PSWG3: Privacy and data protection as fundamental rights: A narrative

Prepared for the GPA WG3 on Privacy and Human Rights

Table of Contents

Privacy and data protection as fundamental rights: A narrative

About this document

This document is a product of the Global Privacy Assembly ("GPA") Policy Strategy Workgroup Three ("PSWG3").

The PSWG3's mandate is to develop a narrative highlighting the relationship between privacy and data protection and other rights and freedoms, building on the *International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other Fundamental Rights*, adopted at the 2019 GPA Conference.[1]

To achieve this goal, the PSWG3 developed a plan based on four phases:

1. Research and information gathering (fact-finding),
2. Developing a draft narrative,
3. Receiving external feedback on the narrative draft, and
4. Finalization of narrative for consideration and adoption in 2021.

We would like to thank our data protection colleagues from every region around the globe who have provided vital facts, clarifying research and thoughtful reflection upon the results presented below. This effort would not have been possible without their participation, contributions, commentary and active involvement. These included:

- The National Directorate for Personal Data Protection, Argentina
- National Data Protection Authority, Belgium
- Office of the Privacy Commissioner of Canada
- Catalan Data Protection Authority, Catalonia
- Council of Europe
- Chilean Transparency Council
- Dubai International Financial Centre
- European Data Protection Supervisor
- European Union Fundamental Rights Agency
- State Inspector's Service of Georgia
- Federal Commissioner for Data Protection and Freedom of Information, Germany
- National Institute for Transparency, Access to Information and Personal Data Protection, Mexico
- National Center for Privacy and Data Protection, Moldova
- Office of the Information and Privacy Commissioner, Newfoundland
- Personal Data Protection Office, Poland
- Data Protection Authority, Republic of San Marino
- Personal Data Commission, Senegal
- Information Regulator, South Africa
- Federal Data Protection and Information Commissioner, Switzerland
- Instance nationale de protection des données personnelles, Tunisia
- Information Commissioner's Office, United Kingdom

- Federal Trade Commission, USA
- Office of the Victorian Information Office, Victoria

We would also like to acknowledge the vital contribution of external peer-reviewers and other regulators who commented upon the document, including:

- Canadian Human Right Commission
- Chilean Transparency Council
- Council of Europe
- European Data Protection Supervisor
- European Union Agency for Fundamental Rights
- State Inspector's Office of Georgia
- Office of the Information and Privacy Commissioner, Newfoundland
- Data Protection Authority, Republic of San Marino
- Office of the Victorian Information Office, Victoria
- Members of the Global Privacy Assembly Reference Panel**.**

Finally, we would like to thank and acknowledge the invaluable research, analysis and writing effort of Professors Orla Lynskey and Judith Rauffoer, whose thinking and synthesis formed the backbone of this report.

1. Executive Summary

A. Purpose of the narrative

Over the past decade several major international data protection instruments have been modernised, including the Organization for Economic Co-operation and Development's (OECD) Privacy Guidelines, the Council of Europe's Convention 108 and the European Union's (EU) data protection framework, while data protection laws have been proliferating at the national level.[2]

This narrative takes stock of these developments and reinforces a case for adopting a fundamental rights approach to data protection and privacy globally. It addresses the query "what do we protect when we protect privacy and ensure data protection?" and articulates the connection between these rights and other rights and interests, such as human dignity, liberty, and freedom of expression. Finally, it identifies potential impediments to the development of these rights and suggests how they may be overcome, paving the way for the reinforcement of these rights in national and international legal forms.

B. Links to the GPA Working Group initiative

The core idea at the forefront of our work is that privacy and data protection are universal human rights – and are themselves fundamental to our democracy as well as to the exercise of other rights we value collectively in our societies. In many contexts it is our rights to privacy and data protection that allow for meaningful exertion of other fundamental rights, such as; freedom of political belief, of movement and association, exercise of democratic rights, peaceful dissent, or freedom of conscience and expression.[3]

For example, in the past five years the vulnerabilities of election procedures to intrusion and manipulation has become increasingly evident, demonstrating how the problems of foreign interference, online safeguards, and the rights to privacy and data protection are deeply intertwined. Government, legislators, regulators, businesses and civil society all need to engage with each other to address these complex challenges.[4]

Irrespective of motivation, complex privacy risks can no longer be minimized or ignored. Some argue that institutions should do more in the name of fundamental legal obligations, others to ensure protection of individual rights.[5] Other commentators highlight organizational obligations to improve accountability and governance, or to innovate with data more transparently.[6] Each of these views have their critics and advocates. However, while the ends and motivations of varied stakeholders remain fluid, this report demonstrates concrete action to safeguard privacy and data protection is now a non-negotiable obligation in many jurisdictions.

The goal of our international effort is to take stock of these lessons and experiences from around the world, so we can better understand how the meaningful protection of privacy is integral to other fundamental rights that we need to respect and foster in open and free societies.[7]

C. Why this matters

Over the past decade, technological advances, emerging digital economies, globalized data networks, data-driven governance, novel business models and far-reaching digital government initiatives have made the protection of civil liberties a complex and global challenge.

At the centre of these shifts is mass data collection and sharing, automated-decision making, and profiling, by both public organizations and private commercial entities. These digital and data-driven technologies and processes are not only raising concerns for privacy as a human right, but also have implications for human dignity, equality, non-discrimination, and the right to reputation, amongst others.[8] It is not an exaggeration to say that the advent of new digital platforms, practices and technologies have had and will continue to have profound, historic effects on individuals and society.[9] These will be akin to those witnessed in the industrial revolution, or in the early modern period with the proliferation of the printing press, which led to the Reformation, the Renaissance, the rise of the nation-state and new political ideas, along with the wars and conflicts associated with this history.

Digital tools have equally transformative potential.[10] While we are at the onset of this transformation as a society, we are already seeing the first generation of children born into a world where their digital life is a daily reality. The question remains how will digitization affect the individual and society and how can we ensure that our laws protect our values and rights as digital transformation accelerates?[11]

2. Introduction: Why this matters now

Given the multiplicity of data protection laws worldwide, and the existing commitment to privacy and data protection as fundamental rights in many countries, one might legitimately query: why does this matter now? This narrative sets out the case for the recognition of a right to privacy and a right to the protection of personal data in states that do not yet recognise such rights and, for those where this recognition already exists, it calls for a renewed and explicitly stated commitment to these rights and their underlying principles. Such recognition and reaffirmation is urgently required to address important technological and societal changes.

Our daily interactions are increasingly digitized. Technology continues to be applied in ways that advance and promote our fundamental rights in some instances but challenge them in others.[12] A good example of the latter is affective computing, or emotion detection technology. 'Emotional AI' uses machine learning methods to, arguably, infer the mental states of its subjects and is being used for a broad array of purposes ranging from road safety surveillance of drivers to the delivery of targeted advertising.[13] A company such as EyeQ, for instance, offers an emotion recognition technology that claims to provide retailers with real-time data on customer emotion and demographics (such as gender and age) 'which can be used to improve service and raise the retention rate'.[14]

Such technologies can exacerbate the asymmetries of power and information between those who gather and use such data and those whose emotions are gauged in this way. In particular, there is clear potential for this technology to be used to exploit our emotional fragilities and cognitive weaknesses. While evidence of such exploitation can be difficult to gather, there are indications that it is already occurring. An Australian media outlet reported in 2017 that Facebook pitched to advertisers its capability to identify when teenagers felt in 'need of a confidence boost', 'insecure' or 'worthless'.[15]

In considering how to regulate such technology, the starting premise of market-based legislation, such as consumer protection laws, that are limited to agreements between a "consumer" and a "business" and assume individuals act as rational agents in their decision-making will necessarily be deficient.[16] This is where data protection and the right to privacy have a role to play.[17] Technology itself has therefore changed in the way it seeks to capture and represent our actions and to influence our behaviour. However, we are also seeing increasing pressure to "capitalise" on these technological advances, irrespective of the broader societal consequences of doing so.

In the private sector, the "move fast and break things" ethos epitomised by Silicon Valley start-ups has cultivated the perception that any form of regulation, in particular fundamental rights regulation, acts as an impediment to innovation and thwarts efficiency.[18] By making such a straw man of data protection and privacy regulation, it becomes easier to propagate the myth that by violating fundamental rights such as the rights to privacy or data protection and accepting a new reality in which the untapped potential of personal data is unleashed, we will all be beneficiaries. Yet, as this narrative argues, it is only by embracing core data protection and privacy principles that technologies will constitute real societal progress, be trusted by

individuals and consumers and our existing social, democratic and ethical values will continue to be respected.

Granted, there are schools of thought that disagree with this formulation. For reasons of accelerating innovation or limiting legal liability, for example, many commentators stress corporate social responsibility and governance models (over fundamental human rights obligations) in addressing privacy concerns.[19] The technology industry has voiced similar arguments for decades, in tandem with discouragement of restrictive regulation. At another pole of the debate, there are respected researchers who focus on power, privilege and surveillance as social control, not individualized privacy rights. Both groups advance legitimate arguments.[20] However, while profit and power clearly are legitimate factors, regulators view many of the terms (e.g. demonstrable accountability) and concepts (e.g. independent oversight) from these voices as complementary, not contradictory.

Counterpoint: privacy, technology and rights protections

Not all examples of digitization and advancing technologies have eroded privacy, and it is important to note that some recent advances in privacy-enhancing technologies have been important contributors to the protection of human rights. Technologies such as multi-factor identity verification (as a protection against device searches), anonymization tools (as a counter-measure to internet content blocking), and end-to-end encryption (as a stopgap against government surveillance) all present us with concrete examples where digital technologies now offer very real and tangible protections against privacy risks. One such example of end-to-end encryption technologies are Virtual Private Networks. Virtual Private Networks, or 'VPNs', is a term used to define technologies that allow users to safely and privately access the internet. VPNs can encrypt a user's communications device and reroutes their network data (typically an IP address) though a secure channel to the VPN service provider's foreign servers, thereby masking the user's IP address. In this way, VPNs can allow users to circumvent internet censorships and social media disruptions caused by domestic governments. This privacy preserving technology not only enables users to access blocked websites, it also allows them to safely coordinate social movements and political protests. For example, in 2019 when the Egyptian government blocked access to social media sites like Facebook and BBC News in an attempt to discourage political protests, Egyptian individuals were able to get around the social media disruptions by using VPNs and could continue to coordinate protests. VPNs are also commonly used in other parts of the world, particularly in countries where governments have placed internet restrictions. The use and popularity of VPNs highlights the relationship between privacy, data protection and human rights, as VPNs encourage and enable people to exercise their right to protest.

Sources: *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (May 2019); L. Gill, T. Israel, C. Parsons, Shining a Light on the Encryption Debate (2018); "Ensuring Human Rights for Digital Citizens" (29-37) from Global Commission on Internet Governance report (June 2016); Katherine Barnett, "The impact of social media on modern protest movements and democracy," The Sociable, September 20, 2019.* https://sociable.co/social-media/impact-social-media-modern-protest-movements-democracy/

Trust and transparency remains a recurring theme across all these sub-literatures, just as the question of how we prioritize and regulate questions of technology. Governments and public sector agencies have shown a clear and persistent desire to address societal problems with data-driven technological solutions.[21] The advantage of resorting to technology to engineer solutions to societal challenges is its perceived efficiency (in terms of cost and performance) as well as the capacity for automated solutions to be audited and to be consistent.[22] We might add to this the reluctance of states to lag behind in their data processing capacity, as this would hinder their competitive edge in the geopolitical competition for AI in the future.[23]

Such technological fixes have been the first port of call for many public sector bodies during the Covid-19 pandemic. A prime example was the deployment of an algorithm to calculate final school examination (A-level) results for students in the UK. Such was the outcry against its deployment that the British Prime Minister labelled it a "mutant algorithm" and it was abandoned.[24] While the algorithm was introduced to offset the optimistic predictions of teachers regarding the examination performance of their students, in practice the model penalised schools that helped students improve significantly between state examinations by benchmarking them against average school performance and its accuracy was contested.[25]

However, as the President of the Open Data Institute noted, this story simply highlighted the problems around automated decision-making when deployed by the public sector yet in other sensitive contexts where it is used - it is equally impactful as private sector-based algorithms yet does not attract the same critical attention.[26] The lack of transparency (prior and during the deployment process) is amplified by the blurring between public and private use. In many cases, the public sector will rely on tools developed, sold, offered for trial by firms with no scrutiny in the procurement process. This leads to tools being launched before having a public discussion on goals and impacts.

This example shone a spotlight on the underlying inequalities in the educational system by, for instance, systematically favouring students in smaller cohorts over those in larger cohorts with the former being more typical in fee-paying schools. This confirms an obvious danger of such technological solutionism beyond data protection and privacy; that societies look to technology as the default for addressing almost every problem – from inequality to climate change and shift focus away from the root causes of such crises.[27] While such root causes cannot be overlooked, nor should the capacity of respect for data protection and privacy to enhance trust in such systems be downplayed. If anything, by embedding existing inequalities in technological solutions, we run the risk of perpetuating these challenges rather than tackling their causes.

During the pandemic, digital service delivery accelerated across both the public and private sectors, with rights-based concerns often pushed aside in the wake of a worldwide crisis.[28] If left unchecked, the growth of this form of surveillance capitalism will have deep and long-lasting effects on many sectors. In fact, it could reduce or even reverse previous reasonable expectations of privacy in areas such as work, education and medicine.[29] In light of these technological and societal developments, it is now more important than ever for states to affirm, or reaffirm and explicitly state in written statutes, their commitment to data protection and privacy.

Affirming rights, explicitly, in constitutional documents or legal statutes, makes it clear to all citizens and organizations that a right is protected and recognized in such jurisdictions. While states have jurisprudence that affirms or clarifies rights, this remains a domain of lawyers and academics, and hence a more opaque affirmation of a right. In most societies, the general public are often unaware of legal decisions, and therefore poorly positioned to raise concerns about a breach of their rights. While judicial affirmation is legally sound, it does not always improve access to justice in practice or protections of privacy rights.

In brief, this protection cannot be left to non-accountable public bodies or market forces alone. It is needed as an essential check on the increasing power that data and technological infrastructures enable public and private actors to exercise over us as individuals, as groups and as society as a whole. Ultimately, our goal is to ensure that individuals and society can continue to benefit from digital services – to socialise, to learn, to shop, to interact with critical services – in a way that respects data protection and privacy, and other dependent fundamental rights. People, after all, have a right to live free from unwarranted state and corporate surveillance.

3. Origins of the right to privacy and data protection

To expand international support for the development of a rights-based international legal instrument on privacy and data protection, it is useful to first explore the scope and history of both the general privacy right and the right to informational privacy/data protection.

A. The origin of the right to privacy

In Western developed nations and the global north, the right to privacy has had a particular trajectory as a universal human right. In its original cultural understanding, individuals often link the idea of privacy to a physical dimension or a sense of place, such as the home, with the level of protection depending on how accessible that place is or should be to others. In a less tangible context, privacy is also often viewed as a form of secrecy (meaning privacy ceases to exist when the secret is shared) or confidentiality (whereby an intrusion is defined by a violation of mutual trust). This was demonstrated some two thousand years ago when Cicero penned his *Treatise of State Offices* as advice to his son, who was considering a career in the Roman State service.[30] Cicero asked the younger family member to consider what we citizens expect of government. For what is government, ultimately, established to achieve. What do we expect of it?

Cicero rose from the role of public prosecutor all the way to the consul of Rome asking such questions of his government. Why did Roman law insist on making such a sharp distinction between private things and personal space, versus things of the state and public property? He concluded that any proper government must protect the sanctity of both public and private spheres. That reasoning stands the test of time – why else do we have government and law if not to be clear on the line between the personal lives of citizens and the goals of the state?

Therefore, ancient Roman law extends the notion that government power to trespass on private property, search private space, and seize private papers or property – must be severely limited by law if privacy is to be meaningfully protected.[31] Such limitations and restrictions upon state intrusion and coercion into the private sphere places privacy squarely within the intellectual apparatus supporting both due process and the rule of law.

The other commonality between the right to privacy (in particular in communications) and rule of law (particularly its due process requirements) is that both are specific grassroots reactions to the problem of intrusive state power.[32] If we pick out an even more specific strand of the legal privacy debate, such as the privacy of personal papers and communications, we find still other early echoes. Most notably, in 1215 when King John signed the Magna Carta, it entrenched the personal right against unlawful government seizure or access to one's personal belongings. Specifically, the Magna Carta and its 39th clause, reads:

> *'No free man shall be seized or imprisoned - or stripped of his rights or possessions - or outlawed or exiled - or deprived of his standing in any other*

way - nor will we proceed with force against him - or send others to do so - except by the lawful judgment of his equals or by the law of the land.

