, matter. Privacy rights are transnational issues, requiring transnational measures of protection."
>
> Binoy Kampmark[390]

5.1 Introduction

This chapter concludes that existing international law is no longer adequate and proposes that we start exploring the idea of making a new, comprehensive, and modern international instrument to guide (especially foreign and mass) surveillance activities and ensure real protection of a truly universal right to privacy. The chapter then highlights key elements to be considered as part of the new instrument.

5.2 Towards a New International Surveillance and Privacy Instrument

Throughout our analysis in the previous chapter, certain facts have emerged. First, states have embraced the tendency to offer lesser privacy protections to foreigners, vis-à-vis their citizens/residents, thereby rendering questionable the idea of a universal right to privacy. Second, there are controversies regarding the foreign application of the ICCPR, which instrument itself poses interpretative challenges. Third, although mass surveillance, particularly mass foreign surveillance, has become a standard part of some states' national security and foreign relations practices, international law has failed to accept mass (foreign) surveillance as a reality of state surveillance, let alone seek to regulate its deployment. Finally, there are issues with the privacy guarantees under international law as there is little clarity on what the 'right to privacy' actually entails.

[390] Binoy Kampmark, 'Limits on surveillance: A global right to privacy' (*Index on Censorship*, 29 January 2014) <https://www.indexoncensorship.org/2014/01/international-right-privacy/> accessed 17 August 2022.

These issues combine to paint a picture depicting that "existing international law approaches to the protection of global privacy rights face significant hurdles when applied to the digital age of signals intelligence, leading to an apparent normative gap in the law."[391] And while attempts have been made to fix some of these issues through soft law resolutions and general comments, there is "a strong argument that these steps are not progressive enough [as] most of these [efforts] can be seen as mainly regional agreements or soft law without any real binding obligations on states for the protection of privacy."[392] This point of view is conceivable given that soft law resolutions and general comments "do little to affect [sic] real change [as they are] still far from the kind of effective international treaty that has a chance at solving global issues."[393]

It seems necessary, therefore, that we start exploring the possibility of making a new, comprehensive, and modern international instrument to guide (especially) foreign surveillance activities and ensure real protection of a truly universal right to privacy. It is not surprising to note that more than 500 of the world's leading authors agree with this opinion and think that a "new international charter" is necessary to prevent states from undermining democracy by further eroding individuals' right to privacy and check intelligence agencies' powers.[394] Indeed, this sentiment has also been echoed at least once in the past by the former UN Special Rapporteur on human rights and counterterrorism, Professor Martin Scheinin, who noted as far back as 2009 that the HRC ought to begin a process for the creation of a "global declaration on data protection and data privacy."[395]

Unfortunately, despite the developments and revelations of the past decade, no long-lasting changes have yet been made at the global stage; and since states are unlikely to self-regulate "… the development of international surveillance law has to be actively pursued"[396] by the international community. That said, the new international instrument proposed in this thesis is

---

[391] Asaf Lubin, 'A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens' (2017) 42 (2) YJILO <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038500> accessed 23 August 2022 (Citing Sourgens (n 11).

[392] Kristian P. Humble, 'Human rights, international law and the right to privacy' 1, 9.

[393] Schrepferman (n 263).

[394] Matthew Taylor and Nick Hopkins, 'World's leading authors: state surveillance of personal data is theft' (*The Guardian*, 10 December 2013) <https://www.theguardian.com/world/2013/dec/10/surveillance-theft-worlds-leading-authors> accessed 22 August 2022; Writers Against Mass Surveillance, 'A Stand for Democracy in the Digital Age' (*Change.org*) <https://www.change.org/p/a-stand-for-democracy-in-the-digital-age-3> accessed 22 August 2022.

[395] Martin Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin: addendum' (18 Feb. 2010) A/HRC/13/37/Add.1 Para. 73; LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Statement by Professor Martin Scheinin (EUI), formerly UN Special Rapporteur on human rights and counter-terrorism, currently leader of the FP7 consortium SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency) (European Parliament, 2013).

[396] Schrepferman (n 263).

intended to be a binding document, which will take the form of a treaty, because soft laws are, by their very nature, prone to "promot[ing] compromise, or even compromised, standards… and can lead to uncertainty, as competing sets of voluntary standards struggle for dominance".[397]

Now, whilst the making of a binding international treaty is admittedly a more difficult and challenging process,[398] it is, in the final analysis, the only meaningful way to ensure states' adherence in the short- and long-term. This is because not only are the higher sanctions generated by hard laws necessary in our current context to deter behaviours that diminishes or infringes the increasingly important right to privacy; there is also sufficient clarity regarding specific rules to be adopted to safeguard privacy in the face of growing states' surveillance capabilities—a fact that bolsters our proposition and supports our view on adopting a binding treaty.[399]

Bold and ambitious, a new binding international treaty "would permit operational speed and assured legitimacy for *justified* intelligence gathering while plugging the legal black holes in current international law that currently are ripe for exploitation and abuse."[400] Much more than that, the treaty could also singlehandedly "strengthen international human-rights norms… [and] preserve the social, political and economic benefits that people the world over have reaped from the unobstructed global Internet."[401]

In making a new international treaty on privacy and foreign surveillance, we are not trying to make any radical changes, but instead attempting to regulate what is already happening and ensure certain minimum safeguards. To develop the treaty, insights can be gained from: (a) regional privacy laws including the Asia-Pacific Privacy Framework, the African Convention of Cybersecurity and Personal Data Protection, and the EU General Data Protection Regulation; (b) privacy and internet bills of rights already prepared by states, civil societies, and privacy experts;[402] and (c) relevant soft law resolutions and general comments.

---

[397] Hema Nadarajah 'Fewer Treaties, More Soft Law: What Does it Mean for the Arctic and Climate Change?' (*Artic Portal)* < https://issuu.com/arcticportal/docs/ay2020/s/11293424> accessed 24 August 2022.

[398] Ibid. Because the process of making an international treaty is time-consuming, resource-intensive, and generally challenging—not to mention that states have to willingly agree to be bound for the treaty to have any effect—it might be useful to consider the making of a non-binding instrument as an intermediate step to negotiating a treaty.

[399] Besides the above points, it is also worthy to note that some have even claimed that, viewed from a certain perspective, soft laws are not laws at all. As one writer puts it, "[t]he subject of soft law has always been an awkward one for international legal scholars. On the one hand, it is not law at all, strictly speaking. Under traditional approaches, as Prosper Weil states, these obligations "are neither soft law nor hard law: **they are simply not law at all**" See: Andrew T. Guzman and Timothy L. Meyer, 'International Soft Law' (2010) 2 JLA 171, 172.

[400] Stephen J. Schulhofer, 'An international right to privacy? Be careful what you wish for' (2016) 14 I.CON 238, 243.

[401] Ibid.

[402] Yilma (n 8) 128.

In the following paragraphs, I propose six key elements that must be considered in the formulation or development of a new international treaty.

5.2.1 De-emphasize the Distinction Between Domestic and Foreign Surveillance

As seen above, many states have taken advantage of the lack of a binding international instrument on foreign surveillance to create in their domestic laws lesser privacy protection for foreigners in view of their foreign surveillance activities. One of the first things that an international treaty on surveillance and privacy should do, therefore, is to reduce or eliminate the disparity in treatment of citizens/residents and foreigners.[403]

This is especially important now that the distinction between domestic and foreign surveillance makes less and less sense as the world becomes increasingly connected and communications take unpredictable routes from one point to another. In fact, "… as many foreigners have learned, on the Internet you may not even know that your communication has crossed national borders, because a domestic communication may well be routed through another country without your knowing it."[404] This line of thought is reflected in the Big Brother case, where the court has also observed that analysing "whether a particular communication is external or internal may… only be possible to carry out with the benefit of hindsight. Today's closer interconnectedness of living and communication conditions across borders is certainly not an argument for treating external and internal communications differently, but rather the opposite".[405]

5.2.2 Resolve the Extraterritoriality Problem by Redefining/Jettisoning the Concept of Jurisdiction

A new international treaty should also settle, once and for all, the debates on whether or not states bear privacy obligations when they conduct foreign surveillance because exercising power or effective control over a foreigner is tantamount to exercising jurisdiction, thereby bringing their surveillance action under the scope of the ICCPR. One part of this would be to explicitly adopt the UN HRC's interpretation of Article 2 of the ICCPR, as captured in the HRC's General Comment No 31:

---

[403] Schrepferman (n 263).
[404] Cole (n 289); see also: Timothy B. Lee, 'Why "we only spy on foreigners" doesn't work any more for the NSA' (*The Washington Post*, 7 July 2013. <https://www.washingtonpost.com/news/wonk/wp/2013/07/07/european-outrage-about-the-nsa-could-force-us-to-rethink-our-surveillance-laws/> accessed 24 August 2022
[405] Big Brother Watch and Others v The United Kingdom (n 251).

> States parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. *This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State party, even if not situated within the territory of the State party*.[406]

In order to avoid extending the scope of jurisdiction to anywhere in the digital sphere—which would then completely overturn the meaning of the concept of states' jurisdiction—[407] the new treaty could develop a new, reasonable conception of jurisdiction. To achieve this, the approach could be that states would not only have to take responsibility for their action where they exercise effective control—which is the basis of imputing jurisdiction under current international law—but also in places and spheres where states' surveillance actions have effect.