The *Magna Carta* was a rule of law response to intrusive Crown warrants, so too was the Fourth Amendment of the *US Constitution*.[33] At its root, rule of law sets out a series of conditions before government can execute intrusive or coercive action. In other words, the government may only arrest, search or seize an individual or her possessions, property and papers with lawful process, be that through a judge (the lawful judgment) or what parliament has enacted (the law of the land).[34] With the Magna Carta's 800-year-old injunction in mind, comes the birth of debate around warrants, basic due process, government's powers of search and seizure.[35] The thread of concerns carries through from the thought of James Madison and Alexander Hamilton in their *Federalist Papers*, to the jurisprudence of Warren and Brandeis.[36]

While it took time for an individual right to privacy to evolve (prior to the seventeenth century) there was a long-drawn distinction in the Latin term *privatus*, between matters which belonged to the collective arena (and thus subject to public authority) versus what pertained to an enclosed community (governed under a household).[37] "The mistaken assertion that the notion of physical privacy was absent in medieval society", writes Diane Shaw, "perhaps derives from the modern assumption that privacy is individual and absolute, rather than communal and relative."[38] As noted succinctly by David Vincent, the narrative of privacy is not a progression from absence to invention, or necessarily less to more, but rather a fundamental right which has always underpinned our understanding of individual and collective life, where 'there are no beginnings in this history, only threatened endings."[39]

These western historical underpinnings of privacy and its understanding as a form of secrecy (meaning privacy ceases to exist when the secret is shared) or confidentiality (whereby an intrusion is defined by a violation of mutual trust) remained largely unchallenged until the late 19th century, when Samuel Warren and Louis Brandeis penned their 1890 essay, *The Right to Privacy*. Warren and Brandeis framed privacy as the "right to be left alone," challenging the traditional conceptualization.[40]

Specifically, the essay sought to identify a basis in law for a more active right of individuals to control and prevent the disclosure of their "thoughts, sentiments, and emotions" in the same way as they were already able to exclude others from any physical space under their control (using the rules of trespass).[41] Going beyond notions like "place", "secrecy" or "confidentiality", the novelty of this approach therefore lay, not least, in the extension of privacy's protective sphere. Rather than limiting the right to a purely spatial dimension it includes, among other things, the individual's right to control information relating to them.

This notion of privacy as an individual's right to control information continued on into the 20th century, as the rise of authoritarian and totalitarian regimes around the globe catalysed efforts to establish a right to privacy. Specifically at issue was the ability of these regimes to exercise power over their citizens as a direct result of their access to detailed information about the identity, thoughts, beliefs and actions of these citizens and to influence and control their behaviour accordingly.

Following World War II, this experience led to a widely shared acknowledgement among democratic governments that privacy as a human right had to be established and recognized in order to uphold democracy. This would protect individuals from interference with their private and family life, particularly, but not exclusively, by state actors. To be clear, we fully acknowledge these are particularized points in traditional liberal thought. In some instances, global privacy discourse has been shaped by that specific set of historical experiences. That should not, however, dissipate the concern. Privacy and data protection should be promoted as universal rights, through international instruments, precisely because these once-particularized risks have now been 'universalized' - by free flow of data, new technologies, international business models and congruence of government practices.

i. The right to privacy at the international level

At the international level, the *American Declaration of the Rights and Duties of Man* (ADRDM), was the first document to enumerate a list of rights, and was adopted by the nations of the Americas in May 1948. In the same year, the United Nations (UN) proclaimed the *Universal Declaration of Human Rights* (UNDHR), which provided expansive protections for privacy. According to Article 12 UNDHR:

> *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.*

By foregrounding a broad general concept of privacy, the ADRDM and UNDHR paved the way for more wide-ranging conceptions of privacy, going beyond privacy in certain places, such as the home, or contexts, such as in family life. Later international instruments followed this trend for broader privacy protection. For example, at the regional level, the Organization of American States (OAS) recognised an individual's general "right to have his honour respected and his dignity recognized. 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 honour or reputation," in the *Inter-American Convention on Human Rights (Pact of San Jose, Costa Rica)*.

The *European Convention on Human Rights* (ECHR), adopted by the Council of Europe in 1950 and entered into force in 1953, was the first legally binding international instrument to recognise a general right to privacy. Article 8(1) sets out the right ("Everyone has the right to respect for his private and family life, his home and his correspondence") before identifying the conditions for limiting this right in Article 8(2) ECHR.

Subsequently, the UN adopted the *International Covenant on Civil and Political Rights* (ICCPR) and an accompanying Optional Protocol in 1966.[42] These additional documents were open to accession and ratification by UN states and were binding for those that ratified them. The right to privacy is found in Article 17 of ICCPR, which 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.*

In order to oversee compliance, the UN Human Rights Council (HRC) considers periodic reports (submitted by the State parties to the ICCPR) on compliance with the ICCPR rights.[43] To date, the HRC has issued over 100 views touching upon compliance with Article 17 ICCPR by State parties.[44] However, the legal status of its findings or "views" remains contested.[45] As of 2015, there was also created a UN Special Rapporteur on the Right to Privacy, who researches and publicizes reports on a wide range of data protection and digital rights issues.[46]

Another body, the International Law Commission, is tasked by the UN Charter to initiate studies and make recommendations to encourage "the progressive development of international law and its codification."[47] The "protection of personal data in the trans-border flow of information" was included in the long-term work programme of the International Law Commission in 1997. That work has been further developed through the policy work and reports of various relevant Special Rapporteurs, like those for Freedom of Opinion and Expression, the Right to Privacy, and the Rights of Children. As well, the international advocacy of individual rights-holders and national human rights institutions continue to inform and influence the development and interpretation of modern rights instruments and reviews at the UN. These efforts have resulted in clear progress (e.g. the UNDRIP) and will likely play a key role in any future development of new privacy instruments.

ii. The right to privacy at the national level

At national level, a right to privacy and/or data protection was commonly established in one of four ways:

Constitutional provisions: Firstly, countries may expressly include rights to privacy as a fundamental right in their national constitutions or Bill of Rights.[48] Although rare until the 1960s/70s, this approach is now followed, among others, by Mexico, Switzerland, Belgium, Korea, Philippines, Hong Kong, Portugal, Colombia, Chile, Trinidad and Tobago and Gabon, several of which subsequently included such rights in their existing constitutions.[49] Not all of these countries recognise a general right to privacy. Instead, their constitutions may include rights that protect a specific aspect of privacy. For example, the Bermuda Constitution protects a very specific right to protection for the privacy of an individual's home and other property.[50] In countries with a federal structure, rights to privacy and/or data protection may also be included in the relevant state, rather than federal, constitutions. For example, in Germany, the state Constitutions of all of the "*Neue Bundesländer*" (states that became part of the Federal Republic following reunification between West Germany and the GDR in 1990) and several of the other states include an express right to privacy, informational self-determination, information privacy or data protection.[51] Similarly,

the Australian state of Victoria has enshrined the right to privacy in Article 13 of the Victorian Charter of Human Rights and Responsibilities 2006.

Specific legislation: discussed in detail in the next section ("the origin of the right to data protection"), many jurisdictions in the 1960s and 70s created sector-specific privacy law or data protection legislation. Some states may even explicitly recognize the right in quasi-constitutional statute such as domestic human rights codes or privacy laws.

Jurisprudence: In countries whose constitutions do not expressly include rights to privacy or data protection, domestic courts may nevertheless establish such rights by reference to, or relying on a combination of, one or more other rights. For example, the German Constitutional Court recognises a "general personality right" as well as a "right to informational self-determination" on the grounds of Article 2(1) ("right to self-determination") in conjunction with Article 1(1) ("human dignity") of the German Basic Law.[52] Canada protects certain aspects of individuals' privacy as part of the rights to liberty and freedom from unreasonable searches and seizures set out in Article 7 and 8 of the Canadian Charter of Rights and Freedoms.[53] A similar approach is taken in the US, which protects an individual's "reasonable expectation of privacy" as part of the Fourth and Fourteenth Amendments (protection against unreasonable search and seizure and due process). In Japan, Article 13 of the Constitution (right to the pursuit of happiness) has been interpreted by the courts to include the right to privacy.[54] More recently, in 2017, the Supreme Court of India ruled that privacy is a fundamental right because it is an integral part of the right to life and personal liberty guaranteed in Article 21 of the Indian Constitution. The decision framed privacy within the entire spectrum of fundamental rights enumerated by their constitution and noted how this enables other rights such as such as freedom of speech and expression, freedom of association, freedom of religion and the right to equality.[55]

International agreements and treaties: Alternatively, countries may decide to give direct domestic effect to international human rights instruments to which they are a party, or they may adopt those international instruments as binding domestic law in a way that allows for their enforcement before the domestic courts. For example, the 55 countries that are Parties to Convention 108 have adopted legislations that comply with the provisions of the Convention. The EU Charter of Fundamental Rights directly applies in all 27 EU member states when they adopt or apply a national law implementing an EU directive or when their authorities apply an EU regulation directly.[56] Austria, retrospectively granted the ECHR domestic constitutional status in 1964, while the UK, after having been one of the Convention's original signatories (and drafters), eventually decided to make it binding and capable of being enforced before the British courts in 1998.[57] A similar approach was taken by the Isle of Man, a British Crown dependency, when it adopted its Human Rights Act in 2001.

B. The origin of the right to data protection

Unlike the right to privacy, which was introduced in a decidedly "top down" manner as part of, mostly international, fundamental rights instruments, it could be argued that the right to data protection developed more from the bottom up. Its emergence is

often described as a response to advances in technology and the development of new data-heavy business models and stemming from a desire to protect individuals from their potentially adverse effects. Those effects include, in particular, the unauthorised collection, use, storage, combination, sharing and disclosure of individuals' personal data.

The contemporary origins of modern frameworks for data protection law can be traced back to the German state of Hesse, which is credited with the adoption of the first statutory data protection instrument, the Hesse Data Protection Act 1970.[58] Although arguably the first to adopt a law of this kind, it was, however, quickly followed by a number of other, mostly European, countries including, in 1977, the Federal Republic of Germany.[59] At the time, no right to data protection was expressly included in the German Constitution nor in any of the state constitutions of the German "Länder", nor in any other constitution of a European country .[60]

Inspired by those changes and conscious about an increasing flow of personal data across political boundaries, international experts drafted two international documents in the late 1970s: the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and Convention 108. The latter was an open multilateral instrument based on the Vienna Convention of the Law of Treaties which paved the way for future national and regional data protection legislations, including the EU's Directive 95/46/EC. Convention 108 was the first legally binding multilateral instrument on data protection, laying down the foundations for modern data protection legislation, by requiring its state Parties to apply the overarching principles of data protection (such as fair and lawful data processing, the specified and legitimate purposes, data quality, and a transborder data flow regime) , which rapidly became influential, first among the Member States of the Council of Europe and as of 2013 also on other continents. The European Union, as the perceived global standard bearer for data protection and with its quasi-federated regional/national/state structure of governance, serves as a useful example for scrutinising this "creation myth".

The EU expressly referred to Convention 108 when adopting its comprehensive data protection framework as "secondary law,"[61] stating that it intended to "give substance to and amplify" the principles found in Convention 108.[62] The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('1995 Directive') was adopted in 1995 as a common market instrument with the intention of harmonising the national data protection frameworks of EU member states that had developed over the previous two decades.[63] The 1995 Directive meant to provide a basic standard of protection across member states with the dual aim of protecting "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data", and facilitating the free flow of personal data between the member states in line with the objectives of Convention 108.[64]

At that time, the EU had not yet adopted its own fundamental rights framework. Instead, it largely relied on a shared understanding between the member states that the "fundamental rights" referred to in Article 1 of the Directive included the provisions of the Council of Europe's ECHR (which all member states had ratified) as well as any fundamental rights protected by the member states' own national constitutions or bills of rights. The absence of an overarching fundamental rights

framework did not therefore stop the EU from adopting a comprehensive data protection framework largely based on Convention 108. The EU Charter of Fundamental Rights, which now includes an express right to data protection in its Article 8, was adopted as part of the Lisbon Treaty and came into effect on 1 December 2009.[65] This very close link, even symbiosis, based on shared principles and values between the two data protection frameworks was yet again emphasised when both were updated by a statement from the EU Commission on the EU joining Convention 108+ once it enters into force.[66]

Within the United Nations context, the only UN instrument to specifically deal with data protection is a set of non-binding "Guidelines for the regulation of computerized personal data files", dating from 1990.[67] As Kuner notes, while the normative basis of data protection law is heavily reliant on international human rights texts such as the 1948 UNDHR and the 1966 ICCPR, these instruments do not mention data protection specifically.[68] Therefore, while the right to data protection is recognised explicitly in some domestic Constitutions, the EU's Charter of Fundamental Rights is the only existing international instrument to recognise data protection as a distinct fundamental right.[69] The EU reformed and upgraded its data protection framework in 2016 with the adoption of the General Data Protection Regulation (GDPR) and the Police Directive. The two legislation remain rooted in the principles advanced in Convention 108.

i. Modern efforts to strengthen rights to data protection and privacy internationally

We can see that while privacy and data protection are now widely recognised in countries around the world and in the context of a variety of constitutional arrangements, they remain under-developed and underutilised at international level. The right to data protection has yet to emerge as an internationally recognised right. It is therefore unsurprising there are calls to strengthen the recognition and application of these rights at international level.

One prominent example of such a call to strengthen these rights is the 2005 Montreux Declaration made by the International Conference of Data Protection and Privacy Commissioners (ICDPPC), now known as the Global Privacy Assembly (GPA).[70] Through the Montreux Declaration, the ICDPPC noted, "it is necessary to strengthen the universal character of this right [to privacy and data protection] in order to obtain a universal recognition of the principles governing the processing of personal data whilst respecting legal, political, economical and cultural diversities."[71] The Declaration requested the UN to prepare a legally binding instrument, which "clearly sets out in detail the rights to data protection and privacy as enforceable human rights."[72] The ICDPPC's Madrid Resolution on International Standards on the Protection of Personal Data and Privacy was a similar call, made in November 2009.[73] Subsequent attempts have been made through the ICDPPC/GPA to draft a global legal instrument on data protection in 2009 and to advocate for the adoption of a 3rd Optional Protocol to the ICCPR to adopt an international privacy standard consistent with ICCPR Article 17.[74]

These efforts to reinforce the rights to data protection and privacy at international level remain works in-progress. This might be attributed to the ineffectiveness of existing enforcement mechanisms and differing perspectives across jurisdictions. Other contributing factors might include imbalances of information and power in modern digital environments, or that regulatory priorities are spread across a wide range of sectors, issues, and stakeholders. Both phenomena prevent privacy risks from being easily perceived or rights to be effectively exercised. Nevertheless, the path for international cooperation is becoming clearer.

First, existing international cooperation in these fields has had mixed success.[75] This is owing to a number of factors. Some relate to the characteristics of the UN instruments. They consist of a patchwork of rules across various instruments and this "normative dispersion" affects their accessibility and effectiveness. Moreover, given their soft law nature, many of the existing instruments (such as the Guidelines for the Regulation of Computerized Personal Data Files) are not invoked or applied by the HRC.[76] Some attribute this lack of practical utility to timing, as relevant UN Guidelines were adopted after important international instruments, such as the OECD Privacy Guidelines and the Council of Europe Convention 108.[77] Yet, even in data protection regimes that are held up as success stories from a fundamental rights perspective, such as the EU's GDPR, there remains a disconnect between the letter of the law and its practical application.[78]

Yet, while more should be done to promote and apply existing international and regional data protection frameworks, it would also be wrong to conclude that these frameworks have not had impact. The Inter-American Court of Human Rights has developed an important line of case law establishing a multi-faceted vision for the right to privacy and imposing a positive obligation on States to guarantee the respect of this right by public and private entities as well as individuals.[79] The provisions of international agreements, including the UN instruments, are also often given constitutional status by domestic Constitutions. For example, the Basic Law of the Hong Kong SAR gives constitutional effect to the provisions of the ICCPR. Regional human rights instruments recognising rights to data protection and privacy, such as the EU Charter of Fundamental Rights, have also been invoked to significant effect in challenging and ultimately invalidating incompatible legislative instruments.[80] In sum, while improving the effectiveness of these supranational legal frameworks remains challenging, these efforts are already having tangible impact and are worth pursuing further.

Differing perspectives have also limited the recognition of data protection and privacy as rights.[81] Today, opinions on this question are not as easily divided along geographic lines. Many business stakeholders and officials fear a continued, strong commitment to fundamental rights protection will require foregoing technological and commercial developments. This view is prevalent, despite rapid growth and rising profit margin across technology sectors. Others erroneously see privacy as a "barrier" or "impediment" to innovation. Or they may recognize only the commercial and business aspects of innovation, while disregarding an equally urgent need to support social and legal evolution.

This perspective explains in large part why, “once one descends from the highest level of abstraction, there can be significant differences in detail” amongst regional and national data protection approaches.[82]

Differences: free expression in the UK

Another common point of differentiation between States is their stance on freedom of expression. Typically, in states where there is a strong legal tradition of freedom of expression, there has been a reluctance to recognise or fully develop the right to privacy. In England and Wales, the Courts refused to develop a right to privacy without a legislative underpinning. As recently as the 1990’s, the Court of Appeal explicitly stated “it is well-known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person’s privacy”. However, this example also illustrates that once a right to privacy is recognised in a domestic legal system, as it was in the UK through the Human Rights Act 1998 and ultimately by the House of Lords in its 2004 Campbell judgement, it can be quick to entrench itself and become an established part of the legal landscape. These cultural and ideological impediments to cooperation are therefore surmountable, leaving reason to be optimistic about the scope to develop the rights to privacy and data protection at international level. **Sources:** *Kaye v Robertson* [1991] FSR 62, per Glidewell LJ; *Campbell v Mirror News Group* (MGN) [2004] UKHL 22.

We can differentiate between two approaches to the development and implementation of regional privacy and data protection instruments. One set is built primarily on the recognition of the *fundamental rights* implications of personal data processing (such as the African Union Convention on Cyber Security and Personal Data Protection, Convention 108 and the GDPR). The other set view *data as an essential commodity*, commercial asset or input for goods and services, and therefore seek to maximise its potential for exchange and trade by minimising regulatory friction (such as the OECD *Privacy Guidelines* and the APEC *Privacy Framework*). In practice, such regimes differ in five important ways.

First, the interpretation of rights-based frameworks is guided by fundamental rights reasoning (including, for instance, incorporating necessity and proportionality assessments). By contrast, market-based approaches incorporate market-based assumptions (such as the “notice and choice” paradigm). Second, rights-based frameworks grant rights to individuals (the rights-holders), such as the right to access, the right to obtain deletion of personal data, and object to its processing. These rights have correlating duties which must be met by states and by private entities (the duty-bearers), to respect these rights. Such rights are absent or less prominent in market-oriented regimes. Third, rights-based regimes are often backed up by binding statutes and enforcement mechanisms applied by an independent authority with a public law aspect.

This rights-based system recognizes both that a breach of individual rights is a harm to the public good, and that there is a public interest in protecting, enforcing, and promoting these rights by holding accountable those who breach them. Whereas in market-based approaches, accountability more often arises in the form of private law actions such as commercial dispute resolution, or lawsuits under contract or torts jurisprudence. Finally, a rights-based approach recognizes the inherent right to

dignity of citizens, and explicitly addresses power imbalances to protect those less powerful from harm, whereas a private market approach often ignores power imbalances and assumes harms will be automatically calculated into the cost of a good or service through market forces.

Nevertheless, there remains scope for convergence between these ostensibly distinct logics. Respect for data protection and privacy is often a legal prerequisite for the liberalisation of personal data flows, blurring the boundaries between market-based and rights-based approaches. Equally, respect for these rights is also a prerequisite to ensure user trust in innovative data uses. Therefore, just as promoting respect for environmental principles helps to ensure long-term sustainability, so too promoting respect for data protection and privacy can help to ensure sustainable innovation.

C. What is data protection and how is it different from privacy?

As previously noted, compared to the right to privacy, the origin of data protection as a right and its precise, fundamental character is a bit more recent.[83] Since the right to data protection first found its way into national constitutions in the 1970s and '80s, courts and academic scholars have found it difficult to identify clear demarcation lines between the two rights. This situation is not helped by the fact that, although a right to data protection now appears in a growing number of national and state constitutions, the EU Charter is to date the only international legal instrument to differentiate explicitly between the rights to data protection and privacy.[84]

National and international legal instruments that expressly include a right to data protection share a number of common characteristics.[85] Most notably, national and international legal instruments that specifically protect the right to data protection often require that an independent supervisory authority be established to enforce those rights and obligations.[86] The procedural nature of this approach has led some to argue that, unlike the right to privacy, the right to data protection is not so much a substantive but a procedural right that ultimately gives effect to the right to information privacy by establishing a set of detailed rules for its performance.[87] In order to establish whether this is true, we must analyse in more detail the specific character of the right to data protection and what it is designed to protect.

i. The relationship between data protection and privacy

Some experts continue to doubt whether data protection should have fundamental rights status at all. Veil, for instance, suggests that data protection only becomes a defensive right in court when combined with another fundamental right and, as a result, data processing should only be relevant under fundamental rights if it specifically impairs, or risks impairing, freedom.[88] Amongst those who accept the designation of data protection as a fundamental right, there are differing conceptions of its relationship with the right to privacy. These can be broadly grouped in three (or four) ways.[89]

A first conception is that the two rights are *completely distinct yet complementary* in so far as both seek to achieve higher order values, such as dignity, autonomy or the

control and limitation of power. De Hert and Gutwirth suggest that privacy is a “tool of opacity” which helps to set limits on power and prevent illegitimate and excessive use of power, while data protection is a “tool of transparency” that controls and channels power through transparency and accountability.[90]

A second conception is that *data protection is simply a subset of the right to privacy*. This is perhaps the most commonly held view of the relationship. For the European Court of Human Rights, for instance, personal data protection is viewed and regulated in relation to Article 8 ECHR, the right to privacy. Similarly, as Solove notes in the US, the “constitutional right to information privacy has emerged in the courts as a spin-off of the regular constitutional rights”.[91] Yet, even when the right to privacy subsumes data protection, it is possible to distinguish between situations where data protection is treated *as privacy* and those where the main purpose of data protection is considered the protection of privacy.[92]

A third conception, with a growing number of adherents, is that *data protection and privacy are distinct yet heavily overlapping rights*, with data protection serving a multitude of functions including, but not limited to, respect for privacy. Data protection and privacy are distinct as far as they have different scopes of application; privacy covers areas that data protection does not, such as issues of bodily autonomy and family life, while data protection is not concerned with issues of “reasonable expectations” of privacy and extends its protection unconditionally to public and voluntary data processing activities.[93] This notion is reflected in Article 1 of Convention 108+, which states that “the right to data protection is autonomous, contributing to the respect for human rights and fundamental freedoms, in particular the right to privacy.” The text defines the right to data protection as a separate, contributing right to other human rights, particularly the right to privacy.

A fourth conception views data protection as emerging from a positive duty of the state. This is especially relevant in jurisdictions such as India and US, where fundamental rights are primarily structured as “vertical” rights, offering protection against state action. The right to data protection, conversely, is most often framed as a ‘horizontal’ right against private entities.[94] The evolving nature of fundamental rights is not merely one of negative rights (namely, protection preventing state action) but also positive rights, creating obligations for the state to protect rights (against private entities). Thus, privacy acquires indirect, horizontal application, even in jurisdictions where fundamental rights are only available as vertical right.[95] Thus conceived, data protection is not a subset of privacy, but emerges from a positive duty of the state via its privacy obligations.

As de Hert and Gutwirth suggest, “few direct manifestations of intimacy-oriented conceptions of privacy can be found in the provisions of data protection laws and, conversely, broader privacy concepts are not of a nature to explain data protection principles such as purpose limitation, data quality or security.”[96] Data protection also grants individuals a broader array of rights in relation to their data than privacy, including rights to access data and even rights to portability.[97] Yet, as the scope of the right to privacy is jurisprudentially expanded to address concerns in the digital age, the overlap between these rights grows.

Lastly, in human rights law writ large, there is a mutual recognition of rights as developing in concert with each other, and with society. In considering the rise of importance of data protection and privacy, it is useful to note that a rights based framework acknowledges the ever-developing nature of rights. . Rights are not be frozen in time, nor static, but evolve as society itself evolves. This responds to real needs of individuals for protection, so they may live with dignity and respect. International human rights law is based on a fundamental principle that rights are interrelated and interdependent, and that as one right is better protected, others may in turn be better realized. In this framework, one could examine the modern context as a deepening of interrelatedness and interdependencies between privacy, data protection, and other rights which are all simply arising into public and legal consciousness with different rates of speed and impact.

ii. Information privacy and informational self-determination

Regardless of whether we view data protection as a subset of privacy, as two rights that are "distinct but overlapping", or as the inherently interrelated and interdependent evolution of modern rights progressing, there is undoubtedly a clear overlay between what is protected by the right to data protection as defined in the EU Charter and certain national or state constitutions and what Westin and Fried, in the late 1960, described as "information privacy". According to Westin, information privacy is the "claim of individuals, groups, or institutions to determine for themselves how, when, and to what extent information about them is communicated to others."[98]

This definition of information privacy as individuals' right to "determine" or "control" what can be done with their data suggests a close relationship between this right and the general right to privacy. This follows the same path as 19th century American privacy scholars, Samuel Warren and Louis Brandeis, who had earlier expanded the material scope of the right to privacy by adding to the commonly recognised physical or "spatial dimension" element with a new privacy dimension that included the protection of an individual's "thoughts, sentiments and emotions".

Others like Ruth Gavison or Shoshana Zuboff point to other, broader definitions. These acknowledge the current imbalance of power in data and privacy fields, and recognize that new powerful systems of gathering and commercialization of digital information about citizen's private lives are akin to other historical shifts, such as the shift from natural land to real estate markets, or from barter economies to human resources which are market-driven labour.[99]

Both the right to informational self-determination (or information privacy) and the right to the protection of the private sphere are rooted in the same fundamental values that also highlight that, aside from their common origin, the two rights share a common objective, namely the protection of human dignity and of individual autonomy.

iii. The "added-value" of data protection

Once recognised as a distinct fundamental right, this begs the question of what independent values the right to data protection offers to individuals or society. As already highlighted above (and further discussed below), when we ask ourselves

what we protect through the right to data protection, informational self-determination is a common retort.

Beyond informational self-determination, some view data protection through the lens of fairness and good data governance.[100] Post, for example, suggests that Article 8 EU Charter "creates fair information practices that establish bureaucratic rules to structure the decision-making of persons who are figured as asocial and autonomous."[101] Van der Sloot contrasts the "Athenian ideal of private life" with the focus of data protection on "whether data is used fairly and with due process".[102]

Others go further and suggest that the right to data protection provides "a right to a rule" or a right to a legal framework governing data processing. Following the logic of the EU Charter right to data protection, this legal framework would, at a minimum, include rights for individuals, impose obligations on those who process personal data and set out an effective and independent oversight and enforcement mechanism.[103] In this sense, the value served by data protection is simply to lay down the rules of the game in order to facilitate other rights and interests.[104]

iv. Data protection as a procedural or substantive right

If an independent right to data protection exists to give people more control over their personal data, or to guarantee the existence of a legal framework for personal data processing, does this then make data protection a procedural right? Some certainly think so, suggesting that data protection "does not directly represent any value or interest per se; it prescribes the procedures and methods for pursuing the respect of values embodied in other rights".[105]

Yet, it may be an over-simplification to dismiss data protection as purely procedural. In reality, it is a hybrid right. If it seeks to achieve informational self-determination, this is an end in itself as well as a vehicle to achieve human dignity and to promote democracy.[106] If the right to data protection is a right to a legal framework governing data processing, then we must recognise that some elements of that framework are primarily procedural (such as transparency and accountability requirements) while others are substantive, requiring a legal process in which to consider the weighting of interests and rights.[107] Even if data protection were considered a "procedural" right, serving no independent value, this is no reason not to consider it to be fundamental.[108]

In fact, the UN has recognized that specific rights that may be emerging or more recently articulated, are just as fundamental. For example, the UN Convention on the Rights of Persons with Disabilities (CRPD) Article 9 notes that the accessibility principle is key to the realization of the rights of persons with disabilities. The CRPD treaty body has noted that "accessibility" is not simply a procedural right, but rather an expression of a fundamental right of access guaranteed in the ICCPR and CESCR.[109] Its emergence and recognition over time did not diminish that universal recognition. In a similar way, data protections might be seen as a vital precondition for the effective enjoyment of civil, political, economic, social, and cultural rights in our current era, and deserving of similar recognition in international law.

Expanding privacy rights: the German Census decision

The German Constitutional Court set out a practical instance for expansion of the meaning of the right to self-determination in their seminal 1984 "Census" decision. This was in response to the excessive data collection and processing powers granted to the German Government by the *Census Act 1983*. The Court developed a new right to informational self-determination that limited those powers. Mirroring, almost to the letter, the sentiments expressed by Westin more than 15 year earlier, the Court held that the German Constitution specifically protected the individual's right "to decide himself when and within which limits details of his personal live should be disclosed". In the absence of a specific right in the *German Basic Law*, the court defined this new "right to informational self-determination" as an aspect of the "general personality right" of the individual that was itself based on two existing rights. These were the right to self-determination in Article 2(1) and the right to human dignity in Article 1(1) of the *German Basic Law*. That general personality right, which had been recognised by the Court since 1973, and before it by the Federal Civil Court since 1954, had until then solely protected the individual from the unlawful interference with their private sphere. However, rather than describing the right to informational self-determination as a subset of that older right, the court moved to grant the two rights equal yet separate status with a shared origin. In substance, the right to informational self-determination guarantees the right of individuals to control both the disclosure of their personal data and the way in which and the purposes for which those data are used. The Court argued that in the context of modern data processing procedures the individual requires protection against the unlimited collection, storage, use and disclosure of their personal data. The right has therefore traditionally restrained public authorities from the bulk collection and processing of personal data or from using specific identifiers linked to such data to make decisions that have a legal effect on individual citizens. Because of the ability of modern IT systems to connect and combine data, the Court found that "immaterial data" no longer existed (even data that in itself seemed irrelevant could gain relevance in conjunction with other data). Consequently, the Court ruled that the protection of personal data could not be dependent on whether such data related to an individual's private or intimate sphere. Instead, in order to assess how relevant the processing was in the light of a potential violation of an individual's dignity and self-determination, it was essential to establish the purpose for which that data was collected and how it could be used or linked to other data. Thus, was born the idea that personal data deserved fundamental rights protection equivalent to the right to privacy even where those data could not be considered "private". **Sources:** Census Act, BVerfGE 65, 1; English translation provided by German Konrad-Adenauer-Stiftung; available at https://freiheitsfoo.de//files/2013/10/Census-Act.pdf; last accessed on 20 October 2020.

4. What do we protect when we protect privacy and data protection?

The development of both the right to privacy and the right to informational self-determination in the EU legal context (noted above) arguably highlights something that may be less apparent in later fundamental rights instruments that include an express right to data protection. Namely, that privacy (as a concept and as a legal right) is itself derived from (and designed to protect) a variety of individual and public interests, rights and values. This includes individuals' right to self-actualisation and the development of their own personality.

Self-actualisation encompasses the right to decide how an individual presents themselves to others (e.g. control over one's public image and reputation) and the extent to which they make themselves and their lives accessible (e.g. consent and control over publication of personal details). It covers their right to both develop and communicate opinions and convictions free from unwanted observation by others (e.g. dissent from government policies or critique of political decisions). As well, it supports the right to make decisions and take action based on those opinions and convictions that may affect not just them but also collective and public interests.

The assumption underpinning all of these rights is that without privacy and data protection – without the right to exclude others from accessing our space, our actions and our thoughts – we cannot develop and express our own individuality to its fullest potential. Consequently, we are prevented from participating in communal interactions and decision-making processes as our own authentic self (e.g. where employees self-censor in a workplace for fear of reprisal). This ideal of individual self-determination, self-actualisation and control, expressed in both the general right to privacy and the right to information privacy, therefore reflects more fundamental values of human dignity, liberty and autonomy. We will examine those values in turn.

A. Human dignity

Human dignity is arguably the most significant among these values as it protects the essence of what it is to live as a human being, to be valued for one's own sake and to be treated with respect. The overarching importance of this right is highlighted by the UN Declaration of Human Rights which recognizes the inherent dignity of all members of the human family as well as Convention 108+ and the EU Charter of Fundamental Rights, which incorporates the respect and protection of human dignity as its very first article.[110] The right to human dignity is also the first right of the German Basic Law and one of the few absolute rights included therein. It is one of only two rights included in the Basic law that cannot be amended except through the adoption of a new constitution. Human dignity is thus protected as an important ethical and legal value. More practically, it also reinforces prohibitions on such inhumane practices as slavery, torture, and human trafficking.

The requirement to treat everyone as a person with respect for their humanity, and not to subject them to inhumane treatment reflects Kant's moral concept of dignity as the need "to treat humanity, whether in your own person or in that of any other, in every case at the same time as an end, never as a means only."[111] The immediate

implication of such a requirement, thus, would be that no one should be used only as a means to achieve other ends.

This possibility has, however, been raised as a concern in relation to personal data processing practices which might reduce individuals from subjects to mere objects. Lyon, for instance, warns that the increasingly intensive use of personal data by computers might run the risk of degrading individuals to mere commodities and subjecting human values to mere efficiency.[112] Citron and Pasquale share a similar concern, showing how the present-day practices of data-driven scoring could turn individuals into ranked and rated objects.[113] Many scholars in the field of surveillance studies have been very critical of privacy – as a discourse and as a regime of governance.[114] They believe that it does little to restore power imbalances and regard legal and constitutional protections of a right to privacy with suspicion.

Human dignity, social sorting and digitization

An illustrative phenomenon in this context is credit scoring. For the financial sectors, the use of Big Data (including using non-credit information such as social media or purchasing or browsing patterns) to assess credit scoring is likely to result in cost savings, because data can be used to identify patterns of potential default that would correctly apply to most of their customers. However, any individual who ostensibly matches the pattern criteria but who is in fact not likely to default will suffer from this categorisation as they are not treated as they should have been based on their own individual circumstances. Their individual situation is instead simply ignored in the interest of the company's revenue maximizing strategies. Similarly, companies and other data users may fail to make allowances for the fact that the raw data that feed their decision-making algorithms may be incorrect or out of date. This could affect not just the individual in question but also the further development of the algorithmic pattern itself (particularly where the raw data is part of a training set of data) with long-term consequences for those for whom the algorithm produces practical or legal effects. Finally, in the age of machine learning, algorithms are designed to "improve" on their original programme based on the data they are fed. Companies themselves may no longer be able to identify the criteria the algorithm uses, resulting in "computer says no" scenarios where algorithmic decision-making eludes accountability and potential algorithmic bias towards specific types of individuals becomes undetectable in practice, thus defying regulatory oversight. This opacity of algorithmic decision-making is further examined on page 34.