Thus, even where a state does not exercise effective control in another country or territory, but is able to reach, monitor, or influence the actions of an individual in that other country or territory, the state should be deemed to have and to have exercised jurisdiction in that other country or territory and regarding that individual. In other words, wherever virtual surveillance would produce the same effect as physical surveillance, states should be held accountable for any privacy infringements that might have occurred, even where they do not have effective control of or in the jurisdiction or territory where the infringement has occurred.[408] This approach is necessary because "the established criteria of control over territory or a person are no longer adequate in deciding whether a person is within the jurisdiction of a State…"[409]

Considering that jurisdiction is a central concept with multiple implications and attempts to expand it might prove difficult, perhaps a different—and possibly less controversial or complicated—way to go about attaching states' responsibility is to jettison the concept of jurisdiction altogether for this purpose and establish at the minimum baseline standards or principles of privacy protection. These privacy

[406] UN Human Rights Committee, General Comment no. 31 (n 334) Para. 10. See also: International Court of Justice (ICJ) Advisory Opinion (n 316) (emphasis added).
[407] Martin Weiler, 'The Right to Privacy in the Digital Age: The Commitment to Human Rights Online' (2014) 57 GYBIL 651, 661.
[408] Ibid.
[409] Ibid.

principles would serve to guarantee foreigners' privacy and guide states' actions whenever they conduct foreign surveillance.

5.2.3 Stipulate Minimum Safeguards for Mass (Foreign) Surveillance

Another focus of the international treaty on privacy and surveillance should be mass (foreign) surveillance, current lack of regulation of which is "[a] gap [that] invites submissions that global signals intelligence surveillance programs are presumptively permissible because they are not prohibited by any one rule of international law."[410]

Given that many states have gone ahead to adopt mass foreign surveillance as a standard practice, it seems pointless to keep casting a blanket prohibition on it on the international stage. Instead, the international community should learn from the EU,[411] which has become "the site of actively developing international human rights law."[412] In the EU, the Court of Justice of the European Union and ECtHR has reiterated that states have wide 'margin of appreciation' and recognized mass foreign surveillance as a standard form of state surveillance. According to the ECtHR, "[u]nlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, *bulk interception is also – perhaps even predominantly – used for foreign intelligence gathering and the identification of new threats from both known and unknown actors*."[413] Much more than mere recognition, the ECtHR has even stated that it "accepts that bulk interception is of vital importance" to EU member states.

Beyond recognizing/accepting mass foreign surveillance as normal, the new international treaty should prescribe rules around when and how states may conduct mass foreign surveillance. At the very minimum, any domestic law authorizing mass surveillance: (a) must be public and sufficiently precise in defining the range of national security threats and the circumstances in which those threats may trigger mass surveillance; (b) must be restricted in each case to specific geography and time; and (c)

---

[410] Sourgens (n 15) 10 (citing Cmd. Michael Adams, 'Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace' (2014) 5 HNSJ 377, 403 and 404 (applying the principle that no prohibition equals permission in international law)).
[411] The UN has consistently welcomed and referred to EU jurisprudence in reaching its own conclusion. In recent past, the International Court of Justice has expressed approval for the mass surveillance safeguards set out in the Big Brother case by the ECtHR (see: International Commission of Jurists, 'European Court of Human Rights issues landmark ruling on mass surveillance' (*International Commission of Jurists*, 26 May 2021) <https://www.icj.org/european-court-of-human-rights-issues-landmark-ruling-on-mass-surveillance/> accessed 13 August 2022.)
[412] Schulhofer (n 400) 249.
[413] Big Brother Watch and Others v The United Kingdom (n 251) Para. 322 (emphasis added).

must be resorted to only as the last resort. Regarding (c), it should be stipulated that states must always first consider and adopt the least intrusive means when conducting mass surveillance, and where they have to interfere with people's privacy through mass surveillance—as privacy is interfered with even through the mere collection (as opposed to analysis or dissemination) of bulk information—states must present a concrete and overriding justification.

In prescribing rules on mass foreign surveillance, the "Weber Criteria", as laid down in the case of *Weber and Saravia v. Germany*,[414] can also help form a base standard for and inspire further development. For clarity, the Weber Criteria are essentially a list of minimum safeguards that must be set out in law and observed when carrying out mass surveillance in order to prevent abuse. The criteria require the express stipulation of: the categories of offences that may necessitate interception; ascertainment of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for analysing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed.[415]

In addition, judicial authorization, though not a perfect safeguard, should always be obtained prior to the conduct of any mass surveillance operation, and an independent authority should review the operation after the fact. And as suggested in the Big Brother case, "[e]ach stage of the bulk interception process… [must] be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the 'interference' to what is 'necessary in a democratic society'."[416] Thus, not only must 'tags' or 'selectors'—i.e., the pre-set identifiers or predetermined base criteria determining what and whose information is collected—be carefully selected and approved, there must also be procedures in place to guarantee that only necessary information is subsequently analysed. Meanwhile, where information collected contains confidential journalistic, legal, or medical work, their analysis should be separately authorized. Finally, all information swept as part of a particular mass surveillance operation must be deleted or erased within a set timeframe—a rule that

[414] *Weber and Saravia v. Germany* (n 258).
[415] Ibid.
[416] Big Brother Watch and Others v The United Kingdom (n 251) Para. 356.

would constitute a clear departure from states' current practices of storing data collected perpetually.

5.2.4. Define Privacy and Specify its Scope

Perhaps the most important thing that a new international treaty on privacy and surveillance should set out is a conceptualization of the privacy right it seeks to protect.[417] The scope of privacy defined in this thesis—i.e., information, communication, and individual privacy—seems appropriate. Regardless of the scope or taxonomy of privacy adopted, what is important is that account is taken of the current and foreseeable digital privacy concerns that have emerged, and continue to emerge, given the unprecedented advancements in technology and increase in state surveillance capabilities.

Although defining privacy may have some drawbacks, in that the potentially infinite number of claims that could be brought under an uncategorized privacy is immediately curtailed, clarity and specificity would mirror current privacy laws around the world and eliminate confusions regarding the scope, extent, or reach. Reconceptualizing privacy also has the distinct advantage of including and extending equal privacy protection to subsets of digital communications such as metadata and subsets of privacy rights such as the right to encryption, which though it forms the backbone of the internet, is currently under serious attack from many states.[418] As Kinfe Michael has observed about protecting subsets of privacy right:

> *Rights which could be termed as 'subsets' to the classic right to privacy such as the 'right to anonymity', 'right to encryption' and 'right to algorithm' are not expressly*

[417] As they are more comprehensive, regional and national privacy laws should naturally complement any scope or aspects of privacy considered not so crucial to merit specific inclusion or protection under international law.

[418] Anyone with a basic understanding of the level of technological advancements and the sheer extent that people who want to keep their communications secret can go can knows that taking away communications encryption on the internet is a futile, ineffective measure. Criminals or people with criminal intent will simply find one of the possibly hundreds of secure network currently available on the web, build their own communication network, or even communicate in clear sight of law enforcement using codes—their own encryption style—that appear as gibberish to the untaught eye. In any case, as Tom Scott has argued, eliminating encryption would not stop bad things from happening, as the problem with fighting crime and maintaining safety is not the absence of information on crime, but the capability to investigate every possible lead. [<https://www.youtube.com/watch?v=LkH2r-sNjQs>]. After all, Salman Abedi, the Manchester bomber, was reported to the authorities 5 times, including by his own friends and family, and the UK intelligence agency, the "MI5 is managing around 500 active investigations, involving some 3000 subjects of interest at any one time". Reuters Staff, 'UK security services have thwarted five plots since March Westminster attack: source' (*Reuters*, 25 May 2017) <https://www.reuters.com/article/us-britain-security-manchester-plots-idUSKBN18L1H0> accessed 26 August 2022.

regulated within the existing human rights norms or are only implicit in them. Wider recognition of such rights… could be useful in two ways.

First, courts presented with cases that implicate new communication technologies could potentially be able to understand the human right to privacy in a broader and contemporary context. Developments in digital privacy advocacy might assist in the process of 'digital rights translation' through litigation. Secondly, they might also create expectations of privacy among netizens [i.e., a person actively involved in online communities or the Internet in general], and later to put pressure on governments and corporations to act in respect to such expectations.[419]

5.2.5. Prescribe Rules on Intelligence Sharing among States

By way of introducing clear rules or safeguards to guide current mass foreign surveillance practices and further strengthen the right to privacy, the new international treaty should also prescribe rules on intelligence sharing.[420] This is especially important given that intelligence-sharing agreements have become a common means of surveillance for states. For context, it is worthy to note that in the EU alone, "at least thirty-nine [EU states] have either concluded intelligence sharing agreements with other [s]tates, or have the possibility for such agreements."[421]

Interestingly, despite their growing popularity, these agreements are entered into by states who have no need or obligation to comply with or concede to any international restrictions; yet these agreements allow states to not only extend their foreign surveillance capabilities but to also evade domestic regulations. To see how this can happen, consider how a matrix of boundless surveillance was once created between the UK, the US, and Germany because "Britain's GCHQ intelligence agency can spy on anyone but British nationals, the NSA can conduct surveillance on anyone but Americans, and Germany's BND (Bundesnachrichtendienst) foreign intelligence agency can spy on anyone but Germans."[422]

---

[419] Yilma (n 8) 126.

[420] The UN has also noticed the problem of lack of international regulation of intelligence-sharing arrangement. In their Resolution A/69/397, the UN observed that "[t]he absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority" (United Nations General Assembly (n 248).

[421] Big Brother Watch and Others v The United Kingdom (n 251) Para. 245.

[422] Von Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark and Jonathan Stock, 'How the NSA Targets Germany and Europe' (*Spiegel International*, 01 July 2013) <https://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html> accessed 27 August 2022.

In addition to prohibiting the tendency by states to want to grant preferential privacy treatments to the citizens/residents of other states who are party to an intelligence-sharing agreement, the new treaty should also impose certain privacy requirements to be incorporated into these agreements. These clauses may include, but not limited to "homomorphic encryption,[423] differential privacy,[424] zero knowledge proofs, and other 'structured transparency'[425] approaches";[426] and, of course, "[intelligence] usage restrictions and assurances to ensure that data were handled and deleted in accordance with the rule of law."[427]

Although intelligence-sharing alliances, such as the UK and the US, have recently recognized privacy as an important consideration in intelligence sharing—and even announced plans to partner on a prize challenges to develop privacy-enhancing technologies ("PETs")[428]—there is no evidence that they have actually implemented privacy measures or furthered their self-imposed PETs-development ambitions.[429]An international treaty can ensure and monitor states' intelligence-sharing protocols and certify them as complying with the new international standard.

5.2.6. Offer Protections for Whistle-Blowers

Apart from the suggestions highlighted above, an additional key consideration revolves around the question of how to protect whistle-blowers, whose role in the grand scheme of things is clearly important, given how they have been instrumental in exposing states' surveillance excesses, abuse of public trust, and violation of both domestic and international privacy laws. Till today, Snowden is still running from a certain

[423] Homomorphic encryption is a relatively new technology that makes it possible to conduct mathematical operations on encrypted data without first decrypting that data, such that, once completed, the result of the mathematical computation also remains encrypted.
[424] Often used in the context of personal data contained in a database, differential privacy describes the highly advanced system for ensuring that information about particular individuals is unfindable or undetectable within a dataset that is shared publicly.
[425] Structured transparency is based on the notion that privacy is not about complete anonymity but about careful distribution and seeks to overcome the privacy-transparency dilemma. By implementing a structured transparency framework, one is able to ensure that information is made transparent without the possibility or risk of misuse. An example would be the examination by a sniffer dog of a piece of luggage without ever needing to reveal or see the private content. See: Private AI Series, 'Structured Transparency: Ensuring Input and Output Privacy' (*OpenMined*, 14 March 2021) <https://blog.openmined.org/structured-transparency-input-output-privacy/> accessed 27 August 2022.
[426] Jake Harrington and Riley McCabe, 'The Case for Cooperation: The Future of the U.S.-UK Intelligence Alliance' (*Center for Strategic and International Studies*, 15 March 2022' <https://www.csis.org/analysis/case-cooperation-future-us-uk-intelligence-alliance> accessed 27 August 2022.
[427] Big Brother Watch and Others v The United Kingdom (n 251) para 249, 250, 251 and 252.
[428] Press Release, 'US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies' (*The White House*, 8 December 2021) <https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/> accessed 27 August 2022.
[429] Harrington and McCabe (n 426).

prosecution and incarceration in the US,[430] and he—and others like him—should not have to constantly look behind their shoulders, in a world where international law has stepped up to protect and offer some refuge to whistle-blowers.

Although online platforms such as Wikileaks, Globaleaks, and Associated Whistleblowing Press have been built to enable anonymous disclosure and support investigative journalism, they have not been very effective in protecting whistle-blowers. This is in part because states are able to attack or request information from or on these platforms through or from website hosting services and website owners. As a classic instance, immediately following Snowden's disclosure in 2013, the US government approached *Lavabit*, a secure email service, to turn over its encryption keys and secure socket layer,[431] because the service had been used by Snowden to leak details of NSA's mass surveillance program, PRISM.[432].

Another obvious problem with these platforms is that, no matter how secure they are, they cannot prevent reprisals against whistle-blowers, and states somehow manage to always uncover whistle-blowers' identities and punish them severely. For instance, "Chelsea Manning… who provided WikiLeaks with classified military documents in 2009 and 2010, is currently serving a 35-year prison sentence. [And] American hacktivist Jeremy Hammond, 30 is serving a decade for his part in stealing private data… that was later published by WikiLeaks… "[433]

Despite the above, there is no single international legal instrument on whistleblowing,[434] and no clear protection for whistle-blowers like Snowden, who have disclosed states' surveillance excesses and privacy right infringement, even though [a] growing number of international instruments [has] recognise[d] the importance of

[430] Anton Troianovski, 'Edward Snowden, in Russia Since 2013, Is Granted Permanent Residency' (*The New York Times*, 2 November 2020) <https://www.nytimes.com/2020/10/23/world/europe/russia-putin-snowden-resident.html> accessed 25 August 2022.
[431] *Lavabit's* owner refused to comply with the government's request, shut down the service, and only relaunched in 2017 (see https://theintercept.com/2017/01/20/encrypted-email-service-once-used-by-edward-snowden-to-relaunch/> accessed 27 August 2022.
[432] Kim Zetter, 'A Government Error Just Revealed Snowden Was the Target in the Lavabit Case' (*Wired*, 17 March 2016) <https://www.wired.com/2016/03/government-error-just-revealed-snowden-target-lavabit-case/> accessed 27 August 2022.
[433] Association for Progressive Communications, 'The protection of sources and whistleblowers' (*OHCHR Official Website)* <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Protection/AssociationProgressiveCommunications.pdf> accessed 29 August 2022.
[434] Kafteranis Dimitrios, 'The International Legal Framework on Whistle-Blowers: What More Should Be Done?' (2021) 19 SJSJ 729.

whistle-blowers and require or encourage states to adopt measures to protect disclosure."[435]

5.2.7. Outline Clear and Feasible Enforcement Procedures

Finally, in order to be effective, the new international treaty should also contain some enforcement mechanisms. Thus, where their surveillance activities are suspected to have violated established norms or boundaries, states should be subject to the obligation to afford claimant(s) the opportunity to seek redress in a competent, preferably domestic, forum, which "while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings".[436] Such authority should have the "power to grant a binding remedy (including, where appropriate, an order for the cessation of surveillance or the destruction of the [information collected])"[437] The new treaty could also impose and enforce sanctions on serious privacy violations occasioned by clearly excessive state surveillance operations.

5.3 Conclusion

Since the 19th century, many states have built and expanded their surveillance capabilities. Riding on the back of incredible advancements in technology, the nature of state surveillance has radically evolved, and now features such sophisticated techniques as internet and telephone surveillance to government hacking and fibre optic cables tapping.

The existence of and continued investment in state surveillance are justified chiefly on the basis of security and the nothing to hide arguments. The security argument revolves around claims that surveillance is vital to prevent threats and necessary to secure peace and order. However, this argument has been countered from different angles. For examples: (a) surveillance, particularly mass surveillance, undermines the very security it is intended to ensure; (b) there is scant evidence that surveillance actually works; and (c) there is always the danger that intelligence gathered from state surveillance could be used for secondary objectives—e.g., economic and industrial espionage, profiling on political grounds, or illegal cracking down on dissidents.

On the other hand, the nothing to hide argument is used to justify state surveillance by those who attempt an uneducated balance between the privacy interests of individuals against the

[435] Association for Progressive Communications (n 433).
[436] Big Brother Watch and Others v The United Kingdom (n 251) Para 359.
[437] United Nations General Assembly (n 248).

security of many claim. The argument is also used to buttress the view of those who argue that only miscreants have something to hide, and that in the absence of any wrongdoing, an individual should be open to constant surveillance. However, this argument has been discredited as stemming from ignorance about the essence of human rights, and a lack of understanding of the concept of privacy and the multi-dimensional interests protected by privacy.

Without arguing that state surveillance is inherently bad, this thesis recognizes that surveillance raises major concerns for and threatens fundamental human rights, particularly the right to privacy. The thesis notes that the threats posed to privacy are magnified in light of the increasing digitalization and states' tendencies to implement preventive enforcement policies by seeking increased access to private communications, waging a war on encryption (the backbone of the internet), and conducting unsanctioned mass surveillance operations. Yet, there is no denying the fact that privacy matters. This is so much so that privacy has since been recognized and protected as a fundamental right in international instruments, with the provisions in and interpretations of these instruments promoting the notion of a global right to privacy, i.e., the idea that everyone everywhere is entitled to privacy.

Unfortunately, as it has not developed as such since the early- to mid-20th century, international law encounters numerous challenges and proves increasingly inadequate in the face of new and emerging privacy concerns and the evolution of states' surveillance capabilities. As such, whatever is left of privacy in an increasingly 'curious' and connected world is endangered now more than ever, largely due to states' surveillance practices, many of which have become irreconcilable with current international law.

As discussed in chapter 4 of this thesis, the challenges that existing international law faces are manifold: first, states have embraced the tendency to offer lesser privacy protections to foreigners, vis-à-vis their citizens/residents, thereby rendering questionable the idea of a universal right to privacy. Second, there are controversies regarding the foreign application of the ICCPR, which instrument itself poses interpretative challenges. Third, although mass surveillance, particularly mass foreign surveillance, has become a standard part of some states' national security and foreign relations practices, international law has failed to accept mass (foreign) surveillance as a reality of state surveillance, let alone seek to regulate its deployment. Fourth, there are vagueness issues with the privacy guarantees under international law as there is little clarity on what the 'right to privacy' actually entails.

Given these challenges, this thesis proposes that a new international treaty is necessary to set some baseline standards and formulate clear privacy requirements vis-à-vis state surveillance activities. In doing this, consideration should always be given to the fact that privacy cannot be said to be a universal right if states continue to offer lesser protection to foreigners.

There are certain key elements that must be considered in drafting a new international treaty. First, the new treaty should de-emphasize the distinction between domestic and foreign surveillance. By doing this, states would be less inclined to create, and find it hard to justify or legitimize offering, separate and unequal protections to citizens/resident and foreigners. Second, the new treaty should stipulate minimum safeguards for mass (foreign) surveillance. The baseline standards are necessary to clarify on the international stage the rules of engagement when it comes to mass surveillance of foreigners. Third, rules on intelligence sharing among states should be prescribed to require the necessary inclusion of privacy consideration when drafting intelligence-sharing agreements.

The new treaty should also consider: (a) clarifying its conception of privacy, which should take into account current and foreseeable digital privacy concerns that have emerged, and continue to emerge, given the unprecedented advancements in technology and increase in state surveillance capabilities; (b) resolving the problem of extraterritoriality by redefining or altogether jettisoning the concept of jurisdiction in this context, which has generated controversies on the obligations of states when conducting foreign surveillance; and (c) offering protections for whistle-blowers, whose role in the grand scheme of things is clearly important, given how they have been instrumental in exposing states' surveillance excesses, abuse of public trust, and violation of both domestic and international privacy laws.