Credit scoring is only one of many examples.[115] All of these cases show that the *datafication* of individuals in a way that is outside of those individuals' control reflects a disrespect of individuals as humans that violates human dignity as data users show no care either for those individuals' welfare or their right to equal treatment. Over the past two decades, shifts in the scale of digital data-gathering (as well as the extent of their global reach and storage capabilities) underscore a stark imbalance of informational control. The resulting power imbalances (flowing from digitization and data markets) creates risk for political, social, economic and cultural rights (not only human dignity).[116] The power imbalances at play and the scope of potential harm are a strong argument for why privacy should be clearly articulated as a human right. A right to information privacy that enhances individuals' control over their data is therefore seen as a way to protect against such violations.

B. Liberty and self-determination

Much of the discussion surrounding the right to privacy has further been oriented to the goal of protecting individuals from interference by government agencies, especially taking into account the present existence of ubiquitous electronic surveillance. In this context, the right to information privacy is enlisted to protect the arguably even more fundamental value of "liberty" as the ultimate right of the individual to be free from such state interference. Indeed, Lyon argues that liberty is a preferable term over privacy when talking about the totalitarian tendencies in a surveillance society.[117] Although the exact meaning of liberty is not immutable, it is generally understood as individuals' unabridged natural right to follow their own will.[118] In this context, the metaphors of the Big Brother and the Panopticon are commonly viewed as a constraint on one's free will through surveillance that is both obvious and real or where the individuals believe themselves to be under observation without being able to verify exactly when and on what conditions that surveillance takes place.[119] In both of those cases, so the argument goes, individuals will adapt their behaviour to meet the rules and expectations of the observer.

C. Autonomy and choice

Lastly, the notion of privacy as individual control is arguably underpinned by the concepts of "autonomy" and "choice". In liberal theory, individuals are first and foremost autonomous agents achieving self-actualisation through even mundane decisions.[120] Both the idea of human dignity and of individual liberty suggest that we ourselves should be the author of our story, the "master of our fate", and the "captain of our soul".[121] Liberal economic frameworks also argue that choices of consumers in the market are free choices as they assume that both parties have complete information – that meaningful choice implies full information and transparency.

However, in reality, a delicate balance of constraints and choices nevertheless informs our decisions. Specific economic, social and political environments within which we operate determine these. In the current environment, both the state and the private sectors which gather, trade in, and use big data of citizens, have both an enormous information advantage, and the opacity of how they use this data.[122] Additionally, current examinations of online consent forms make it clear that citizens and consumers may not have meaningful choices, nor the autonomy to opt out of consent to have their information gathered and used in ways that advantage companies and states, and disadvantage consumers and citizens.[123] Even in democracies, this data can be exploited to opaquely manipulate voters, without their knowledge or consent. Rights and enforcement of fair rules to respect these, may be seen as a way to allow fuller autonomy and more meaningful choice.

As individuals, we do not exist in a vacuum, and we do not make decisions outside of the prevailing power structures that either privilege or disadvantage us (or sometimes both in different ways). In truth, autonomy is bounded by existential self-interest, economic dependencies, our relationships with, and obligations towards, others, and by the relative power (as well as any responsibility, see above) that we may have as members of our respective communities. These are presented for consideration and reflection in an Annex to this narrative.

5. Privacy and data protection as individual or collective rights

The “communal” element of the rights to privacy and data protection is a matter of some contention. On the one hand, the status of those rights as individual rights in most liberal human rights instruments has been met with extensive criticism from proponents of communitarianism and from those that advocate for the adoption of a greater focus on collective or societal interests. However, this criticism is not without its own challenges. If privacy amounts essentially to a “right not to participate in the collective” and to “isolate the individual from various kinds of interference”[124], how then can it reliably be employed to promote community needs? How does privacy as a ‘right to be left alone’ (Warren and Brandeis), on the one hand, interact with the “social value” of privacy (Priscilla Regan)?[125]

Arguably, an approach that combines the commodification of personal data with a conception of privacy/data protection as a tool designed solely to facilitate individual control, may convince individuals, businesses and legislators more easily of the intrinsic value and legitimacy of certain “privacy trade-offs.”[126] As already explained above, in those cases, the “privacy risk” attached to a processing activity – whether carried out by private or public sector controllers – will be perceived as only one of a number of competing risks, where other risks include existential threats, economic detriment and the fear of social exclusion.

In practice, this makes it easier for individuals to justify data processing (to themselves and to others) that they view as serving overriding individual, commercial or communal interests. However, this also means that privacy and data protection as fundamental rights are often deemed secondary to other rights and freedoms. The right to life, freedom of expression, or freedom of the press are just three common examples. Similarly, public interests that compete with or often override privacy include public order, national security or public health, which more obviously benefit both individual and collective or societal interests.

A. Cultural differences?

Equally, it is often suggested that the idea of “privacy” as an individual right is a liberal construct that does not map well onto the cultural, historical, religious, and philosophical traditions that shape the worldviews of communities, particularly, in parts of Africa, some parts of the Asia-Pacific economies, and also in areas where colonial history has harmed Indigenous populations, such as Canada and Australia.

Clearly different regions and polities debate issues of rights, responsibilities and redress from their own unique history and societal experience. To acknowledge those divergences and nuances is a prerequisite to understanding how to improve data protection, not a hurdle. Development of any regulatory ecosystem - whether in the EU, North America or Latin America – represents conscious evolution and deliberate negotiation. None came into being ‘naturally’, nor are any ‘inevitable’.

In point of fact, at present, many of the countries around the world (in the Asia-Pacific, Africa and Latin America) considering adoption or review of their data protection regime do so *unencumbered* by the history and philosophy which

underpinned adoption of the first-generation of privacy laws.[127] As noted above (see 'origins of the right to privacy'), many of those were particular legislative responses to specific government surveillance practices tied to WWII and the early Cold War.

Societies in the developing world, by contrast, have had considerable remove from that aftermath. Instead, their particular governments have been preoccupied with reconstruction, development and integration into a globalized economy in order to provide a better future to their population.[128] From that standpoint, they and their citizens actively support innovation, digitization and cross-border sharing of data.[129] Those perspectives and priorities need to be acknowledged, validated and supported, not marginalized, ignored or excluded.[130]

To highlight just one example of that complexity, within the APEC region, there are multivalent traditions, legal systems, political models and socio-economic models. That variance arguably outstrips even that of Europe or the Americas, and privacy debates are ongoing. For instance, discussions at the Osaka Summit in June 2019 reignited the simmering tensions over data governance, with many Asian nations opting for very different paths on critical data issues.[131] India in particular argued that any rulemaking on data governance outside of the World Trade Organization (WTO) would dilute the voices of emerging economies in the debate and suppress their sovereign right to frame rules that further their citizens' best interests.[132]

In practice, data protection laws have developed organically in Asia as they have elsewhere, in countries that live under the influence of Daoism, Buddhism, and Confucianism (e.g. Korea or Japan) and have adopted such measures for decades.[133] Korea's PIPA for example has the reputation to be one of the strictest data protection laws in the world. So these divergences are not simply economic and political; they can extend to societies views of the philosophical and sacred as well.

Kitiyadisai explains that it is difficult to align the liberal Western concept of privacy as an individual right with, inter alia, Buddhist values, because Buddhism perceives concepts of human rights and privacy rights as man-made rules that would "inevitably be in conflict within themselves as these are created to serve human avarice". Because those rules, "reflect the prevailing force in the society", they "would lead to further competition and aggressive posturing for protecting and furthering the interests among various groups".[134] In other words, aspects of certain cultures and societies may perceive human rights, including privacy and data protection, as tools that reflect and support existing power structures rather than challenging them.

In an African context, Olinger and Britz have claimed that "[p]rivacy as a notion does not function in African philosophical thinking" because it is at odds with the idea of *Ubuntu*.[135] *Ubuntu*, often translated as "I am because we are", is commonly described as a particular form of African humanism that prioritises communalism and interdependence over individualism and competition. As such, "[p]rivacy was glaringly absent as a cherished value or right within Ubuntu societies" because "[a]n individual right will only be accepted if it serves the community".[136]

While this criticism of the right to privacy seems to overlap with variations in some of the other regions identified above, it highlights a problem that is also faced by

privacy and data protection advocates everywhere: namely that it has always been "difficult to make the case for the social benefit of personal privacy."[137] However, given the potential for detriment that an increasing absence of privacy, caused by the widespread appropriation of personal data by new technologies and business models, may have not just on an individual but also on collective and societal interests, we would argue that now is the time to make that case. [138]

In addition, questions of various cultural conceptions of privacy are enmeshed in the philosophical realm. Throughout history, one can observe the *problematique* of our common humanity versus cultural difference. Similarly, one reaches as far back as the ancient philosophical problem of the One and the Many, found in many domains of application.[139] For difference (the Many) to be intelligible, we need a conception of commonality or identity. Just as the meaningfulness of the idea of the common (the One) is predicated on differentiation (the Many). This analogy applies equally to conceptions of privacy, as the private is intelligible only in the context of the concept of the public just as the public is meaningful only in relation to that which is private.[140] Strictly speaking, therefore, it is not possible for people to have a meaningful public, group life without having an individual private life.[141]

These worldview differences also exist within modern democracies, most prominently in those where Indigenous peoples live. These worldviews have informed the development of an international instrument, the *UN Declaration on the Rights of Indigenous Peoples*. The rights and worldview of diverse Indigenous peoples have come to the foreground in many parts of the world. So has the importance of respecting these rights, adjusting laws, and undertaking reconciliation in those nations where colonialism has had horrific and unjust impacts. This worldview encompasses new interpretations of both individual and group rights. Consequently, any new international instrument or domestic law, should consider and consult with Indigenous persons living there.

B. Individual v collective v societal harms

It has long been difficult to make a convincing case for an interpretation of the rights to privacy and data protection that includes a communitarian or societal perspective. This is largely because of the strong focus in Western liberal thinking on fundamental rights as individual rights, where an interference must always also result in verifiable detriment to the individual.[142] The concept of "harm" in privacy and data protection law is complex and contested. Some argue that to be actionable, impact must relate to some form of reputational or material harm, while others claim that the concept of harm must be directly related to a specific risk and the time at which that risk materialises.

So, for example, in the context of discussions about the mandatory retention of communications data for law enforcement purposes, authorities have often argued that the mere collection and retention of personal data do not represent any risk and that therefore no interference with the right to privacy and data protection exists until those data are actually accessed. At EU level, this argument was rejected by the CJEU in *Digital Rights Ireland* and subsequent jurisprudence,[143] but the argument itself prevails in many other contexts.[144]

The problem with this approach is that it relies solely on a concept of privacy harm that is both economic and individualized. Adopting this approach, harm will only arise if the data subject suffers verifiable (economic) damage or distress. However, developments in recent years have shown this conceptualization of privacy harm is insufficient. This is not just because of its economic bias but also because it ignores a whole range of risks and harms that are suffered not by the relevant data subject but by others – often those with whom the data subject shares certain characteristics – as well as by society as a whole.

By contrast, a human rights approach does consider non-economic harms, such as a harm to human dignity. Human rights statutes are also public law, and recognize that a harm to any on persons' rights is also a harm to the public good. When looking at the right to privacy and data protection as fundamental rights, we must therefore also consider those more "invisible" harms and the extent to which those harms affect not just individual but collective and societal interests.

Just as decisional autonomy is a key principle for the right to privacy, group interests rely on the idea of self-determination, now recognised as a core tenet of public international law. While first formulated as a political principle, during the era of decolonization, the internal aspects of self-determination have gained more importance recently. Shaw has described self-determination as "a people's pursuit of its political, economic, social and cultural development within the framework of an existing state."[145]

i. Invisible harms

The ability of public and private entities to collect vast amounts of personal data in a variety of contexts, to combine it with other data, and to analyse that data at speed has led to a situation where personal data circulates freely. Our information flows as through a set of "revolving doors", from public to private (and *vice versa)*, public to public and private to private bodies, with little regard for the purposes for which they were originally collected. Indeed, there is now increased pressure on public authorities to share administrative data they hold with the private sector to promote 'innovation'. The prevailing attitude inherent in many contemporary processing practices seems to be "if the data is already there, we should be able to use it".[146]

This approach not only clearly illustrates the existence of Ohm's "database of ruin," that is, the risk that data previously considered anonymous may be at risk of re-identification through their combination with other data, it also highlights the invisible privacy harms that can occur when the contextual integrity of personal information disclosure is breached.[147] As has been previously stated:

> *From the data subjects' perspective, it is now almost inevitable that sooner or later personal data they disclose to one entity will be shared across two or more public or private entities without their specific consent and often without their conscious knowledge. It thus becomes impossible for the data subject to appreciate, at the time of collection, how long their data will be stored, how it will be used in the future, for what purposes and by whom. Data subjects, when disclosing their data to anyone, are thus unable to make an informed*

decision about the risks involved in that disclosure and they are consequently prevented from taking reasonable precautions against those risks.[148]

This represents a shift in the balance of "information power" in favour of the already more powerful entity (usually the business or public body) that facilitates the commodification of individuals, enables discrimination, and "more fundamentally […] subordinates considerations of human wellbeing and human self-determination to the priorities and values of powerful actors."[149] As a result, we have been able to observe a loss of control by individuals over self-articulation.[150]

Similarly, current data processing practices increasingly ignore the principle of data minimization, which has long been a cornerstone of the CoE and EU data protection framework.[151] It provides that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected." However, all too often, the attitude of data controllers in both the public and the private sector is one of "all the data all the time."

In the commercial context, Shoshana Zuboff has described this process as "surveillance capitalism," which "unilaterally claims human experience as free raw material' that will then be 'translated into behavioural data' and used to 'fabricate prediction products."[152] This tailoring of the user experience to the user's known preferences arguably allows for a level of manipulation never before witnessed. At the more benign end, this may increase sales of a business to a customer or simplify the provision of public services.[153] However, it may also trap individuals in an

Profit-as-innovation: Google's 2012 data linkage policy

In the private sector, the increasing concentration of entire sectors to fewer and fewer players has also meant that those players gain much of their "data power" from the combination of different types of personal data, often collected by different parts of their business for different purposes. For example, in 2012, Google imposed a new privacy policy on users across all of its various businesses. It granted itself the right to combine user data from sources as distinct as its search business, its content businesses and its analytics business and to use those data for purposes never communicated to or anticipated by those users at the time of data collection.
Source: "Updating our privacy policies and terms of service", Google blog, 24 January 2012; Available at http://googleblog.blogspot.co.uk/2012/01/updating-our-privacy-policies-and-terms.html; last accessed on 18 October 2020.

environment where their existing biases are both reinforced and amplified, where they are no longer exposed to different goods, services, information, views or experiences, or where they are nudged towards viewpoints favoured by the state or other organizations in attempts to affect fundamental rights such as the right to vote, or the right to form opinions.[154]

ii. Collective and societal harms

In addition to the direct impact new data use practices might have on individuals, we must also consider the long-term effect they may have on collective and societal interests. Collective harms can arise when the processing of an individual's personal data affects others with whom the individual shares particular features or characteristics. This is generally the case where pattern analysis is performed on the personal data obtained from a sufficient and representative number of individuals, which allows for inferences to be drawn that will equally apply to other members of the same group even if their data were not available for direct analysis. For example, at a psychological/emotional level, psychometric tests may allow the identification of biases and vulnerabilities in certain types of people that can prove useful in "nudging" them and others with similar characteristics towards certain desirable or profitable behaviours.

At a physiological level, the result of DNA tests, often privately obtained by individuals for their reference, can be used in a research context to identify whether a person is likely to succumb to a particular disease. This information, in the hands of marketers, health professionals and insurance companies could then inform decisions on the sort of products and medications with which individuals with similar characteristics will be targeted, insurance premiums or even access to certain health services. Equally, personal data that individuals specifically disclose to obtain a financial or other material advantage, can then be used to create expectations on the part of the data user (in terms of desirable or acceptable behaviours) that is then imposed on others that have not consented to this kind of financial or convenience trade-off. In the data life cycle, this kind of data disclosure often starts out as a way to obtain a particular incentive, but quickly moves to becoming the generally adopted and unquestioned standard until it finally turns into a tool of exclusion.

Using all the data: Snowden and AI

One obvious example for this 'collect it all, use it all' approach is the law enforcement and national security context where Edward Snowden's revelations have highlighted the indiscriminate and bulk collection by US and UK security agencies of both content and traffic data travelling across, and generated by, electronic communications services. Further proof, should it be needed, can also be found in other areas like commerce and research. Most recently, the almost messianic promotion of AI technologies gives further support to the idea that nearly every commercial, administrative, financial, public policy, or public health problem could be solved (or solved more cheaply), if only we had access to enough data. Companies and governments alike have therefore begun to reassess the value of their databases not for facilitating existing relationships with their customers and citizens, but with a view to extracting maximum profit or utility from the data they hold on those customers and citizens.

Societal harms can arise when the processing of an individual's personal data contributes to data collections or facilitates data processing activities that either make the exercise of democratic rights and duties difficult or impossible, or because they enable the manipulation of individuals and groups in a way that is capable of shifting existing power relationships in society. The chilling effect of ubiquitous surveillance of communications is often cited as an example for the first possibility. Individuals, who know that their communications are intercepted or even capable of interception, will not use certain means of communications for particular purposes. In the German Democratic Republic (Communist East Germany), for example, there was an understanding that certain conversations were "not for the telephone". However, this change in behaviour can then also have wider implications for political participation, resistance and the general resilience of a body politic.

Health information, insurance and exclusion

In recent years, health insurers have increasingly encouraged their customers to upload fitness and nutritional data to their digital systems in exchange for points that could then be used to lower insurance premiums or receive cash back. One of the benefits of this approach is of course that it encourages responsible behaviour on the part of the insured that will not just save the insurer money in the end but will also benefit the individual, who should enjoy additional health benefits. However, there is a risk that rather than using the points system as an incentive, it will someday be used to calculate insurance premiums for all customers, leading to higher premiums for those that do not engage in activities judged to enhance their health. From there it is a quick hop and a skip to a situation where the latter may no longer be offered health insurance at all because they are deemed by insurers to be a bad risk. Insurers will have obtained the personal data that will allow them to make those, in their view purely commercial, decisions from only a subset of their customers. Nevertheless, the decisions themselves will ultimately affect all of them.

At the same time, the tools of surveillance capitalism outlined above (online tracking, profiling, targeting, prioritizing) may be used to target certain messages to the specific biases of each individual and, as such, may either encourage those individuals to act in a certain way or, indeed, not to act at all. Although it is still contested whether political micro targeting was actually successful in influencing people's behaviour – for example, with regard to their vote in the 2016 US presidential election or the UK Brexit referendum of the same year – it is clearly capable, in general, of amplifying some kinds of information while suppressing others.[155]

Real societal harms currently arise from the fact that we simply cannot yet fully ascertain the actual risk posed by those techniques and are therefore incapable of defending against it. In comparable contexts where the harm caused by a device, a process or a behaviour – were it to manifest itself – would be disastrous for society and/or societal values, this has traditionally led to calls for employing the "precautionary principle."[156] However, in the context of information, we are often faced with a situation where "[i]nformation businesses […] have begun to develop a new metaphoric frame that positions the networked information and communications environment as a de-politicised, self-regulating apparatus for truth production" when, in reality, it is neither and has instead "catalyzed tectonic shifts in relations of

accountability."[157] The development of an alternative and effective narrative is therefore dependent on emphasizing not just the *individual* but also the *public and collective value of privacy and data protection*.

C. The public and collective value of privacy and data protection

Pioneering privacy thinkers have always recognised that individuals' actions (or inaction) when controlling (or not) access to their data have the potential of affecting not just their own interests but also impact the rights of others and the public interest. As one of the first US scholars to address this question, Regan highlighted as early as 1995, that in a society that is increasingly reliant on technology "privacy is becoming less an attribute of individuals and records and more an attribute of social relationships and information systems or communication systems."[158]

She affirms that privacy, in addition to being an individual value, is also a public and collective value, and argues that the collective value of privacy is instrumental in underpinning democratic institutions and practices. These distinctions between privacy as a collective value, public value and a common value, take on very different meanings within her framework. Anticipating the more recent developments with regard to collective and societal harms caused by data processing activities based on individual consent, she argued even then that there is a risk that "[i]f one individual or a group of individuals waives privacy rights, the level of privacy for all individuals decreases because the value of privacy decreases."[159]

Even earlier, in 1987, Spiros Simitis, posited that "modern forms of data processing have altered privacy discussion in three principal ways."[160] One, they express conflicts affecting everyone, but do so in a way, which represents them as individual concerns. Two, they make it possible, using new technologies, to record and reconstruct individual activities in minute detail, thus normalising perpetual surveillance. Three, they are increasingly used to enforce standards of behaviour, thus granting additional power to those that are in a position to determine what those standards should be. All three of those developments solidified into the ubiquitous online behavioural tracking of individuals, the creation of detailed profiles about them and the use of those profiles to influence their beliefs and their commercial and political decisions.[161]

Referring back to the German Constitutional Court's 1984 *Census* decision, Simitis emphasises the extent to which privacy facilitates the exercise of other rights, including freedom of speech, freedom of association and freedom of assembly. As none of those rights "can be fully exercised as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed", he argues that a loss of privacy will always also constitute a loss of "democratic substance."[162] Privacy protection must become more than just the protection of any particular right. Rather the level of protection granted to individuals may "determine the choice between a democratic and an authoritarian society."[163]

The Court made a similar point in its decision.[164] In particular, the court noted that individuals who are unsure whether their behaviour is indeed observed by those with power over them might be significantly inhibited in their exercise of other rights that

are generally viewed as important rights of political participation (including, for example, their freedom of association or assembly).[165] This, the court argues, impacts not only the individuals themselves. On the contrary, informational self-determination is “an elementary prerequisite for the functioning of a free democratic society predicated on the freedom of action and participation of its members”. Unlike traditional views of liberty and self-determination, the court viewed those rights not as existing in isolation. Instead, individual liberty and the public interest (in the existence of a free society) are framed as equal targets of constitutional protection.

6. Relationship of privacy with other rights and values

The rights to privacy and data protection are not absolute rights. One of the fundamental human rights principles is that they are each all interrelated and interdependent. Incursions into and derogations from these rights are possible when necessary to reconcile privacy and data protection with other societal rights and interests. In its General Comment on Article 17 ICCPR, the UN's HRC provides that privacy must not be interfered with unless reasoned by law and only where essential in the interests of society.[166]

Article 8 ECHR similarly recognises that interferences with the right to respect for private life are permissible where the interference pursues a legitimate aim, is in accordance with the law and is proportionate, that is it does not go beyond what is necessary to achieve that aim. Such qualifying provisions ensure that the rights to data protection and privacy give way to other rights and interests where desirable, yet only to the extent necessary to achieve these rights and interests.[167]

To cite one example of these interactions, consider Article 27 of the UDHR which states that "everyone has the right freely …to share in scientific advancement and its benefits." It is not hard to imagine scenarios, given current research protocols, where if someone was forced to relinquish personal data in order to share in the scientific innovation of the digital age, this may be a contravention of article 27. Similarly, Article 29 states "in the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."

Which is all to say, even privacy as a fundamental right has to be framed in context. As already discussed, not only can privacy and data protection be reconciled with other rights and interests, in a variety of circumstances, respect for these rights is key, or, at least, will facilitate the attainment of other relevant rights and interests of individuals, such as freedom of expression. Another example is the right to freely form and hold an opinion under the UDHR (Article 19) where a clear linkage is made between privacy and the rights to autonomy and forming opinions.[168] These rights could therefore correctly be classified as both qualified rights and enabling rights.

A. Security

Public and national security is most often cited as a right that conflicts with the rights to privacy and data protection. This is particularly the case since the attacks of 11 September 2001 in the U.S., which sparked a host of new laws that granted law enforcement and security/intelligence services wide-ranging powers to collect and process citizen's personal data. Indeed, national security is one of the interests specifically listed in many human rights instruments as a ground to restrict qualified rights like privacy and data protection.[169]

As a result, human rights instruments and human rights courts have developed strong substantial and procedural safeguards to limit the interference by law

enforcement and security services to that which is necessary and proportionate. For example, the European Court of Human Rights in *Klass v Germany* insisted that any exception to the right to privacy, particularly where the measure in question facilitates the surveillance of citizens' communications, was to be narrowly interpreted. It held that, "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."[170] Moreover, in 2021 the CJEU determined in Case C-746/18 (Prokuratuur) that access to a set of traffic or location data for criminal investigative purposes, which provides precise conclusions concerning a person's private life, "is permitted only in order to combat serious crime or prevent serious threats to public security". [171]

B. Political Participation

Connected to the question of security is the threat that restrictions on privacy and data protection present for democratic institutions, as documented for example by the UN Special Rapporteur on rights to freedom of peaceful assembly and association.[172] Bennett and Raab have argued that, in the context of much of current public policy, privacy is viewed as an obstacle that must be overcome because it conflicts with public or community values like national security or, currently, public health.[173] However, this ignores the fact that privacy is itself a social or public value that supports other objectives of public administration. For example, good protections for voter privacy (e.g. secret ballots, mail-in and advanced polling, etc.) result in higher voter turnout and satisfaction with the process and thus promote the objective of political participation.[174]

In other areas, this also suggests that the convenience and efficiency that both public and private entities derive from the creation of large data stores (for example, centralized national health records) or methods of ubiquitous surveillance (like CCTV, facial recognition technologies or online behavioural tracking) must be balanced against the possibility of abuse. Effective technical and regulatory security features can prevent the "database state" from becoming the virtual equivalent of Jeremy Bentham's famous Panopticon prison model. This is because the "unequal gaze" that characterizes that kind of surveillance carries the risk of causing the internalisation of a disciplinary mind-set in those observed. While, on the one hand, this means that individuals living under that gaze are less likely to break rules or laws, on the other hand, they may be deterred from exercising their individual rights and freedoms or from generally participating in the democratic process. In the words of Bloustein, "privacy guards our individual wants against conformist pressure".[175]

Moreover, the unchecked use of personal data by public authorities is also likely to have other negative effects on society, including on social trust and social coherence. Lyon has argued that automated means of data processing can lead to a situation where "human beings are siphoned as data flows, to be reconstituted as 'data images' in the databases of the authorities".[176] What has become clear in recent years, is that if data users can use those data images for the purpose of risk profiling, such profiling has the potential to evolve into a form of "social categorising" which may privilege some citizens and disadvantage others by including them in "suspected categories" in advance of any crime committed by them.[177] In other

words, what begins as a problem of untargeted over-collection devolves into potential discrimination and mistreatment of specific individuals.

In addition, profiling systems also represent a risk "of reproducing and reinforcing social, economic and cultural divisions in informational societies". [178] Measures that undermine social trust also undermine, through their emphasis on individual behaviour, social solidarity.[179] In this context, Regan emphasises the importance of privacy in preventing fragmentation of the public realm by encouraging individuals to operate within it on the basis of their commonality rather than their differences.[180] Bennett and Raab further point out that social categorising may lead to privacy inequities where the "political public realm is harmed if restraint on arbitrary power can only be exercised by certain, perhaps privacy-privileged, persons or categories".[181] The existence of "privacy haves" and "have nots" may therefore be just as damaging to the social fabric of society as the privacy intrusions carried out by public and private institutions.

C. Public Health and other public interests

The issue of public health has been at the forefront of public consciousness in recent times. Many states have proposed data-informed responses to the Covid-19 pandemic, raising concerns, on the one hand, about the compatibility of such initiatives with fundamental rights, and, on the other, that fundamental rights protection might impede effective responses to the pandemic.[182] A primary example of a data-centric response to the pandemic has been the rollout of "contact tracing" applications in states across the world. These applications provide an excellent example of the qualified nature of the rights to privacy and data protection as well as the role respect for these rights plays in promoting public trust.[183]

Contact-tracing mobile applications

Contact-tracing applications detect when one mobile device is proximate to another one and log this encounter. This log of contacts can be maintained on the device or on a centralised server. If an individual has relevant symptoms, or tests positive for COVID-19, then this information can be input into the application. The risk of other contacts contracting the illness is then calculated, whether on the device or on a centralised server, and "at risk" contacts are notified. Applications based on both centralised and decentralised personal data processing entail an interference with the rights to privacy and data protection. However, provided that such interferences are in accordance with the law and relevant safeguards are put in place to minimise this interference, such applications are nevertheless deemed compatible with these rights. For instance, in England and Wales, the original application proposed by the National Healthcare Service (NHS) and supported by government was one which collected the details of proximate encounters on a centralised server where the risk of infection was also calculated before being communicated to affected individuals. This application attracted a lot of negative publicity as a result of the failure to articulate clearly the purposes of centralised data processing and who would have access to data as well as to comply with basic data protection safeguards such as storage limitation. Respect for these fundamental rights could bolster public trust in these applications, thereby improving their overall effectiveness as research suggests high take-up rates (of 60% of the population or more) are critical to their efficacy.

While the temptation might exist, therefore, to cast aside or limit the application of these rights in times of turmoil such as a pandemic, the existence of legal frameworks giving expression to these rights can prove beneficial. Indeed, the absence of regulation to protect these rights, or very limited regulation (for instance, only applying to public sector health providers), could leave the door open to a wide array of actors providing contact-tracing applications. In the context of contact-tracing applications, one reliable application that is human rights compliant is infinitely superior to a variety of competing applications of questionable quality.

D. Freedom of expression

The Internet is credited with disintermediating speech; whereas once mass communication was only available to privileged speakers, such as television and radio channels and the print press, now anybody with an Internet connected device has the capability to broadcast to the masses. The Internet also challenged traditional territorial borders, allowing individuals and groups to connect with new audiences and to discover new content. These developments are generally viewed as positive from a freedom of expression and information perspective. They have, however, brought freedom of expression and information into increasingly frequent tension with the rights to privacy and data protection, with the most prominent example of this being the application of the so-called “right to be forgotten”. Yet, what the application of the “right to be forgotten” illustrates is that, if neither freedom of expression and information, nor data protection and privacy are treated as absolute rights, they can be reconciled in a manner that respects the essence of all rights.

The 'Right to Be Forgotten'

The "right to delete" found in EU data protection law can be invoked by an individual against a search engine when their name is used as a search term in order to have certain links de-listed from the results returned. In the *Spain* CJEU judgment the Court indicated that such deletion, in that instance of information regarding an insolvency almost two decades earlier, could occur where the data processing was incompatible with data protection law. In practice, this finding required the Court to reconcile the data protection and privacy rights of the individual concerned with the freedom of expression and information of users of Google's search engine. In so doing, the Court held that, as a rule, the data protection and privacy rights of the individual would override the interest of the public in receiving this information, unless there is a preponderant interest of the public in receiving the information. The Court indicated given the sensitivity of the information for the individual concerned and that the events to which it pertained had occurred 16 years previously that the link should be delisted in some circumstances. Subsequent case law in the UK and Germany has recalibrated the "general rule", in order to balance more evenly the scales between data protection and privacy and freedom of expression. While this fine-tuning is inevitable, the qualified nature of the Court's findings has always allowed for such reconciliation. A number of important qualifications merit noting.

- While the judgment led to claims that "legal" materials were being delisted from search engines, the materials delisted are "illegal" as they are incompatible with data protection law. The right to delete does not give the individual a right to have any information they wish deleted. It is compatibility with the legal framework that is decisive, as opposed to the subjective preferences of the individuals or whether they were prejudiced by the information.

- The right does not require the personal data to be struck from the historical record. The Court distinguished between publication by the original website and the availability of the information on Google's search engine, which affects the fundamental rights to privacy and data protection "significantly and additionally", compared to website publishers. (*Google Spain*, para 38). This reasoning recognises that publication and distribution in different contexts can have qualitatively different impacts on the rights to data protection and privacy.

- The right does not apply when the individual data subject plays a part in public life, such as "senior public officials, business people and members of (regulated) professions". In practice, this means that delisting requests will 'systematically take into account the interest of the public in having access to the information. If the interest of the public overrides the rights of the data subject, de-listing will not be appropriate'. By recognising that not all information in which the public has an interest is of public interest, these rights can be reconciled in a way that respects the core tenets of all.

It is important also to recall the role of data protection and privacy in enabling the right to freedom of expression and information. Privacy is co-constitutive of free speech[184] and has been described by a former UN rapporteur on free speech "as a gateway for freedom of opinion and expression."[185] Richards explains this facilitating role eloquently when he argues for our "intellectual privacy"; a type of privacy required not just by intellectuals but also by all of us.[186] From a normative perspective, he argues that intellectual privacy is the bedrock of free speech. This recognises that freedom of thought and belief are needed for new ideas to develop

and for citizens to be able to “make up their own minds about ideas big and small, political and trivial.”[187] Privacy is a pre-condition for this kind of thought.

From a related empirical perspective, in the absence of privacy, when we are surveilled (by public or private actors) there is evidence to suggest that our freedom of thought and action is affected. Richards claims that “when we are watched while engaging in intellectual activities, broadly defined – thinking, reading, web-surfing, or private communication – we are deterred from engaging in thoughts or deeds that others might find relevant.”[188] We can therefore see that privacy protects key aspects of expression, ranging from initial opinion formation to the subsequent dissemination of that opinion. It creates the environmental conditions in which free speech can flourish.

Moreover, beyond the need for intellectual privacy, it is possible to envisage many circumstances where a denial of access to information may itself constitute a breach of the right to private life. One vivid example of this is the case taken against the Irish government by *Open Door and Dublin Well Woman*.[189] The applicants had been subject to an injunction restraining them from providing certain information to pregnant women by way of non-directive counselling about abortion facilities. The applicants argued that the denial to them of access to information concerning abortion abroad constituted an unjustifiable interference with their right to respect for private life in addition to a violation of their freedom to receive this information.[190]

The relationship between privacy and data protection and freedom of expression and information is multi-faceted. Where these rights conflict, each cedes ground to accommodate the other, as occurs with the right to be forgotten. In other circumstances, these rights are two sides of the same coin, complementing and supporting one another. For example, it is the experience of many marginalized groups that their right to free expression can often only be protected and exercised with a tangible right to privacy (e.g. LGBTQ2SI teens living with adults who are homophobic or transphobic, or women in domestic abuse situations).[191]

E. Equality and non-discrimination

Equality, non-discrimination, and privacy are intrinsically linked together in the modern era.