The solutions discussed above are proposed to be considered in the form of new prescriptive and proscriptive legal instrument, rather than process-oriented or political solutions.

This thesis goes further than previous work as it critically examines the ills of state surveillance and the essence of privacy in a modern society and why it deserves protection; it evaluates doctrinal gaps in current international law; and it proposes concrete considerations in the making of a new international treaty. Put differently, this thesis is important because it investigates the doctrinal holes or problems that beset current international law on privacy—problems tangible enough to necessitate a serious consideration of a new treaty—and then analyses what the new treaty should look like in terms of specific provisions.

BIBLIOGRAPHY

LEGISLATION

An Act Respecting National Security Matters 2019

Canadian Security Intelligence Service Act 1985

The Canadian Charter of Rights and Freedoms 1982

Communications Security Establishment Act 2019

An Act To Amend The Foreign Intelligence Surveillance Act Of 1978 to Establish a Procedure for Authorizing Certain Acquisitions of Foreign Intelligence, and for Other Purposes 2008

An Act Respecting the Criminal Law 1985

Foreign Intelligence Surveillance Act 1978

An Act Respecting the Office of the Intelligence Commissioner 2019

Internal Security Code [(Legislative part (Articles L111-1 to L898-1) Amended by Ordinance No. 2018-1125 of 12 December 2018 - art. 22]

Joint Committee on the Draft Investigatory Powers Bill: Written Evidence (2015) 180

Loi n°2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement (codified in the Code of Internal Security, Book VIII "On Intelligence" (article L. 801-L. 898-1))

An Act Respecting National Defence 1985

An Act to Establish the National Security and Intelligence Review Agency Act, 2019

An Act to Deter and Punish Terrorist Acts in the United States and Across the Globe, to Enhance Law Enforcement Investigatory Tools, and for Other Purposes 2001

An Act to Extend the Present Laws of Canada that Protect the Privacy of Individuals and that Provide Individuals with a Right of Access to Personal Information about Themselves 1985

A Bill for an Act of Parliament to Make Various Amendments to Statute Law 2020

JURISPRUDENCE

Appl. No. 10090/16 Centre for Democracy and the Rule of Law v. Ukraine (2020) ECHR

Appl. No. 11105/84 Huvig v. France (1990) ECHR A/176-B

Appl. No. 11801/85 Kruslin v. France (1990) ECHR

Appl. No. 12244/86; 12245/86; 12383/86 Campbell v. the United Kingdom (1990) ECHR

Appl. No. 13134/87 Costello-Roberts v. the United Kingdom (1993) ECHR 16

Appl. No. 13308/87 Chorherr v. Austria (1993) ECHR
Appl. No. 13710/88 Niemietz v. Germany (1992) ECHR
Appl. No. 173/15 Liblik and Others v Estonia (2019) ECHR 383
Appl. No. 17895/14 Evers v. Germany (2020) ECHR
Appl. No. 2346/02 Pretty v. the United Kingdom (2002) ECHR
Appl. No. 25498/94 Messina v. Italy (no. 2) (2000) ECHR
Appl. No. 26772-95 Labita v. Italy (2000) ECHR
Appl. No. 27057/06 Gorlov and Others v Russia (2019) ECHR
Appl. No. 27915/95 Niedbała v. Poland (2000) ECHR
Appl. No. 28524/95 Peers v. Greece (2001) ECHR
Appl. No. 30194/09 Shimovolos v. Russia (2011) ECHR 987
Appl. No. 32555/96 Roche v. the United Kingdom (2005) ECHR
Appl. No. 33810/07 Association "21 December 1989" and Others v. Romania (2011) ECHR
Appl. No. 35252/08 Centrum for Rattvisa v. Sweden (2018) GC
Appl. No. 36936/05 Szuluk v. the United Kingdom (2009) ECHR
Appl. No. 37138/14 Szabó and Vissy v. Hungary (2016) ECHR
Appl. No. 37328/97 A.B. v. the Netherlands (2002) ECHR 9
Appl. No. 37717/05 Dudchenko v Russia (2017) ECHR 965
Appl. No. 40365/09 Ekinci and Akalın v. Turkey (2012) ECHR 246
Appl. No. 43514/15 Catt v The United Kingdom (2019) ECHR
Appl. No. 44647/98 Peck v. the United Kingdom (2003) EHRR 287
Appl. No. 44787/98 P.G. and J.H. v. the United Kingdom (2001) ECHR.
Appl. No. 4558/98 Valašinas v. Lithuania (2001) ECHR
Appl. No. 47143/06 Roman Zakharov v. Russia (2015) GC
Appl. No. 5488/72, X v. Belgium, Yearbook XVII (1974) 222.
Appl. No. 54934/00 Weber and Saravia v Germany (2006) ECHR
Appl. No. 55721/07 Al-Skeini v. United Kingdom (2011) GC
Appl. No. 58170/13;62322/14;24960/15 Big Brother Watch and 15 Others v The United Kingdom (2021) ECHR.
Appl. No. 58361/12;25592/16;27176/16 Zoltán Varga v Slovakia (2021) ECHR
Appl. No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 Silver and Others v. the United Kingdom (1983) ECHR
Appl. No. 59589/10 Konstantin Moskalev v Russia (2017) ECHR

Appl. No. 61496/08 Bărbulescu v. Romania (2017) ECHR 268.
Appl. No. 62540/00 Association pour l'intégration européenne and les droits de l'homme and Ekimdzhiev v. Bulgaria (2007) ECHR.
Appl. No. 70078/12 Ekimdzhiev and Others v. Bulgaria (2022) ECHR 1
Appl. No. 7215/75 X v. The United Kingdom (1978) ECHR
Appl. No. 76639/11 Denisov v. Ukraine (2018) ECHR
Appl. No. 8290/78, A, B, C and D v. the Federal Republic of Germany, DR 18 (1980) 176
Appl. No. 8355/78 X v. the Federal Republic of Germany (unpublished)
Appl. No. 9237/81, B v. the United Kingdom, DR 34 (1983) 68
Appl. Nos. 30562/04 and 30566/04 Marper v The United Kingdom (2008) ECHR 1581
Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (2005) ICJ.
Carpentar v. United States (2018) 585 US
CCR v. Obama (formerly CCR v. Bush) (2006) 3:07-cv-01115 U.S District Court for the Northern District of California
Clavir v Levi (1979) 84 F.R.D. 612
Digital Rights Ireland and Seitlinger and others v Minister for Communications; Marine and Natural Resources and others (Joined cases C-293/12 and C-594/12) (2014) ECR I-238 Paras. 26-27, and 37
Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) (2014) The Grand Chamber C-293/12 and C-594/12
Dombrowski v Eastland (1967) 387 U.S. 82
Eisenstadt v Baird (1972) 405 U.S. 438
Griswold v. Connecticut (1965) 381 U.S. 479
Haasev Webster (1985) 608 F. Supp. 1227.
Hassan v City of New York (2015) 804 F.3d 277.
Kinoy v. Mitchell (1971)
Klass and Others v. Germany (1979) 2 EHRR 214
Klayman v Obama (2015) No. 14-5004 D.C. Cir.
Liberty and Others v. the United Kingdom Appl. No. 58243/00 (2008) ECHR.
Mohamud v United States (2016) 843 F.3d 420

Oleynik v. Russia Appl. No. 23559/07 (2016) ECHR 553

Olmstead v. United States (1928) 277 U.S. 438

Olmstead v. United States, 277 U.S. 438, 470 (1928)

Osborn v. United States (1966) 385 U.S. 323

R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67

R. (Smith) v. Secretary of State for Defence (2010) UKSC 29

Roe v Wade (1973) 410 U.S. 113

Rotaru v. Romania Appl. No. 8341/95 (2000) ECHR

United States v Moalin (2021) 9th Circ. 10CR4246-JM

INTERNATIONAL LAW SOURCES

African Declaration on Internet Rights and Freedoms

American Convention on Human Rights, "Pact of San Jose, Costa Rica" (adopted 22 November 1969, entered into force 18 July 1978) 1969

American Declaration of the Rights & Duties of Man. Organization of American States. 1948

Arab Charter on Human Rights (adopted 22 May 2004, came into force 15 March 2008) 2004.

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

Association of Southeast Asian Nations (ASEAN), ASEAN Human Rights Declaration (adopted and came into force 18 November 2012) (AHRD) 2012

Charter of Fundamental Rights of the European Union (CFR) 2012/C 326/02

Convention on the Right of the Child (adopted 20 November 1989, entered into force on 2 September 1990) (CRC) 1989

Declaration of Principles on Freedom of Expression and Access to Information in Africa

European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 1950

International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (adopted 18 December 1990, entered into force 1 July 2003) 1990

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

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

BOOKS

Bennett CJ, *Regulating Privacy* (Cornell University Press 1992)

Bentham J, *The Collected Works of Jeremy Bentham: Political Tactics* (Clarendon Press 1999)

Bradley CA & Goldsmith JL, *Foreign Relations Law*: Cases *and Materials* (6th edn, Wolters Kluwer 2017)

Buergenthal T, *To Respect and to Ensure: State Obligations and Permissible Derogations* (Louis Henkin ed., 1981).

Cannataci J, *Privacy & Data Protection Law* (Norwegian University Press 1986)

Coughlan S, Currie RJ, Kindred HM, Scassa T, *Law Beyond Borders. Extraterritorial Jurisdiction in an Age of Globalization* (Irwin Law Inc 2014)

Crossman G et al., *Overlooked: Surveillance and Personal Privacy in Modern Britain* (The Nuffield Foundation 2007)

Engelhardt T, *Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World* (Haymarket Books 2014)

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Science & Business 2014)

Greer S, *Human Rights File No 15: The exceptions to Articles 8 to 11 of the European Convention on Human Rights* (Council of Europe Publishing 1997).

Joseph SL and McBeth A, *Research Handbook on International Human Rights Law* (Edward Elgar Publishing 2010)

Krishnamurthy V., *A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy* (AJIL Unbound 2020)

Lubell N, *Extraterritorial Use of Force Against Non-State Actors* (Oxford University Press 2010)

Munk P, *Does State Spying Make us Safer: The Munk Debate on Mass Surveillance* (House of Anansi Press Inc 2014)

Nissenbaum H, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009)

Orwell G, *Nineteen Eighty-Four* (London: Penguin 2008)

Rengel Alexandra, *Privacy in the 21st Century* (Martinus Nijhof Publishers, Leiden, 2013)

Schneier B, *Data And Goliath: The Hidden Battles to Collect Your Data and Control Your World*, (W.W Norton & Company 2015)

Solove DJ, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press 2011)

-- -- *Understanding Privacy* (Harvard University Press 2008)

-- -- *The Privacy Advocates: Resisting the Spread of Surveillance,* (The MIT Press 2008)

Von Tigerstrom B, *Information and Privacy Law in Canada* (Irwin Law Inc, 2020)

Watt Eliza, *State Sponsored Cyber Surveillance: The right to online privacy as a customary international law rule* (Edward Elgar Publishing, 2021)

Westin AF, *Privacy and Freedom* (IG Publishing 1970)

ARTICLES

Adams M, ‘Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace’ (2014) 5 HNSJ 377

Adeyoju A, ‘Africa and the Protection of Digital Privacy: The State of Play’ (2021) (Unpublished).

Barnard M, 'Legal Reception in the AU against the Backdrop of the Monist/Dualist Dichotomy' (2015) 48 CILJSA 144

Bernal P, ‘Data gathering, surveillance and human rights: recasting the debate’ (2016) JCP 252.

Bignami F and Resta G, ‘Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance’ (2017) 67 GWU Law School Public Law and GWU Legal Studies 1

Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 NYULR 962.

Brown I, Halperin MH, Hayes B, Scott B and Vermeulen M, ‘Towards Multilateral Standards for Surveillance Reform’ (2015) 1

Browne Jane Kathryn, 'The Paradox of Peacetime Espionage in International Law: From State Practice to First Principles' (2017) 23 Austl Int'l LJ 109Buchan Russell, 'Taking Care of Business: Industrial Espionage and International Law' (2019) 26 Brown J World Aff 143

Casey T, ‘The Value of Deviance: Understanding Contextual Privacy’ (2019) 51 LUCLJ 65.

David C and Federico F, ‘Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders’ (2016) 14 IJCL 1

Demarest B. Geoffrey, 'Espionage in International Law' (1996) 24 Denv J Int'l L & Pol'y 321

Dennis MJ, ‘Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation’ (2005) 99 AJIL 119

Diggelmann O and Cleis MN, ‘How the Right to Privacy Became a Human Right’ (2014) 14 HRLR 441

Dimitrios K, ‘The International Legal Framework on Whistle-Blowers: What More Should Be Done?’ (2021) 19 SJSJ 729

Galetta A, ‘Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance’ (2014) 10 ULR 55

Georgieva, I ‘The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR’ (2015) 31 UJIEL 104.

Gerber P, Kyriakakis J and O’Byrne K, ‘General Comment 16 on State Obligations Regarding the Impact of the Business Sector on Children’s Rights: What is its Standing, Meaning and Effect?’ (2013) 14 MJIL 1

Gormley K, ‘One Hundred Years of Privacy’ (1992) 5 WLR 1335

Guzman AT and Meyer TL, ‘International Soft Law’ (2010) 2 JLA 171

Himma KE, ‘Privacy Versus Security: Why Privacy is Not an Absolute Value or Right’ (2007) 44 SDLR 857

Humble KP, ‘Human rights, international law and the right to privacy’ 1

Humphrey J, ‘No Distant Millennium: The International Law of Human Rights’ (1989) UNESCO/SHS/230).

Kang J, ‘Information Privacy in Cyberspace Transactions’ (2004) 50 SLR 1193.

Königs P, ‘Government Surveillance, Privacy, and Legitimacy’ (2022) PT 1.

Lubin A, 'We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance' (2018) 18 CJIL 502

Margulies P, ‘The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism’ (2014) 82 FLR 2137

McDermott P, ‘Secrets and Lies—Exposed and Combatted: Warrantless Surveillance Under and Around the Law, 2001–2017’ (2018) 2 Secrecy and Society 1.

Milaj J, ‘Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance’ (2015) 30 IRLCT 115-130

Milanovic M, ‘Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age’ (2015) 56 HILJ 81

Murray D, Fussey P, McGregor L & Sunkin M, ‘Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective’ (2021) 11 JNSLP 743

Navarrete Inaki & Buchan Russell, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51 Cornell Int'l LJ 897

Nyst C, ‘Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy Which Fortifies Them – An Activist's Account’ (2018) 7 State Crime Journal 8.

Oloyede R, ‘Surveillance Law in Africa: A review of six countries (Nigeria Country Report)’ Institute of Development Studies 102

Post RC, ‘Three Concepts of Privacy’ (2001) 89 GLJ 2087

Radsan A. John, ‘The Unresolved Equation of Espionage and International Law’ (2007) 28(3) MJIL 596

Reigada AT, ‘The Principle Of Proportionality And The Fundamental Right To Personal Data Protection: The Biometric Data Processing’ (2012) 17 Lex Electronica.

Rengel Alexandra, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) 2(2) GroJIL 33

Richards NM, ‘The Dangers of Surveillance’ (2013) 126 HLR 1934

Roberts T, et al., ‘Surveillance Law in Africa: a review of six countries’ (2021) Institute of Development Studies 1

Rodley N, ‘The Extraterritorial Reach and Applicability in Armed Conflict of the International Covenant on Civil and Political Rights’ (2009) 5 EHRLR 628

Satterthwaite M, ‘Rendered Meaningless: Extraordinary Rendition and the Rule of Law’ (2007) 75 GWLR 1333

Schulhofer SJ, ‘An international right to privacy? Be careful what you wish for’ (2016) 14 I.CON 238

Schwartz PM and Peifer KN, ‘Prosser‘s Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?’ (2010) 98 CLR 1925

Severson D, ‘American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change’ (2015) 56 HILJ 465

Shackelford J. Scott ‘Should Cybersecurity Be A Human Right? Exploring The 'Shared Responsibility' Of Cyber Peace’ (2019) 55(2) SJIL

Sidhu DS, ‘The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans’ (2007) 7 University of Maryland Law Journal of Race, Religion, Gender and Class 375.

Solove DJ, ‘A Taxonomy of Privacy’ (2006) 154 UPLR 477.

-- -- ‘I've Got Nothing to Hide and Other Misunderstandings of Privacy’ (2007) 44 SDLR 745 (Yale University Press 2007)

-- -- ‘Non-Application of Civil and Political Rights Treaties Extraterritorially During Times of International Armed Conflict’ (2007) 40 ILR 453

-- -- ‘The International Bill of Rights: Scope and Implementation’ (1976) 17 WMLR 527

Sourgens FG, ‘The Privacy Principle’ (2017) 42 YJIL 345

Taylor JS, ‘In Praise of Big Brother: Why We Should Learn to Stop Worrying and Love Government Surveillance’ (2005) 19 PAQ 227

Terry C.R. Patrick, '"The Riddle of the Sands" - Peacetime Espionage and Public International Law' (2020) 51 Geo J Int'l L 377

Thomson JJ, ‘The Right to Privacy’ (1975) 4 PPA 295

Van Schaack B, ‘The United States’ Position on the Extraterritorial Application of Human Rights Obligations’ (2014) 90 ILS 20

Vera R, ‘Legalization of “Mass Surveillance” by the European Court of Human Rights: What is Behind the Ruling in the Case of Big Brother Watch and Others v. the United Kingdom?’ (2018) 4 IJ 1

Watt E, ‘The right to privacy and the future of mass surveillance’ (2017) 21 IJHR 773

Weiler M, ‘The Right to Privacy in the Digital Age: The Commitment to Human Rights Online’ (2014) 57 GYBIL 651

Woods L, ‘Digital Privacy and Article 12 of the Universal Declaration of Human Rights’ (2019) 90 The Political Quarterly 422

Yilma KM, 'Digital Privacy and Virtues of Multilateral Digital Constitutionalism - Preliminary Thoughts' (2017) 25 IJLIT 115

Zalnieriute M, ‘An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance’ (2015) 0 IJLIT 1.

GOVERNMENT DOCUMENTS AND REPORTS

Canada Parliament, *Debates of the Senate* (42nd Parliamentary 1st Session Vol. 150 No. 308 2019

Committee on Legal Affairs and Human Rights, Council of Europe, *Draft Resolution on Mass Surveillance* (AS/Jur(2015) 01)

Council of the European Union, *Internal Security Strategy for the EU, Towards a European Security Model* (March 2010)

Emmerson Ben and UN Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ben Emmerson: framework principles for securing the accountability of public officials for gross or systematic human rights violations committed in the course of States-sanctioned counter-terrorism initiatives' (17 April 2013) A/HRC/22/52

European Court of Human Rights, *Factsheet – Mass surveillance* (European Court of Human Rights 2022).

European Parliament, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (Directorate-General for External Policies, Policy Department 2012).

Executive Office of the President, *Big Data and Privacy: A Technological Perspective* (Executive Office of the President of the United States 2014)

Intelligence and Security Committee of Parliament, *Uncorrected Transcript of Evidence: Given by Sir Iain Lobban, Director, Government Communication Headquarters; Mr Andrew Parker, Director General, Security Service; Sir John Sawers, Chief, Secret Intelligence Service* (Intelligence and Security Committee of Parliament 2013)

International Court of Justice (ICJ) Advisory Opinion, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory' (9 July 2004) ICJ Reports.