The right to privacy can enable groups of marginalized persons to seek common community without fear, to organize and protest, and to advocate for their equality rights.[192] It can also protect children from harm and aid their full and equal development. It can enable people with disabilities to receive accessible services and to be accommodated without being forced to over disclose personal medical information. It can assist women and LGBTQ2SI persons to find safety and acceptance, and to seek ways out of domestic violence or abuse. It can help protect them from online harassment and real world hate crimes.[193]

The right to privacy can also enable a more meaningful realization of other equality rights.

New uses of AI are of particular concern when used where people are vulnerable and may have little information or resources about how to assert their privacy or human rights. This is especially and alarmingly true for children[194], who are increasingly living their lives deeply affected by surveillance technology from the time of their birth[195]. In the midst of rapidly developing and critical discussions[196] at the UN,[197] regional,[198] and national[199] levels about governance, regulation, and guidance,[200] and the importance of human rights in these frameworks and debates[201] UN bodies[202], civil society organizations[203], human rights advocates[204], academic and research institutes[205], Privacy Commissioners[206] and National Human Rights Institutions[207] all have important roles to play in these debates about how to ensure human rights are fully protected and appropriately enhanced as technology advances.

Tackling Algorithmic Discrimination

In its *Closer to the Machine* report, the Office of the Victorian Information Commissioner provides several examples of algorithmic forms of discrimination in both public and private sector contexts including, for instance, Amazon's use of an experimental hiring tool which scanned and scored the résumés of job applicants, and was biased towards men as the AI had been trained using a dataset compromised of predominantly male résumés (p.29/30). The report (p.32) identifies a number of factors that act as barriers to understanding when algorithmic discrimination has occurred. These include that:

- The affected individual may not realise that the decision had been made by an AI system;
- The user of the AI system may not be obliged to provide an explanation, particularly in a commercial setting;
- The designer of the AI system may resist disclosing its reasoning process in order to maintain commercial and competitive advantages and secrecy; and
- The AI system's audit trail may not identify which factors are deemed particularly relevant to the decision or recommendation made by the AI system.

The EU's GDPR provides for a right to explanation, which includes an obligation to provide the individual with information regarding the "existence of automated decision-making, including profiling" and "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". This obligation applies both when personal data are first obtained or within a reasonable period thereafter (Article 13(2)(f) and 14(2)(g) GDPR) and once personal data processing is underway (Article 15(1)(h) GDPR). In a similar vein, the modernised Convention 108 gives individuals a right to obtain, on request, "knowledge of the reasoning underlying data processing where the results are applied to the data subject" (Article 9(1)(c)). Data protection law therefore helps overcome the barriers to understanding algorithmic discrimination and to uncover discriminatory practices.

It may also be useful to note that operationally, in many states, although an international instrument or a domestic constitution with equality provisions may bind the State's actions, they may not provide accountability or remedy from actions of private companies. Domestic human rights codes which are quasi-constitutional in nature, are an important additional legislative protection. They can promote equality and privacy rights, and they can hold both the public and the private sector equally to account for discrimination. For many states, National Human Rights Institutions such as human rights commissions, exist side by side with national or regional privacy

commission offices, and can support and complement each other's work in both equality and privacy areas.

Another type of relationship between data protection and privacy and the right to equality centres primarily on the role of data protection and privacy in concealing or revealing discriminatory practices. The rules around the processing of sensitive personal information are sometimes said to hinder efforts to gather data for the purposes of assessing and mitigating discrimination.[208] For instance, Binns and Veale suggest that many of the methods to tackle discrimination in algorithmic systems implicitly assume that organisations hold these sensitive data while they may not in order to ensure compliance with the data protection framework.[209]

However, more frequently the rights to privacy and data protection act to support efforts to combat discrimination. Indeed, some of the first international documents on data protection and privacy – two Resolutions of the Council of Europe on the protection of privacy in electronic data banks – set out safeguards to apply "especially when electronic data banks processing information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination".[210] Moreover, many modern data protection frameworks contain a general principle of "fair" personal data processing, which is understood to mean "non-discriminatory" amongst other things.[211] For example, the Brazilian "Marco Civil da Internet" lists amongst the general principles for personal data processing "non-discrimination" rather than fairness, indicating that the Brazilian legislature considered that non-discrimination was the critical element of fairness to be protected.[212] Similarly, the French Data Protection Authority in a recent report on Algorithms and AI has concluded that "a *fair algorithm* should not end up generating, replicating or aggravating any form of *discrimination*."[213]

7. Next steps: Options for the development of the rights to privacy and data protection

In light of both the inherent and the instrumental value of the rights to data protection and privacy for individuals and society, the effort to strengthen their recognition and application is justified. Despite the clear links between data protection and privacy and other rights, as outlined above, we have yet to secure optimal protection of either. While many factors contribute to this lack of effective remedy, two are worth emphasising.

First, as alluded to above, despite the proliferation of data protection regimes worldwide,[214] there are widening distinctions between privacy and data protection frameworks. On the one hand, there are regimes that are underpinned by fundamental rights and secure rights for individuals and society. Conversely, there are those that are more market-oriented and seek primarily to secure data liberalisation interests. Both models have powerful proponents. However, from the standpoint of individual recourse, the more countries that shift towards the fundamental rights model, and interpret their regulatory frameworks in a way that promotes rights protection, the more effective this protection will be.

Second, for those countries that do endorse a fundamental rights approach to personal data protection, it is important that the law is effectively implemented in local legislation, and subsequently applied, and enforced. This includes establishing an independent authority to supervise data protection enforcement and ensuring that the work of that authority is facilitated through adequate resources and freedom from external interference. This public-led regulation should be bolstered through procedures for private recourse as well, one that recognises and facilitates individual actions for damages as well as representative actions to address collective and systemic data protection failings.

Presently, at both domestic and international levels, existing data protection and privacy instruments are inadequately enforced. The failure to address these challenges will void data protection law of any real substance, turning what should be an effective mechanism to protect rights and enhance trust and accountability in the digital era into a tick-box exercise that legitimises rather than challenges data misuse and abuse.

In light of the importance of securing effective data protection and privacy, the question then becomes how such effective rights protection should be ensured. The primary choice here is whether to advocate for new legal instruments that explicitly recognise the fundamental rights dimension of data protection and privacy, or to advocate for the strengthening and enhancement of existing domestic and international legal protections.

Over the past decades, many European States have introduced constitutional protection for data protection within their domestic legal orders. Most recently, for instance, in Luxembourg a constitutional reform project envisages the inclusion of a right to “informational self-determination” in the Constitution (in addition to the existing right to privacy found in Article 11(3)). The EU Charter right to data protection and the German jurisprudence on informational self-determination

explicitly inspires this proposal.[215] While this approach offers the benefit of a firm legal footing for the rights to data protection and privacy, it also risks being cumbersome in states where Constitutional reform requires significant procedural steps (such as approval by referendum). Treaty change at the international level can be even more protracted. It is for this reason that the second approach – the strengthening of existing domestic and international legal protection – is preferable. Not only is this approach more realistic to achieve in practice, it is also more respectful of the divergent constitutional and cultural contexts of states.

A. Maximising the Potential of Existing Protection at Domestic Level

The immediate, and therefore pragmatic, approach to secure widespread recognition of the rights-based nature of data protection law is to advocate for the explicit recognition of the rights to data protection and privacy in domestic constitutional statutes and frameworks, as applicable. Domestic constitutional and supreme courts tend to have the capacity to draw on existing constitutional provisions in order to recognise these rights. As discussed above, this is the path followed by the German Constitutional Court in developing a right to informational self-determination based on existing rights to human dignity and self-determination in the German Basic Law.

This was also the approach taken by the Supreme Court of India in its *Puttaswamy* judgment in 2017. In this judgment, the Supreme Court unanimously concluded that the right to privacy is a constitutionally protected right in India although it is not explicitly provided for in the Indian Constitution. The nine-judge bench delivered six distinct opinions, each of which differed subtly in terms of reasoning. However, what they shared was the view that privacy could not be disconnected from other existing constitutional rights, such as liberty, dignity and freedom of expression. As the judgment states:

> Privacy has not been couched as an independent fundamental right. But that does not detract from the constitutional protection afforded to it, once the true nature of privacy and its relationship with those fundamental rights which are expressly protected is understood. Privacy lies across the spectrum of protected freedoms.[216]

This reasoning offers a promising example for the development of privacy and data protection rights in other jurisdictions. What is also pertinent about the leading judgment (of DY Chandrachud J) is that in addition to its detailed engagement with domestic privacy jurisprudence and constitutional rights, it also examined and drew inspiration from many other jurisdictions including the European Court of Human Rights and the Inter-American Court of Human Rights as well as leading privacy scholarship. Such cross-fertilisation of jurisprudential developments and ideas could also be useful in facilitating the recognition of these rights in other jurisdictions.

The advantage of this approach is that, if permitted under the domestic legal system, it would not require any radical constitutional or other legal reform. In order to assess the viability of privacy promulgation in this way, a starting point could be to examine the existing constitutional framework and jurisprudence and to identify common elements that could be relied upon to support a right to privacy, as well as the courts´

powers to interpret and recognize fundamental rights. Where this seems plausible, the data protection and privacy community (regulators; international organisations, such as the Council of Europe; academics and other stakeholders) could work with local organisations to provide expertise and engage in capacity and awareness building on data protection and privacy issues.

B. Encouraging Convergence around Existing International Rights-Based Instruments

Rather than attempting to reach consensus around a new international data protection instrument, securing convergence around an existing international rights-based instrument may be preferable. In considering which instrument would be best, there are three candidates for consideration.

A first option might be to encourage further convergence on data protection and privacy principles under the auspices of the existing privacy provision in the ICCPR. In particular, the objective would be to encourage compliance and enforcement with the ICCPR right and ensure its interpretation and application are fit for a digital age. For instance, the UN HRC could adopt a new, updated "General Comment" on Article 17 ICCPR, recognising the collective interests served by the right to privacy and modernising its interpretation of Article 17.

However, given that existing UN approaches in this area have not been successful, this approach is risky. In particular, the UN's broad membership includes states that are strongly committed to economic-based approaches to data protection as well as rights-based approaches. There is a risk that these mixed perspectives on the appropriate role of data protection in a digital environment would ultimately weaken any protection offered through the UN.

A second option would be to encourage convergence around the EU's GDPR as an international standard. The substantive provisions of the GDPR for personal data processing are myriad and carefully detailed, as they were drafted with the understanding that personal data processing has ramifications for fundamental rights and must therefore be subject to robust safeguards. Moreover, many states worldwide are already cognisant of these standards. In some states, the GDPR has been explicitly or implicitly taken into account when drafting domestic legislation in a bid to secure an "adequacy" finding necessary to ensure cross-border data flows between EU and non-EU States.[217]

Nevertheless, the option of convergence around the GDPR standard may not be the most desirable for a number of reasons. Most importantly, given that the GDPR is touted as a "gold-standard" for data protection and is designed to ensure further European integration through strict and prescriptive provisions, it may be beyond immediate reach as a legal standard for many states. Moreover, at present the only non-EU signatories to the GDPR are from European Economic Area states (Iceland, Liechtenstein and Norway). There is no other mechanism currently envisaged for non-EU and EEA States to sign up to GDPR standards officially.

The third, and perhaps most viable, option is therefore to encourage convergence around the Council of Europe's Convention 108+. Convention 108+ "modernises" the original Convention 108 through an amending Protocol (CETS No 223). The merits of supporting further international convergence through Convention 108+ are as follows.

First, while Convention 108+ will not enter into force until 2023 at the earliest, non-European State signatories can already request accession to this instrument.[218] Although details of the "Evaluation and Follow-up Mechanism" envisaged by Convention 108+ have not yet been finalised, requests for accession to the Convention will initially be assessed by the "Convention Committee" which will evaluate the effectiveness of the measures the requesting State (or international organisation) has taken to give effect to the Convention's provisions.[219] Following this assessment, the Convention Committee then adopts a positive or negative opinion of the requesting state's eligibility for accession that is sent to the Committee of Ministers of the Council of Europe.[220] At present, eight non-Member States of the Council of Europe have ratified Convention 108, while three have signed and one ratified Convention 108+.[221] Non-European States also currently act as observers in Convention 108's "Consultative Committee" (which will be replaced by the Convention Committee).[222]

A major advantage of Convention 108+ is that it is already designed to be an international, multilateral data protection standard and has the relevant procedures in place for accession.[223] Indeed, the Council of Europe has stated that it remains committed to assist parties in

> *a speedy accession to the Protocol (CETS No 223) by the maximum number of the current States Parties to Convention No. 108 in order to facilitate the formation of an all-encompassing legal regime of data protection under the modernised Convention, as well as to ensure the fullest possible representation of States within the Convention Committee*.[224]

The Council of Europe already has a model in encouraging adoption of its Conventions beyond European borders and ensuring they become truly global in nature. For instance, 21 non-European parties have ratified the Cybercrime Convention.[225]

Second, the standards set out in Convention 108+ are stricter than those found in Convention 108, thereby ensuring the instrument is in line with the most recent generation of data protection laws. However, these standards are not as prescriptive as those found in the EU's GDPR thereby offering a potential "happy medium" and often an important margin of appreciation for many countries. As Greenleaf notes, amongst the advantages that Convention 108+ accession offers for States is "best practice recognition", that is recognition that "a country's data protection standards have achieved 'international best practice', in the opinion of an increasingly global group of the country's peers."[226] Moreover, for States that wish to go further than the standards set out in Convention 108+ this is not precluded (see Article 13 of Convention 108+). Convention 108+ could therefore be seen as an "off-the-shelf" global data protection standard pitched at the right level for widespread accession.

A third advantage of encouraging convergence around Convention 108+ as a global data protection standard, underpinned by fundamental rights, is that such encouragement is already present. The European Commission has encouraged for instance accession by non-European countries to Convention 108+ as "the only binding multilateral instrument in the area of data protection" and "promoted the swift adoption of the modernised text with a view to the EU becoming a Party".[227] Equally, the UN Special Rapporteur on the Right to Privacy has suggested that member states be encouraged to ratify Convention 108+ as "an interim minimum response to agreeing to detailed privacy rules harmonised at global level".[228]

This is not to suggest that accession to Convention 108+ should be viewed as a panacea for privacy and data protection. It presents two key challenges. The first challenge relates to substantive standards. As Greenleaf notes, for many countries some of the pre-requisites for accession (in particular, being recognised as a state and being a democratic state) are unlikely to be fulfilled anytime soon.[229] Accession for these states is therefore an unrealistic near-term prospect. Other conditions for accession include the presence of an independent oversight authority and rules encompassing public sector as well as private sector data processing. While feasible for other states, they would require legal and cultural change. Finally, it is not clear that existing regulators (e.g. national human rights institutions), rights-holders or civil society advocates more broadly favour this specific approach. Open governmental consultation with these groups and bodies should therefore occur in advance of major reforms.

Greenleaf identifies a number of ways in which accession could be facilitated for those with the will to do so. These include:

- The publication of a policy document by the Consultative Committee which emphasised the most important elements of the accession evaluation;[230]
- The need for the 108+ Convention Committee (which will eventually be replaced by the Consultative Committee) and the Committee of Ministers to be flexible when it comes to the application of the Convention's accession standard;[231]
- The appraisal of accession prospects by "independent or 'unofficial' analysts such as academics" to ensure that viable accession requests are prioritised and that there is an "adequate basis for public debate on the future prospects of such international agreements."[232]

Keeping these recommendations in mind, it is evident that while all States cannot achieve Convention 108+ standards at present, there are ways in which such accession can be facilitated and streamlined which the Council of Europe is ready to support.

A second challenge relates to the enforcement of Convention 108+ standards. Currently, the existing regime can only hold signatories of the ECHR liable for non-compliance. However, a straightforward, although non-conventional mechanism is to be established based on article 17 of Convention 108+. This new procedure could represent a powerful instrument in enforcing individual cases even in trans-border contexts and would be based on an obligation for supervisory authorities to cooperate with each other, in particular by a) providing mutual assistance by

exchanging relevant and useful information and co-operating with each other (…) and by b) co-ordinating their investigations or interventions, or conducting joint actions. If a state Party however would be found to be in violation of the modernised Convention, Article 4, paragraph 3 of Convention 108+ should give enough basis to the Convention Committee to a) evaluate the situation, b) recommend measures to take to reach compliance with the provisions of the Convention and to c) apply sanctions based on the provision of the Convention itself (such as in paragraph 1 of article 14) or based on Vienna Convention on the Law of Treaties. Those measures could surely contribute to - or result in – consistent national compliance with the Convention. However, they are still to be developed and put in place for all existing and future Parties, which could represent some challenge.