Martin Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin: addendum' (18 Febuary 2010) A/HRC/13/37/Add.1

Office of the Director of National Intelligence, *Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28* (Leading Intelligence Integration 2014).

Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities* (Office of the Director of National Intelligence 2017).

Official Records of the General Assembly, 36th Session

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Privacy and Civil Liberties Oversight Board 2014).

UN Commission on Human Rights, 'The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (28 September 1984) 41st Session E/CN.4/1985/4).

UN Human Rights Committee (HRC), 'CCPR General Comment No. 15: The Position of Aliens Under the Covenant' (11 April 1986) 27th Session.

UN Human Rights Committee (HRC), '*Delia Saldias de Lopez v. Uruguay'* (29 July 1981) 13th Session CCPR/C/13/D/52/1979

UN Committee on Economic, Social and Cultural Rights, 'Concluding observations on the 4th periodic report of Israel: Committee on Economic, Social and Cultural Rights' **(**12 November 2019) 66th Session E/C.12/ISR/CO/4.

UN Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment' (2 March 2021) CRC/C/GC/25.

UN General Assembly (n 51); UN General Assembly, 'Terrorism and Human Rights' (16 January 2020) 74th Session A/RES/74/147

UN General Assembly, 'Convention on the Rights of Persons with Disabilities' (24 January 2007) 61st Session A/RES/61/106.

UN General Assembly, 'Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights' (13 May 2022) 50th Session A/HRC/50/55.

UN General Assembly, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism' (23 September 2014) 69th Session A/69/397.

UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (21 February 2017) 34th Session A/HRC/34/61.

UN General Assembly, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye' (22 May 2015) 29th Session A/HRC/29/32.

UN General Assembly, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (17 April 2013) 23rd Session A/HRC/23/40.

UN General Assembly, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (28 May 2019) 41st Session A/HRC/41/35.

UN General Assembly, 'Right to Privacy in the Digital Age' (13 October 2021) 48th Session A/HRC/RES/48/4.

UN General Assembly, 'The Right to Privacy in the Digital Age' (10 February 2015) 69th Session A/RES/69/166.

UN General Assembly, ‘The right to privacy in the digital age’ (21 January 2014) 68th Session A/RES/68/167.

UN General Assembly, ‘The Right to Privacy in the Digital Age’ (21 January 2019) 73rd Session A/RES/73/179

UN General Assembly, ‘The right to privacy in the digital age’ (28 December 2020) 75th Session A/RES/75/176

UN General Assembly, ‘The right to privacy in the digital age’ (3 August 2018) 39th Session A/HRC/39/29.

UN General Assembly, ‘The right to privacy in the digital age’ (30 June 2014) 27th Session A/HRC/27/37.

UN General Assembly, ‘The right to privacy in the digital age’ (7 April 2017) 34th Session A/HRC/RES/34/7.

UN General Assembly, ‘The right to privacy in the digital age’ (7 October 2019) 42nd Session A/HRC/RES/42/15.

UN Human Rights Committee (HRC), ‘CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation’ (8 April 1998) 32nd Session.

UN Human Rights Committee (HRC), ‘CCPR General Comment No. 5: Article 4 (Derogations)’ (31 July 1981) 13th Session.

UN Human Rights Committee, ‘General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant’ (26 May 2016) 80th Session CCPR/C/21/Rev.1/Add. 13.

UN Human Rights Committee, ‘Toonen v Australia, Communication No 488/1992, U.N. Doc CCPR/C/50/D/488/1992’ (1994) 50th Session CCPR/C/WG/44/D/488/1992;CCPR/C/46/D/488/1992.

UN Human Rights Committee, ' Concluding Observations on the Third Periodic Report of Tajikistan’ (22 August 2019) CCPR/C/TJK/CO/3.

UN Human Rights Committee, ‘Information in Pursuance of Paragraph 27 of the Concluding Observations of the Human Rights Committee: Netherlands’ (29 April 2003) CCPR/CO/72/NET/Add.1 Paragraph 7.

US Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Department of Justice 2006).

ELECTRONIC SOURCES

A Project of the Electronic Frontier Foundation and a coalition of NGOs, 'Necessary and Proportionate on the Application of Human Rights to Communications Surveillance' (*Electronic Frontier Foundation,* May 2014) <https://necessaryandproportionate.org/principles/#top>

Above Average Jane, 'Interview with Patrick Murphy' (*Above Average Jane)* <http://aboveavgjane.blogspot.com/2005/12/interviewwith-patrick-murphy.html>

Alfred NG, 'Why your privacy could be threatened by a bill to protect children' (*CNET*, 2 July 2020) <https://www.cnet.com/news/politics/why-your-privacy-could-be-threatened-by-a-bill-to-protect-children/>

Andere A, 'Kenya's sneak attack on privacy: changes to the law allow government access to phone and computer data' (*AccessNow,* 27 January 2021) <https://www.accessnow.org/kenya-right-to-privacy/>

Association for Progressive Communications, 'The protection of sources and whistleblowers' (*OHCHR Official Website)* <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Protection/AssociationProgressiveCommunications.pdf>

Australian Border Force, 'Statement of Principles on Access to Evidence and Encryption' (*Australian Border Force*) <https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption>

Ball J and Hopkins N, 'GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief'(*The Guardian,* 20 December 2013) <https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner>

Ball J, 'NSA collects millions of text messages daily in 'untargeted' global sweep' (*The Guardian,* 16 January 2014) <https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>

Ball J, Borger J and Greenwald G, 'Revealed: how US and UK spy agencies defeat internet privacy and security' (*The Guardian,* 6 February 2013) <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

Bamford J, 'The Most Wanted Man in the World' (*Wired,* 13 August 2014) <https://www.wired.com/2014/08/edward-snowden/>

Butz N, ‘Congress Must Put Human Rights at the Center of Surveillance Reform’ (*Amnesty International*, 7 May 2014) <https://www.amnestyusa.org/press-releases/congress-must-put-human-rights-at-the-center-of-surveillance-reform/> accessed 17 August 2022.

Campbell IA, ‘Clearview AI hit with sweeping legal complaints over controversial face scraping in Europe’ (*The Verge,* 27 May 2021) <https://www.theverge.com/2021/5/27/22455446/clearview-ai-legal-privacy-complaint-privacy-international-facial-recognition-eu>

Chappell B, ‘Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail’ (*NPR,* 2 June 2015) <https://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senateis-poised-to-vote-on-house-approved-usa-freedom-act>

Childress S, ‘How the NSA Spying Programs Have Changed Since Snowden’ (*Frontline,* 9 February 2015) <https://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/>

Chowdhury M, Hayes M and Vera A, ‘Roe v. Wade news’ (*CNN,* 26 June 2022) <https://www.cnn.com/politics/live-news/abortion-roe-wade-supreme-court-06-26-22/index.html>

Cole D, ‘We Are All Foreigners: NSA Spying and the Rights of Others’ (*Just Security*, 29 October 2013) <https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/>

Coustick-Deal R, ‘Responding To “Nothing To Hide, Nothing To Fear”’ (*Open Rights Group (ORG),* 4 December 2015) <https://www.openrightsgroup.org/blog/responding-to-nothing-to-hide-nothing-to-fear/>

Davies S, ‘Private virtue: At what point does your business become the legitimate concern of others?’ (*The Guardian UK,* 7 September 2002*)* <https://www.theguardian.com/uk/2002/sep/07/privacy2>

Diffie W, ‘The Encryption Wars Are Back but in Disguise’ (*Scientific American,* 30 June 2020) <https://www.scientificamerican.com/article/the-encryption-wars-are-back-but-in-disguise/>

Dishfire, ‘Overview’ (*Dishfire,* 11 November 2018*)* <https://ldapwiki.com/wiki/DISHFIRE>

Eddington PG, ‘The Snowden Effect, Six Years On’ *(Just Security,* 6 June 2019) *<https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/>*

Electrospaces, ‘A look at the latest French laws on intelligence collection’ (*Electrospace.net*, 26 February 2016) <https://www.electrospaces.net/2016/02/a-look-at-latest-french-laws-on.html>

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse' (*European Union Official Website*, 11 May 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472>

Express Web Desk, 'Right to access internet is part of RTE and right to privacy: Kerala High Court' (*Indian Express*, 19 September 2019) <https://indianexpress.com/article/india/right-to-access-internet-part-of-rte-right-to-privacy-kerala-high-court-6011227/>

Finamore E, 'Are UN resolutions legally enforceable?' (*All About Law*, 31 October 2018) <https://www.allaboutlaw.co.uk/commercial-awareness/commercial-insights/are-un-resolutions-legally-enforceable->

Gallagher S, 'T he Snowden Legacy, part one: What's changed, really?' (*Ars Technica*, 21 November 2018) <https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/>

Gellman B, Julie Tate and Ashkan Soltani, 'In NSA-intercepted data, those not targeted far outnumber the foreigners who are' (*The Washington Post*, 5 July 2014) <https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html>

Gerstein J, 'NSA: PRISM stopped NYSE attack' (*Politico*, 18 June 2013) <https://www.politico.com/story/2013/06/nsa-leak-keith-alexander-092971>

Goujard C and Westendarp L, 'Germany forces EU into damage control over encryption fears' (*Politico*, 10 June 2022) <https://www.politico.eu/article/germany-eu-damage-control-encryption-abuse-online/>

Granick JS, 'Mass Spying Isn't Just Intrusive---It's Ineffective' (*Wired*, 2 March 2017) <https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/>

Green M (@matthew_d_green), 'This document is the most terrifying thing I've ever seen…' Twitter, 10 May 2022 <https://twitter.com/matthew_d_green/status/1524094474187644933

Greenwald G and MacAskill E, 'NSA Prism program taps in to user data of Apple, Google and others' (*The Guardian*, 7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

Harrington J and McCabe R, 'The Case for Cooperation: The Future of the U.S.-UK Intelligence Alliance' (*Center for Strategic and International Studies*, 15 March 2022' <https://www.csis.org/analysis/case-cooperation-future-us-uk-intelligence-alliance>

Hernández Pablo Juan, 'The legality of espionage in international law' (T*he Treaty Examiner: Online Journal of International Law* April 2020) https://treatyexaminer.com/espionage-legality/

Human Rights Watch, 'Human Rights Council: Protect the right to privacy' (*Human Rights Watch,* 8 March 2017) <https://www.hrw.org/news/2017/03/08/human-rights-council-protect-right-privacy>

-- -- 'US: End Bulk Data Collection Program' (*Human Rights Watch,* 5 March 2020) <https://www.hrw.org/news/2020/03/05/us-end-bulk-data-collection-program>

-- -- 'US: Modest Step by Congress on NSA Reform' (*Human Rights Watch,* 8 May 2014) <https://www.hrw.org/news/2014/05/08/us-modest-step-congress-nsa-reform>

Hurst D, 'ASIO Spy Chief Defends Surveillance Network and Argues for Broader Powers' (*The Guardian,* 21 July 2014) <https://www.theguardian.com/world/2014/jul/21/asiospy-chief-defends-surveillence-network>

International Commission of Jurists, 'European Court of Human Rights issues landmark ruling on mass surveillance' (*International Commission of Jurists,* 26 May 2021) <https://www.icj.org/european-court-of-human-rights-issues-landmark-ruling-on-mass-surveillance/>

International Justice Resource Center, 'UN Human Rights Treaty Bodies' (*International Justice Resource Center*) <https://ijrcenter.org/un-treaty bodies/#:~:text=The%20committee%20issues%20a%20decision,agreed%20to%20be%20legally%20bound>

Isikoff M, 'NSA program stopped no terror attacks, says White House panel member' (*NBC News,* 20 December 2013) <https://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588>

Judge Herbert B.D Jr. (Ret.), 'Your Cell Phone Is a Spy!' (*American Bar Association,* 29 July 2020) <https://www.americanbar.org/groups/judicial/publications/judges_journal/2020/summer/your-cell-phone-a-spy/#3>

Kalyanpur N and Newman A, 'Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened' (*The Washington Post,* 25 May 2018) <https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/>

Kampmark B, ‘Limits on surveillance: A global right to privacy’ (*Index on Censorship*, 29 January 2014) <https://www.indexoncensorship.org/2014/01/international-right-privacy/>

Khazan O, ‘The Creepy, Long-Standing Practice of Undersea Cable Tapping: The newest NSA leaks reveal that governments are probing "the Internet's backbone." How does that work?’ (*The Atlantic*, 16 July 2013) <https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>

Kim V, ‘Who’s watching? How governments used the pandemic to normalize surveillance’ (*Los Angeles Times*, 9 December 2021) <https://www.latimes.com/world-nation/story/2021-12-09/the-pandemic-brought-heightened-surveillance-to-save-lives-is-it-here-to-stay>

Kingsmith A, ‘Data Privacy Day 2014: Think you have nothing to hide? Think again’ (*Canadian Journalists for Free Expression (CJFE)*, 27 January 2014)<https://www.cjfe.org/resources/features/data-privacy-day-2014>

Kleeman S, ‘In One Quote, Snowden Just Destroyed the Biggest Myth About Privacy’ (*Mic*, 29 May 2015) <https://www.mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for>

Kravets D, ‘Judge Rules NSA Bulk Telephone Metadata Spying Is Lawful’ (*Wired*, 27 December 2013) <https://www.wired.com/2013/12/judge-upholds-nsa-spying/>

Lake J, ‘How your mobile phone tracks you (even when switched off)’ (*Comparitech*, 25 November 2020) <https://www.comparitech.com/blog/vpn-privacy/stop-mobile-phone-tracking/>

Lambert L, ‘Polling calls to U.S. Muslims raise surveillance fears’ (*Reuters*, 24 November 2016) <https://www.reuters.com/article/us-usa-muslims-idUSKBN13I2PK>

Lankow C and Johansson T, ‘Psychology at Work: Toward the Deepest Understanding of Strengths (It Depends)’ (*Buzz Sprout*, 3 October 2019) <https://www.buzzsprout.com/342416/1785202>

Laperruque J, ‘It’s Time to End the NSA’s Metadata Collection Program’ (*Wired*, 3 April 2019) <https://www.wired.com/story/wired-opinion-nsa-metadata-collection-program/>

-- -- ‘The History and Future of Mass Metadata Surveillance’ (*Pogo*, 11 June 2019) <https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/>

Lawyers’ Rights Watch, ‘Canada: Civil Society Statement Regarding Bill C-59, An Act Respecting National Security Matters | Joint Letter’ (Lawyers’ Rights Watch, 27 March

2018) < Canada: Civil Society Statement Regarding Bill C-59, An Act Respecting National Security Matters | Joint Letter — Lawyers' Rights Watch Canada (lrwc.org)>

Lee TB, 'Why "we only spy on foreigners" doesn't work any more for the NSA' (*The Washington Post,* 7 July 2013. <https://www.washingtonpost.com/news/wonk/wp/2013/07/07/european-outrage-about-the-nsa-could-force-us-to-rethink-our-surveillance-laws/>

Lubin A, 'A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens' (2017) 42 (2) YJILO < A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens by Asaf Lubin :: SSRN>

-- -- 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights' (*Just Security,* 2 August 2018) <https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/>

Lucas R, 'Scathing Report Puts Secret FISA Court Into The Spotlight. Will Congress Act?' (*NPR*, 22 December 2019) <https://www.npr.org/2019/12/22/790281142/scathing-report-puts-secret-fisa-court-into-the-spotlight-will-congress-act>

Macaskill E and Dance G, 'NSA Files: Decoded' (*The Guardian*, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

MacAskill E, Borger J, Hopkins N, Davies N and Ball J, 'GCHQ taps fibre-optic cables for secret access to world's communications' (*The Guardian*, 21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

Manyame A, 'Data protection in the age of technology-based disease surveillance' (*African Internet Rights)* <https://africaninternetrights.org/sites/default/files/Amanda_Manyame-1_1.pdf>

Marczak B, Scott-Railton J, Berdan K, Razzak BA and Deibert R, 'Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus' (*The Citizen Lab,* 15 July 2021) <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>

Marczak B, Scott-Railton J, Rao SP, Anstis S and Deibert R, 'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles' (*The Citizen Lab,* 1 December 2020) < https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>

Marshall R and Skinner Q, 'Liberty, Liberalism and Surveillance: a historic overview' *(OpenDemocracy*, 26 July 2013) < https://www.opendemocracy.net/en/opendemocracyuk/liberty-liberalism-and-surveillance-historic-overview/>

Masnick M, 'EU Proposes It's Own Version Of EARN IT: Effectively Mandates Full Surveillance Of All Messaging & No Encryption' (*Tech Dirt,* 12 May 2022) <https://www.techdirt.com/2022/05/12/eu-proposes-its-own-version-of-earn-it-effectively-mandates-full-surveillance-of-all-messaging-no-encryption/>

McFarland S.J., 'Why We Care about Privacy' (Markkula Center for Applied Ethics, 1 June 2012) <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/>

Milmo D, 'End-to-end encryption protects children, says UK information watchdog' (*The Guardian,* 21 January 2022) <https://www.theguardian.com/technology/2022/jan/21/end-to-end-encryption-protects-children-says-uk-information-watchdog>

Mirkinson J, 'Daniel Ellsberg Calls Edward Snowden A 'Hero,' Says NSA Leak Was Most Important In American History' (*HuffPost,* 10 June 2013) <https://huffingtonpost.com/2013/06/10/edward-snowden-daniel-ellsberg-whistleblower-history_n_3413545.html>

Montagne R, 'Bush Defends Surveillance Without Warrant' (*NPR,* 19 December 2005) <https://www.npr.org/templates/story/story.php?storyId=5061250>

Mullin J, 'The EU Commission's New Proposal Would Undermine Encryption and Scan Our Messages' (*Electronic Frontier Foundation,* 11 May 2022) <https://www.eff.org/deeplinks/2022/05/eu-commissions-new-proposal-would-undermine-encryption-and-scan-our-messages>

-- -- 'The U.K. Paid $724,000 For A Creepy Campaign To Convince People That Encryption is Bad. It Won't Work' (*Electronic Frontier Foundation,* 21 January 2022) <https://www.eff.org/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work>

Nadarajah H 'Fewer Treaties, More Soft Law: What Does it Mean for the Arctic and Climate Change?' (*Artic Portal)* < https://issuu.com/arcticportal/docs/ay2020/s/11293424>

Nakashima E and Gellman B, 'Court gave NSA broad leeway in surveillance, documents show' (*The Washington Post,* 30 June 2014) <https://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-

in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html?hpid=z>

Nakashima E and Marimow AE, 'Judge: NSA's collecting of phone records is probably unconstitutional' (*The Washington Post,* 16 December 2013) <https://www.washingtonpost.com/national/judge-nsas-collecting-of-phone-records-is-likely-unconstitutional/2013/12/16/6e098eda-6688-11e3-a0b9-249bbb34602c_story.html>

Nardi DJ, 'Religious Freedom in China's High-Tech Surveillance State' (*United States Commission on International Religious Freedom Official Website,* September 2019) <https://www.uscirf.gov/countries/china/religious-freedom-chinas-high-tech-surveillance-state>

Naughton J, 'NSA surveillance: don't underestimate the extraordinary power of metadata' (*The Guardian,* 21 June 2013) <https://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama>

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

-- -- 'International privacy guardians urge legislators to reaffirm commitment to privacy as a right and value in itself' (*Office of the Privacy Commissioner of Canada Official Website,* 28 October 2019) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_191028/>

Oli S, 'Canada's public health agency admits it tracked 33 million mobile devices during lockdown' (*National Post,* 24 December 2021) <https://nationalpost.com/news/canada/canadas-public-health-agency-admits-it-tracked-33-million-mobile-devices-during-lockdown>