In the meantime, other Parties and the Convention bodies (the Consultative Committee, the Secretariat and the Council of Ministers) could try to enforce compliance through diplomatic means, this is a non-binding mechanism. There are however a number of alternative possibilities here. Most evidently, the 1st Optional Protocol to the ICCPR has been ratified by 115 UN Member States. It allows individuals who claim that a signatory of the Protocol has violated their ICCPR rights and who have exhausted all available domestic remedies to submit a "communication" to the Committee for consideration.[233] The HRC can then issue non-binding recommendations to the State concerned.

Another option might be to consider the possibility of enforcing the provisions of Convention 108+ through regional human rights frameworks, such as the Inter-American human rights system or by the African Court on Human and Peoples' Rights. Existing data protection networks (such as APPA, GPEN, AFAPDP and the GPA) could also more actively engage with existing UN mechanisms (such as the High Commission for Human Rights, the Special Rapporteur for the right to privacy, and various committees) already involved in analysing and promoting the right to privacy in the digital age.[234]

C. Conclusion

The evidence, trends, case law and findings reviewed and reported upon – both in the body of this report and its accompanying jurisdictional review – lead our GPA working group to the conclusions enumerated below. Some of these may appear self-evident (even axiomatic) for those working in the data regulation or rights protection fields, as they are phenomena that have been unfolding for over two decades. We restate them emphatically below to better direct future deliberations and actions to improve the status of privacy rights globally.

1. **Without clear and rigorous protection and effective enforcement of privacy and data protection rights, other civil and political rights of citizens worldwide are imperilled.** Freedom of belief, freedom of movement, right to free association and peaceful dissent all hinge upon substantive privacy and data protection protections, as do human dignity and equality. Each comes under constant pressure from state and commercial actors. A world where individuals find the gaze of government and corporate surveillance unavoidable cannot be described as open, free or fair.
2. **Any proposed solutions or reforms to the current problems must be workable across national borders and apply to all sectors of distinct economies.** Silo approaches to regulation (as in efforts to bring tax fairness, environmental protections or improve public health) only create further gaps, inequities, blind-spots and exceptions. The rights people enjoy offline should apply equally to their digital selves, and the rights of privacy people expect their governments to respect should be equally observed by commercial entities. Free enterprise does not mean free-for-all and *laissez-faire* should not mean companies get to decide what is fair. The last decades have also shown the flaws and limitation of industry self-regulation and the need for binding protection and remedies for rights to be applied.
3. **Protections afforded by local constitutions and laws, bilateral agreements, or international conventions and covenants need actual, effective real-world analysis, support, promotion, education and enforcement.** Human rights, untethered from reality, which allow no meaningful redress or where remedy is too complex and expensive to seek, are empty promises. For truly effective accountability to occur, oversight bodies must be adequately resourced, political independent, appropriately staffed and able to cooperate locally and domestically with rights-holders and their advocates, and globally with peers, NHRIs, state bodies, regional and international organizations and UN mechanisms. These principles apply equally to regulation of government and commerce, as well as to existing multilateral instruments promulgated by the OECD, EU, Council of Europe and APEC. Without meaningful, proactive enforcement, revised rule-sets, re-issued standards and new protocols will be neither observed nor credible.
4. **Privacy and data protection breaches and violations encompass harms well beyond loss of personal data.** Industry attempts to limit discussions on treatment of information and systems safeguards gravely minimize the damages accruing to individuals and communities. Personal autonomy, basic personal dignity, freedom of conscience and the inalienable right of individual self-determination (meaningful

choice) are actively eroded by poor data practices, uneven enforcement, legal exceptionalism, regulatory capture or constant delay of reform efforts.

5. **Governments need to be reminded of privacy and data protection and their centrality to the underpinnings of democracy.** Privacy and data protection are not a social nicety, urbane novelty, or quaint observation of polite society. On the contrary, they are a bedrock of electoral fairness (e.g. the secret ballot), private communications (e.g. warrant requirements), and due process (e.g. right to access, review and seek correction of government information holdings).
6. **Lawmakers, elected officials, members of the judiciary and appointed regulators all have a role in the reform and reinforcement of rights-protecting institutions.** Fundamental rights are not freedoms we outsource or defer to markets and their orientations. That means maximizing the effects of local enforcement (e.g. stronger arbiters and better access to redress) while directing international cooperation to be a serious priority for government agencies (e.g. broadening OECD, Convention 108+ and GDPR efforts).

Strengthening data protection, privacy, and human rights in tandem will require both a sustained commitment of tangible means, as well as clarity about our intended ends. As noted throughout this report, all indicators show that privacy, human dignity, essential liberty and free expression will otherwise continue to erode without immediate coordination. The alternative – continued fragmentation of reform efforts, localized and sporadic efforts at regulation, and uneven, protracted forays into online enforcement – only reinforce the status quo of self-regulation both in commercial and governmental sectors.

To be clear, the options presented in this report are not mutually exclusive but complementary. For example, while prioritizing instruments like Convention 108 and 108+ presents an expedient avenue for improvement, calls for other international actions (e.g. at the United Nations level) should continue as well. It is possible to imagine dual pathways to further enhance and secure the recognition and protection of the rights to privacy and data protection. One path draws upon existing constitutional provisions, including rights to autonomy, liberty, personality and dignity, to recognise a right to privacy and data protection in the domestic legal order of a state. In the absence of explicit privacy or data protection provisions, a number of states, including Germany and India, have taken this avenue already. The resulting impact has been powerful.

A second, potentially cumulative, path is to encourage convergence around an existing global rights-based instrument. The prime candidate here is Convention 108+. This Convention has been updated to align with the most recent generation of data protection laws; in substance, it is a robust, rights-based instrument yet its provisions are not prescriptive, leaving some margin for manoeuvre in different legal and cultural contexts; and, there is a clear process for accession by non-Council of Europe States.

By following this approach, and maximising the potential of existing legal instruments for privacy protection, a more effective, rights-based approach remains within reach.

Annex: Autonomy bound – self-interest, economic dependence, social relationships and obligations

1. Existential self-interest

Existential self-interest constraints arguably represent the strongest limits to our individual autonomy. We will often willingly consent to the use of our data, where this is a precondition for receiving specific medical treatments or where ongoing data collection is part of the way an innovative medical device, say, a cochlear implant or a pace-maker works. Withholding consent to the processing of our data, where doing so would actually endanger our health or even life, or the health or the life of others, may seem, at first look, self-defeating and thus not be viewed by the individual as much of a constraint at all. However, this assumes that the effective deployment of individual or public health measures is in fact conditional on the processing of identifiable personal data and cannot be achieved in another way.

While this may be true in some cases, in others it may be perfectly sufficient to collect data in anonymised form. Consequently, an effective right to data protection would protect individual autonomy by placing the onus on innovators to develop new technologies in compliance with established data protection principles like data minimisation, purpose limitation and storage limitation.

2. Economic constraints

Economic constraints that influence our choices mostly derive from our relative bargaining power when interacting with other commercial actors. In this context, our own relative power is determined, among other things by our wealth, knowledge, skill, and ability. In practice, this includes the things we cannot do, do not know how to do or cannot afford to do.

Economic constraints can often be observed in contexts, where an individual is in a situation of economic dependency or subordination or where they are willing to make privacy trade-offs in exchange for goods or services. The relationship between an employee and their employer or between a benefits recipient and the public authority providing those benefits are examples for the former context, where it will be almost impossible for the individual to refuse a request for the disclosure of their personal data without running the risk of incurring considerable financial detriment. The trade-offs between providers and users of “free” social media services fall into the second category. Users have become accustomed to “paying with their data” not just because they enjoy receiving services without the need to provide monetary compensation but also because a significant number of users would not be able to afford to use all of those services, were they provided on a cost basis. The use of data as a form of payment thus conceals a more fundamental concern that arises from our data and ad-funded digital economy, namely the fact that monetary compensation would bring the economic inequality, which arguably is a feature not a bug of the prevailing capitalist political economy, into sharp relief.

Economic constraints can further be observed in other contexts, particularly where an individual is in a situation of economic dependency or subordination. This includes, most notably, the relationship between employer and employee, but it can

also be apparent in other relationships. For example, in our technology and data-based world, individuals that are financially reliant on state benefits – the low-paid, unemployed, and people living with a disability – are often required to provide an exceptionally large amount of personal data about their personal circumstances, education, health etc. before a decision about the payment of such benefits is made.

Individuals will inevitably part with their data in those circumstances, given that a refusal to share is literally likely to see them penniless. The things we can buy with money include those that fulfil the most fundamental needs in Maslow's hierarchy of needs, such as food and shelter. In the mind of the average individual, such physiological and safety needs are always likely to outweigh higher-level needs like self-actualisation, including the ability to exercise control over our personal data. However, to argue that the individual exercises their autonomy in those circumstances would likely ignore completely the power imbalance as well the sheer economic need that will influence individuals' decision in those circumstances. Instead, pre-existing political and economic power imbalances are likely to serve as an efficient constraint on the exercise of individual autonomy in the data economy.

As before, the right to data protection may help to address these imbalances and restore a sense of true autonomy to the individual by imposing restrictions on particular data uses proposed by specific controllers. While any such restriction would inevitably also limit – on the face of it – the individual's autonomy to make a bad bargain, in some cases a constraint on autonomy may be required precisely to preserve autonomy.

3. Social/collective constraints

Finally, our individual decisions are also influenced by social and collective constraint, namely the things we will do or not do to fulfil our social obligations. A highly current example for this kind of constraint is our willingness to allow our data to be used in the public interest, for example in response to appeals for "data donation" for public health purposes.

While existential self-interest plays a role in persuading an individual to participate in such public health measures, there are also increasing "social" pressure on individuals to participate. This acts as a further constraint on individuals' autonomy when deciding whether or not disclose their data for those purposes. Social and collective restraints make it difficult for people to refuse their consent, and thus truly exercise autonomy, even if they are concerned about a lack of trust or the possibility that their data, once shared, might subsequently be used for unrelated purposes.

Data protection law that is rooted in the notion of individual autonomy might be able to address some of those concerns through restraints on non-essential data uses and the requirement for effective safeguards. As before, transparency, data minimisation, purpose limitation and a limit on the length of time for which data may be stored could help instil the trust individuals require to participate in altruistic or social value data processing schemes without fear of courting future harms for themselves by doing so.

At the same time, the tension between individual and collective interests in this particular scenario also highlights the fact that it may be time to rethink the individualism that has traditionally informed the concept of fundamental rights in Western liberal democracies. As the German Constitutional Court pointed out in its Census decision, individuals' actions (or inactions) have the potential to affect not just themselves but the rights and interests of others and of the community of which they are a member. That being so, we should also consider whether the rights to privacy/data protection should be viewed as a purely individual or as collective or communitarian rights.

Bibliography / sources cited

Articles

Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 1000

Bradford et al, "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes" (2020)7 *Journal of Law and the Biosciences* (pending publication)

Brandeis, L. D. and S. D. Warren, "The Right to Privacy" *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. - http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Crawford and Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 *Boston College Law Review* 93

de Hert and Papakonstantinou, 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency' (2013) 9 *Journal of Law and Policy* 271

de Schutter and Ringelheim, 'Ethnic Profiling: A Rising Challenge for European Human Rights Law' (2008)71 *Modern Law Review* 358

Diggelmann and Cleis, 'How the Right to Privacy became a Human Right' (2014) 14 *Human Rights Law Review* 441

Ess, 'Lost in Translation?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia)' (2005) 7 *Ethics and Information Technology* 1.

Fried, 'Privacy' (1968) 77(3) *Yale Law Journal* 475

Greenleaf, 'Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside Europe" (2016) *UNSWLRS* 52

Greenleaf, 'How far can Convention 108+ 'globalise'? Prospects for Asian accessions' (2020) *Computer Law & Security Review* (pending publication)

Hoofnagle, van der Sloot & Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28 *Information & Communications Technology Law* 65

Keats Citron and Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1

Kitiyadisai, 'Privacy rights and protection: foreign values in the modern Thai context' (2005)7 *Ethics and Information technology* 17

Kuner, ‘An International Legal Framework for Data Protection: Issues and Prospects’ (2009)25 *Computer Law and Security Review* 307

Lynskey, ‘Deconstructing Data Protection: The ‘Added-Value’ of a Right to Data Protection in the EU Legal Order’ (2014) *International & Comparative Law Quarterly* 569

Madison, *Federalist Papers, No. 51* (1788) - https://billofrightsinstitute.org/primary-sources/federalist-no-51

McStay, “Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy”, January 2020, *Big Data & Society* 1

Newman, ‘The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google’ (2014)40(2) *William Mitchell Law Review* 849

Ohm, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization’ (2010) 57 *UCLA Law Review* 1701

Olinger, Britz, and Olivier ‘Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa’ (2007)39 *The International Information & Library Review* 31

Petkova, ‘Privacy as Europe’s First Amendment’ (2019) 25 *European Law Journal* 140

Post, ‘Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere’ (2018) 67 *Duke Law Journal* 980

Prins, ‘When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter’ (2006) 3 *SCRIPTed* 270.

Prosser, ‘Privacy’ (1960) *California Law Review* 48

Rengel, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) *Groningen Journal of International Law* 33

Richards, ‘The Dangers of Surveillance’ (2013) 126 *Harvard Law Review* 1934

Simitis, ‘Die informationelle Selbstbestimmung—Grundbedingung einer verfassungskonformen Informationsordnung’ (1984) *Neue Juristische Wochenschrift* 394

Simitis, ‘Reviewing Privacy in an Information Society’ (1987)135 *University of Pennsylvania Law Review* 709

Spina, ‘Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?’ (2014) 2 *European Journal of Risk Regulation* 248

Veale and Binns, ‘Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data’ (2017) 4 *Big Data & Society* 1

Veil, ‘The GDPR: The Emperor’s New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law’ (2018). Available at: https://ssrn.com/abstract=3305056

Yilma, ‘The United Nations data privacy system and its limits’ (2019) 33 *International Review of Law, Computers & Technology* 224

Warren and LD Brandeis, ‘The right to privacy’ (1890), 4 *Harvard Law Review* 193

Books

Acemoglu and Robinson, *The Narrow Corridor: states, societies and the fate of liberty* (Penguin Random House, 2019)

Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (University Press of Kansas, 2007)

Bennett and Raab, *The Governance of Privacy* (2nd ed, MIT Press, 2006)

Cohen, J. E. *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019)

Cohen, S. A. *Invasion of Privacy: Police and Electronic Surveillance* (Carswell, 1983)

Cooley, *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract,* (2nd ed, Chicago, Callaghan & Company, 1880)

Donohue, *The future of foreign intelligence: privacy and surveillance in the digital age* (Oxford University Press, 2016)

Emerson, *The system of freedom of expression* (Random House Trade, 1970)

Foucault, *Discipline & Punish: The Birth of the Prison* (Vintage, 1995 edition, 1975)

Gonzalez-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2004)

Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016)

Kant, *Groundwork for the Metaphysics of Morals* (Abbott Thomas K. tr, 2005)

Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2011)

Landau, *Surveillance or security? The risks posed by new wiretapping technologies* (MIT Press, 2010)

Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015)

Lyon, *Surveillance after September 11* (Polity Press, 2003)

Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994)

Mayer-Schönberger and Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2018)

McStay, *Emotional AI* (Sage, 2018)

Raz, *The Morality of Freedom* (Oxford University Press, 1986)

Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995)

Schoeman, *Privacy and Social Freedom* (Cambridge University Press, 1992)

Shattuck, *Rights of Privacy* (American Civil Liberties Union, 1977)

Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004)

Solove, *Understanding Privacy* (Harvard University Press, 2008)

Westin, *Privacy and Freedom* (Atheneum, 1967)

Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)

Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International, 2015)

Book Chapters

Andrade, ‘Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights’ in Fischer-Hübner et al (eds), *Privacy and Identity Management for Life* (Springer, 2010)

Dalla Corte, ‘A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection’ in Hallinan et al (eds), *Data Protection and Privacy: Data Protection and Democracy* (Hart, 2020)

de Hert and Gutwirth, ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action’ in Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009)

de Hert and Gutwirth, ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’ in Claes et al (eds), *Privacy and the criminal law* (Intersentia, 2006)

Larsen, Boulanger and Vandendriessche, ‘Luxembourg’ in *The New EU Data Protection Regime: Setting Global Standards for the Rights to Personal Data Protection* (The Hague, 2020)

Oguru, “Electronic government and surveillance-oriented societies” in D. Lyon (ed.), *Theorizing Surveillance: the Panopicton and Beyond* (Routledge, 2006)

Rauhofer, ‘Round and round the garden?: Big data, small government and the balance of power in the information age’ in Schweighofer et al (eds), *Transparenz* (Oesterreichische Computer Gesellschaft, 2014)

Rouvroy and Poullet, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’ in Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009)

W Webster, “Public administration as surveillance” in Ball, Haggerty and Lyon (eds.), *Routledge Handbook of Surveillance Studies* (Routledge, 2012)

Jurisprudence

Amann v. *Switzerland* App No. 27798/95, (ECHR, 16 February 2000)

Big Brother Watch and ors v United Kingdom Applications nos. 58170/13, 62322/14 and 24960/15, (ECHR, 4 February 2019)

Botta v. Italy App. No. 21439/93, (ECHR, 24 February 1998)

Burghartz v. Switzerland App No. 16213/90, (ECHR, 22 February 1994)