Osisanya S, 'National Security versus Global Security' (*UN)* <https://www.un.org/en/chronicle/article/national-security-versus-global-security)>

Paul E, 'Kenyan government takes another shot at infringing privacy and digital rights' (*Techpoint Africa,* 17 December 2020) <https://techpoint.africa/2020/12/17/kenya-private-data/>

Pew Research Center, 'Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image' (*Pew Research Center,* 14 July 2014) <https://www.pewresearch.org/global/2014/07/14/global-opposition-to-u-s-surveillance-and-drones-but-limited-harm-to-americas-image/>

Pillai Arvind and Kohli Raghav, 'A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice' (*Oxford University Comparative Law Forum*) https://ouclf.law.ox.ac.uk/a-case-for-a-customary-right-to-privacy-of-an-individual-a-comparative-study-on-indian-and-other-state-practice/#3-B

Poitras VL, Rosenbach M and Stark H, 'How America Spies on Europe and the UN' (*Spiegel International*, 26 August 2013) <https://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html>

Poitras VL, Rosenbach M, Schmid F, Stark H and Stock J, 'How the NSA Targets Germany and Europe' (*Spiegel International*, 01 July 2013) <https://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html>

Posner RA, 'Our Domestic Intelligence Crisis' (*The Washington Post*, 21 December 2005) <https://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html>

Power J, 'Australia's early plans for 'dangerous' encryption law revealed' (*Aljazeera*, 5 April 2022) <https://www.aljazeera.com/news/2022/4/5/australias-dangerous-encryption-law-in-works-in-2015-document#:~:text=Australia%20in%202018%20passed%20world,a%20target's%20computer%20or%20phone>

Press Release, 'US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies' (*The White House*, 8 December 2021) <https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/>

Privacy International, 'Apps and COVID 19' (*Privacy International)* <https://privacyinternational.org/examples/apps-and-covid-19>

Privacy International, 'Government Hacking' (*Privacy International)* <https://privacyinternational.org/learn/government-hacking>

Privacy International, 'Most contact tracing apps fail at privacy and security' (*Privacy International*, 25 June 2020*)* <https://privacyinternational.org/examples/4229/most-contact-tracing-apps-fail-privacy-and-security>

Privacy International, 'What Is Privacy' (*Privacy International*, 23 October 2017) <https://privacyinternational.org/explainer/56/what-privacy>

Private AI Series, ‘Structured Transparency: Ensuring Input and Output Privacy’ (*OpenMined,* 14 March 2021) <https://blog.openmined.org/structured-transparency-input-output-privacy/>

Prochko Veronika, ‘The International Legal View of Espionage’ (*E-International Relations* 2018) https://www.e-ir.info/2018/03/30/the-international-legal-view-of-espionage/

Razzano G, ‘Privacy and the pandemic: An African response’ surveillance’ (*African Internet Rights)* <https://africaninternetrights.org/sites/default/files/Gabriella_Razzano_1.pdf>

Reuters Staff, ‘UK security services have thwarted five plots since March Westminster attack: source’ (*Reuters,* 25 May 2017) <https://www.reuters.com/article/us-britain-security-manchester-plots-idUSKBN18L1H0>

Risen J and Poitras L, ‘N.S.A. Collecting Millions of Faces From Web Images’ (*The New York Times,* 31 May 2014) <https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html>

Sanger DE and Schmitt E, ‘Snowden Used Low-Cost Tool to Best N.S.A’ (*The New York Times,* 8 February 2014) <https://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html>

Satter R, ‘U.S. Court: Mass surveillance program exposed by Snowden was illegal’ (*Reuters,* 2 Sepetember 2020) <https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK>

Schrepferman W, ‘Supervising Surveillance: Applying International Law to the Global Surveillance State’ (*Harvard International Review,* 11 November 2020) <https://hir.harvard.edu/global-surveillance-state/>

Scott T, ‘Why Electronic Voting Is Still A Bad Idea’ (2020) [https://www.youtube.com/watch?v=LkH2r-sNjQs

Shackford S, ‘The U.K. Government's Latest Encryption Fearmongering Relies on Child Sex-Trafficking Panics’ (*Reason,* 18 January 2022) <https://reason.com/2022/01/18/the-u-k-governments-latest-encryption-fearmongering-relies-on-child-sex-trafficking-panics/>

Short B, ‘How the federal government failed to protect our mobility data’ (*Open Media,* 2 May 2022) <https://openmedia.org/article/item/how-the-federal-government-failed-to-protect-our-mobility-data

Shubber K, ‘A simple guide to GCHQ's internet surveillance programme Tempora’ (*Wired,* 24 June 2013) <https://www.wired.co.uk/article/gchq-tempora-101>

Siatitsa I, ‘Digital Rights are Human Rights’ (*Digital Freedom Fund)* <https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/

Stepanovich A et al, ‘A Human Rights Response to Government Hacking’ (*Access Now* September 2016) <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>

Taylor M and Hopkins N, ‘World's leading authors: state surveillance of personal data is theft’ (*The Guardian,* 10 December 2013) <https://www.theguardian.com/world/2013/dec/10/surveillance-theft-worlds-leading-authors>

The Citizen Lab, ‘Pegasus’ (*The Citizen Lab,* 2022) <https://citizenlab.ca/tag/pegasus/>

Thompson SA and Warzel C, ‘Twelve Million Phones, One Dataset, Zero Privacy’ (*The New York Times,* 19 December 2019) <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>

Toomey P, ‘The NSA Continues to Violate Americans' Internet Privacy Rights’ (*ACLU,* 22 August 2018) <https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy>

Tosinni JV, ‘The Five Eyes – The Intelligence Alliance of the Anglosphere’ (*UK Defence Journal*, 14 April 2020) <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>

Treguer F, Overview of France’s Intelligence Legal Framework’ (2021) HAL Open Science <https://halshs.archives-ouvertes.fr/halshs-01399548/document>

Troianovski A, ‘Edward Snowden, in Russia Since 2013, Is Granted Permanent Residency’ (*The New York Times,* 2 November 2020) <https://www.nytimes.com/2020/10/23/world/europe/russia-putin-snowden-resident.html>

Tuccille JD, ‘Invasion Of Privacy: Earn It Act Abuses Privacy in the Guise of Protecting Kids’ (*Reason,* 16 February 2022) <https://reason.com/2022/02/16/earn-it-bill-abuses-privacy-in-the-guise-of-protecting-kids>

UN Human Rights Office of the High Commissioner, ‘A/HRC/27/37: The right to privacy in the digital age (focus on surveillance) - Report of the Office of the UN High Commissioner for Human Rights’ (*OHCHR Official Website,* 30 June 2014) <OHC OHCHR | A/HRC/27/37: The right to privacy in the digital age (focus on surveillance) - Report of the Office of the UN High Commissioner for Human Rights>

-- --‘Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe - Hearing on the implications of the Pegasus spyware’ (*OHCHR Official Website*, 14 September 2021) <https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe>

-- -- ‘New record: Translations of Universal Declaration of Human Rights pass 500’ (*OHCHR Official Website*, 2 November 2016) < https://www.ohchr.org/en/human-rights/universal-declaration/new-record-translations-universal-declaration-human-rights-pass-500>

-- -- ‘UDHR Translations’ (*OHCHR Official Website*) <https://www.ohchr.org/en/search?f[0]=event_type_taxonomy_term_name%3AUniversal%20Declaration%20of%20Human%20Rights>

-- -- ‘What the treaty bodies do’ (*OHCHR Official Website*) <https://www.ohchr.org/en/treaty-bodies/what-treaty-bodies-do>

UN, ‘Internet shutdowns now ‘entrenched’ in certain regions, rights council hears’ (*UN Official Website*, 1 July 2021) <https://news.un.org/en/story/2021/07/1095142>

Volz D and Warren PS, ‘NSA Recommends Dropping Phone-Surveillance Program’ (*The Wall Street Journal*, 24 April 2019) <https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247>

Walpin, G., ‘We need NSA surveillance’ (*National Review*, 16 August 2013). <http://www.nationalreview.com/article/355959/we-need-nsa-surveillancegerald-walpin>

Weinberg J, ‘The Real Costs of Cheap Surveillance’ (*The Conversation,* 18 July 2017) < https://www.scientificamerican.com/article/the-real-costs-of-cheap-surveillance/>

Whittacker Z, ‘PRISM: Here's how the NSA wiretapped the Internet’ (*ZDNET,* 7 June 2013*)* < https://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/>

WikiLeaks, ‘Vault 7: CIA Hacking Tools Revealed’ (2017) <https://wikileaks.org/ciav7p1/>

Wittes B, ‘A Global Human Right to Privacy?’ (*Lawfare*, 11 November 2013) <https://www.lawfareblog.com/global-human-right-privacy>

Writers Against Mass Surveillance, ‘A Stand for Democracy in the Digital Age’ (*Change.org*) <https://www.change.org/p/a-stand-for-democracy-in-the-digital-age-3>

Wyden R: United States Senator for Oregon, ‘Wyden and Heinrich: Newly Declassified Documents Reveal Previously Secret CIA Bulk Collection, Problems With CIA Handling of Americans’ Information’ (2022) <https://www.wyden.senate.gov/news/press-releases/wyden-and-heinrich-newly-declassified-documents-reveal-previously-secret-cia-bulk-collection-problems-with-cia-handling-of-americans-information>

Zetter K, ‘A Government Error Just Revealed Snowden Was the Target in the Lavabit Case’ (*Wired*, 17 March 2016) <https://www.wired.com/2016/03/government-error-just-revealed-snowden-target-lavabit-case/>

-- -- ‘Encrypted Email Service Once Used by Edward Snowden Relaunches’ (*The Intercept*, January 20 2017) <https://theintercept.com/2017/01/20/encrypted-email-service-once-used-by-edward-snowden-to-relaunch/>