Campbell v Mirror News Group (MGN) [2004] UKHL 22

Carpenter v United States 138 S. Ct. 2206 (2018)

Copland v. *United Kingdom* App No.62617/00, (ECHR, 3 July 2007)

Digital Rights Ireland Ltd v Minister Commc’n Marine and Nat. Res. And Others & Karntner Ladesregierung and Others (Joined Cases C-293/12 & C-594/12) [2014] ECR 238

Douglas v Hello! Ltd [2005] EWCA Civ 595

Fontevecchia and D’Amico v. Argentina, judgment of 29 November 2011, Inter-American Court of Human Rights, (Merits, Reparations and Costs, Series C No. 238)

French Data Network and Others (Joined Cases C-511/18, C-512/18, C-520/18) ECLI:EU:C:020:791

Halford v. *United Kingdom* App No. 20605/92, (ECHR, 25 June 1997)

Justice K.S.Puttaswamy (Retired). vs Union of India And Ors., 2017

Katz v. United States, 389 U.S. 347 (1967)

Kaye v *Robertson* [1991] FSR 62

Kennedy v. *United Kingdom* App no. 26839/05 (ECHR 18 August 2010)

Klass v*. Germany* (1978) App No.5029/71, (EHRR, 1978)

La Quadrature du Net and Others (C-511/18) ECLI: EU:C:2020:791

Leander v*. Sweden* App No. 9248/81, (EHRR, 26 March 1987)

Liberty and Others v. United Kingdom App No 58243/00 (ECHR 1 October 2008)

Malone v. *United Kingdom* App No. 8691/79, (ECHR, 2 August 1984)

Mosley v News Group Newspapers [2008] EWHC 1777 (QB)

Murray v Big Pictures (UK) Ltd, [2008] EWCA Civ 446

Niemietz v. Germany App. No. 13710/88 (ECHR, 16 December 1992)

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

Open Door and Dublin Well Woman v Ireland, App No. 14235/88 (ECHR, 29 October 1992)

Ordre des barreaux francophones et germanophone and Others (Joined Cases C-511/18, C-512/18, 52/18) ECLI:EU:C:2020:7

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (C-623/17) ECLI:EU:C:2020:790

Rotaru v. *Romania* App No.28341/95 (ECHR, 4 May 2000)

Schüssel v. Austria App No. 42409/98, (ECHR, 21 February 2002)

Smith v. Maryland, 442 U.S. 735 (1979

Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others (Joined Cases C-203/15 and C-698/15) ECLI:EU:C:2016:970

United States v. Jones, 565 U.S. 400 (2012)

United States v. Miller, 425 U.S. 435 (1976)

Volker und Markus Schecke and Eifert (Joined Cases C-92/09 and 93/09) EU:C:2010:662

Von Hannover v Germany App No. 59320/00 (ECtHR, 24 September 2004)

Weber and Saravia v. *Germany* App No 54934/00. (ECHR 29 June 2006)

Zhu Yingguang v Lianyungang City Branch of China United Network Communications Co., Ltd, Intermediate Court of Lianyungang City, Jiangsu Province, No. 0006 of 2014

Legislation and International Instruments

American Convention on Human Rights, Adopted at the Inter-American Specialized Conference on Human Rights, San José, Costa Rica, 22 November 1969

Austria, BGBl. Nr. 59/1964 1958

Bundesgesetz über den Schutz personenbezogener Daten BGBl 565/1978 (AT)

BVerfGE 35, 202 – Lebach and BVerfGE 65, 1 - Census Act

Census Act, BVerfGE 65 2020 (DE)

Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, ETS No. 108, 1 October 1985

Council Directive 95/46/EC of the European Parliament and of the Council of 14 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

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

Datenschutzgesetz of 7 October 1970 (HDSG)

Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet) 2014

European Union, Charter of Fundamental Rights of the European Union [2012] OJ C 326/02

General Principles of Civil Law《民法通则 1987

German Federal Data Protection Act 1977

International Conference of American States, The American Declaration of the Rights and Duties of Man, 9th Sess., UN Doc. E/CN.4/122 (1948)

Loi du 31 mars 1979 reglementant l’utilisation des donnees nominatives dans les traitements informatiques) 1979 (LU)

Loi n° 78-17 du 6 Janvier 1978 relative à l’informatique, aux fichiers et aux libertés 1978 (FR)

Lov nr 294 af 8 juni 1978 om offentlige myndigheders register (DK)

Lov om personregistre mm av 9 juni 1978 nr 48 (NO)

Nihon-koku kenpō, 1947

The Belgian Constitution 1831

The Bermuda Constitution Order 1968

The Canada Act 1982 (UK)

The Canadian Charter of Rights and Freedoms 1982

The Columbian Constitution 1991

The Constitution of Gabon 1991

The Constitution of the Republic of Korea 1987

The Constitution of Trinidad and Tobago 1976

The Datalagen in Sweden in 1973 (Datalagen, 11 May 1973)

The Hong Kong Basic Law 1982

The Human Rights Act 1998

The Mexican Constitution 1917

The Philippine Constitution 1987

The Portuguese Constitution 1976

The Swiss Constitution 1999

Tort Liability Law (《侵权责任法) 2010

Writ Petition (Civil) No. 494 of 2012, 2017

Reports and Resolutions

The Citizen Lab and Canadian Internet Policy & Public Interest Clinic, “Shining a Light on the Encryption Debate” (May 2018) - https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

Global Commission on Internet Governance, “One Internet” (June 2016) - https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf

Global Privacy Assembly, “International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other Fundamental Rights” (October 2019) - http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf

International Conference of Data Protection and Privacy Commissioners, “The protection of personal data and privacy in a globalised world: a universal right respecting diversities” (2005). Available at: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf

International Conference of Privacy and Data Protection Commissioners, “Resolution on anchoring data protection and the protection of privacy in international law’ (2013). Available at: www.globalprivacyassembly.org/wp-content/uploads/2015/02/International-law-resolution.pdf

International Law Commission, “Report on the work of the fifty-eighth session” (2006), A 61/10, Annex D. Available at: https://legal.un.org/ilc/reports/2006/english/annexes.pdf

The Law Society of England and Wales, “Algorithms in the Criminal Justice System”, June 2019. Available at: https://www.lawsociety.org.uk/topics/research/algorithm-use-in-the-criminal-justice-system-report

UN Special Rapporteur on Freedom of Expression, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’, Human Rights Council: Twenty-ninth session, agenda item 3, 22 May 2015. Available at: https://www.undocs.org/A/HRC/29/32

UN Special Rapporteur on the Right of Privacy, ‘Report of the Special Rapporteur on the right to privacy’: Seventy-third session of the UN General Assembly, 17 October 2018. Available at: https://undocs.org/A/73/438

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and express, Report to the Human Rights Council on Surveillance and Human Rights, 28 May 2019. Available at: https://undocs.org/A/HRC/41/35

Other

Agencia Espanola de Proteccion de Datos, ‘Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data’ (unpublished draft, January 2009; updated drafts dated 24 February and 24 April 2009)

Bedingfield, “Everything that went wrong with the botched A-Levels algorithm”, Wired, 19 August 2020. Available at: https://www.wired.co.uk/article/alevel-exam-algorithm.

Clifford, *The Legal Limits to the Monetisation of Online Emotions* (2019, PhD Thesis, KU Leuven). Available at: https://www.law.kuleuven.be/citip/en/research/phd-research/finalized/phd-damian-clifford.

CNIL, ‘How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence’ (2017). Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

Coughlan, “A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco”, BBC, 26 August 2020. Available at: https://www.bbc.co.uk/news/education-53923279.

Commission Européenne pour la Démocratie par le Droit (Commission de Venise), Luxembourg – Proposition de revision portant instauration d’une nouvelle constitution, Strasbourg, le 27 février 2019 (Rapport de la Luxembourg, CDL-REF(2019)006

deNisco Rayome, “The US, China and the AI arms race: Cutting through the hype”, CNet, 8 July 2020. Available at: https://www.cnet.com/news/the-us-china-and-the-ai-arms-race-cutting-through-the-hype/.

de Terwangne, ‘Convention 108+ evaluation and follow-up mechanisms’, 1 July 2020. Available at: https://www.coe.int/en/web/data-protection/follow-up-and-evaluation-mechanism

European Commission, “Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World” COM (2017)7 final

Gonzalez-Fuster and Hijmans, ‘The EU rights to privacy and personal data protection: 20 years in 10 questions’, Discussion Paper, Brussels Privacy Hub

Google, ‘Updating our privacy policies and terms of service’, 24 January 2012; Available at: http://googleblog.blogspot.co.uk/2012/01/updating-our-privacy-policies-and-terms.html

Kuner, ‘Extraterritoriality and Fundamental Right to Data Protection’ (EJIL: Talk, 16 December 2013). Available at: https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/comment-page-1/ .

Levin, “Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'”, The Guardian, 1 May 2017. Available at: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

Malgieri, ‘The concept of fairness in the GDPR: a linguistic and contextual interpretation”, FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020).

Sitaropoulos ‘States are Bound to Consider the UN Human Rights Committee’s Views in Good Faith’ (OxHRH Blog, 11 March 2015). Available at: www.humanrights.dev3.oneltd.eu/states-are-bound-to-consider-the-un-human-rights-committees-views-in-good-faith/

UN Human Rights Committee, General Comment 16, issued 23.3.1988 (UN Doc A/43/40, 181–183)

UN, Guidelines for the Regulation of Computerized Personal Data Files, Final report submitted by Louis Joinet, Special Rapporteur, 21 July 1988 (E/CN.4/Sub.2/1988/22).

UN General Assembly, Optional Protocol to the International Covenant on Civil and Political Rights, 19 December 1966, United Nations, Treaty Series, vol. 999, p. 171, Article 2

Substantive additions following GPA Reference Panel review

p.4 – reference to advocacy for “privacy accountability” (within organizations) as distinct from rights-based regimes (focused on individual redress and remedies)
p. 7 – reference to other models of regulation and views from the tech industry on organizational responsibilities
p. 9 – added elaboration on the importance of explicit codification of privacy rights, esp. given opacity of data practices and complexity of new technologies
p. 11 – added reference to historical notions of communal privacy
p. 12- added caveat around historical / social construction of privacy discourse
p. 13 – added reference to privacy-related work and instruments from UN bodies + reordered section on privacy rights at the national level
p. 18-19 – added description of “rights-based” regime
p. 20 – added reference to vertical / horizontal, positive / negative rights
p. 21- added description of international human rights law (namely, that these rights are both inter-related and inter-dependent)
p. 21 – added explicit reference to contributions of Gavison and Zuboff in discussion of privacy and “self-determination”
p. 22 - added example of how the UN establishes a right to be “fundamental” (using example of rights of persons with disabilities)
p. 25 – added reference to concept of informational asymmetry, in discussion of privacy and human dignity
p. 26 – added reference to opaque collection and use of data, in particular around electoral process
p. 28-29 – added reference to regional divergences in data governance
p. 30 – added reference to indigenous conceptions of privacy and importance of consultation
p. 31 – added reference to privacy as protection for both dignity of the person and principle of self-determination
p. 37 – expanded discussion of UDHR and contextual framing of rights
p. 42 - 44 – expanded link between privacy risks and discriminatory practices
p. 50 – added reference to DPAs potential work with UN bodies engaged on privacy issues

---

Endnotes and references

* Prepared on behalf of the Office of the Privacy Commissioner (Canada) on behalf of Dr. Orla Lynskey (Associate Professor, LSE Law Department) and Judith Rauhofer (Senior Lecturer and Associate Director of the Centre for Studies of Intellectual Property and Technology Law (SCRIPT), University of Edinburgh). Orla Lynskey is an Associate Professor of Law at the LSE and a Visiting Professor at the College of Europe, Bruges. She conducts research and teaches in the areas of data protection, digital rights and technology regulation. Her current research is concerned with the legal and policy challenges of embedding private sector technologies into public sector infrastructure and decision-making. She is an editor of International Data Privacy Law and the Modern Law Review.

[1] *International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other Fundamental Rights* (October 2019) - http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf
[2] See, respectively: Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, 23 September 1980 (hereafter OECD Privacy Guidelines) as modernised by Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] (hereafter Revised OECD Privacy Guidelines); Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108 (hereafter Convention 108) as modernised by Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM(2018)2-final, 18 May 2018 (hereafter Convention 108+); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31 23.11.1995 (hereafter 1995 Directive) as modernised by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4 May 2016 (hereafter GDPR).
[3] S Landau, *Surveillance or security? The risks posed by new wiretapping technologies* (MIT Press, 2010), 10. “Privacy is a fundamental aspect of a functioning human society, a clear necessity for human freedom and dignity … privacy includes the right to control information about yourself, the right to associate as you wish, as privately as you wish, to share confidences in confidence, the right to enjoy solitude and intimacy. It includes the right to anonymity.”
[4] T Oguru, “Electronic government and surveillance-oriented societies” in D. Lyon (ed.), *Theorizing Surveillance: the Panopticon and Beyond* (Routledge, 2006), 280. “Modern legal systems are facing a major turning point in the regulation of political power; law is directed at the regulation of human behaviour but it cannot control computers … democratic regulation based on the rule of law has lost regulatory power.”
[5] UN High Commissioner for Human Rights, “The Right to Privacy in the Digital Age” (2018) - https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx; see also Rengel, Alexandra, “Privacy as an International Human Right and the Right to Obscurity in Cyberspace” (December 2014). *Groningen Journal of International Law*, Vol. 2, No. 2, 2014, Available at: https://ssrn.com/abstract=2599271
[6] OECD, “Data-driven innovation for growth and well-being” - http://oe.cd/bigdata; see also Martin Abrams, “The Origins of Personal Data and its Implications of Governance” from the Information Accountability Foundation (2016) – available at: https://informationaccountability.org/publications/
[7] D Acemoglu and J Robinson, *The Narrow Corridor: States, societies and the Fate of Liberty* (Penguin Random House, 2019), 492. “Rights are intimately connected to our notion of liberty as protection of individuals from fear, violence and dominance. Though fear and violence have been the main drivers … dominance – the inability of people to make choices and pursue their lives according to their own values – is also stifling. Rights are fundamentally ways for society to encode in its laws and norms the capacity of all individuals to make such choices.
[8] W Webster, “Public administration as surveillance” in Ball, Haggerty and Lyon (eds.), *Routledge Handbook of Surveillance Studies* (Routledge, 2012), 313. “In a drive to make government and public services more efficient and cost-effective, huge sums of money have been invested in electronic infrastructure, databases and e-government … societies built around technologically mediated surveillance practices are to a large degree dependent upon the surveillance platform and apparatus created by public administrations … by making surveillance a normal part of everyday life.”
[9] Alan Westin, *Privacy and Freedom* (1967), 359
[10] Canada. *Department of Justice. Privacy and Computers*: report of the taskforce established by the Departments of Communications and Justice (Ottawa, 1971), 10.
[11] Harold Innis, “Industrialism and cultural values” from *The Bias of Communication* (1951), 140
[12] V Mayer-Schönberger and K Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2018), 83-84.
[13] Andy McStay, *Emotional AI* (Sage, 2018), 115.
[14] See Eye Q website available at: https://eyeq.tech/retail/.

[15] S Levin, “Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'”, The Guardian, 1 May 2017. Available at: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.
[16] D Clifford, *The Legal Limits to the Monetisation of Online Emotions* (2019, PhD Thesis, KU Leuven), 266-288. Available at: https://www.law.kuleuven.be/citip/en/research/phd-research/finalized/phd-damian-clifford.
[17] A McStay, “Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy”, January 2020, *Big Data & Society*, 1-12.
[18] This is also highlighted by Cohen, who argues that “[i]n government proceedings and in the popular press, the information processing industries have worked to position innovation and protective regulation as intractably opposed. That strategy has produced a discursive process that infuses “innovation” with a particular, contingent meaning linked to economic liberty and the absence of government oversight.”; see J Cohen, Between Truth and Power: The Legal Construction of Information Capitalism, 2019, OUP, p.90
[19] For example, compare the Ada Lovelace Foundation work on “Data for the Public Good” - https://www.adalovelaceinstitute.org/our-work/library/, with similar work by the Royal Society on “Using Data for the Public Good” - https://royalsociety.org/blog/2020/07/using-data-for-the-public-good/, with work by the OECD on “Enhancing access to and sharing of data” - https://www.oecd.org/digital/ieconomy/enhanced-data-access.htm.
[20] Royal Society of Canada Working Group on Infoveillance (March 2021) - https://rsc-src.ca/sites/default/files/Infoveillance_EN_0.pdf
[21] J Rauhofer (2014) ‘Round and round the garden?: Big data, small government and the balance of power in the information age’ in Erich Schweighofer, Franz Kummer, Walter Hoetzendorfer (eds.), Transparenz (OCG, 203), 606-617, p.615.
[22] For a discussion of the use of algorithms in the criminal justice system see: The Law Society of England and Wales, “Algorithms in the Criminal Justice System”, June 2019, p.15-17.
[23] A deNisco Rayome, “The US, China and the AI arms race: Cutting through the hype”, CNet, 8 July 2020. Available at: https://www.cnet.com/news/the-us-china-and-the-ai-arms-race-cutting-through-the-hype/.
[24] S Coughlan, “A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco”, BBC, 26 August 2020. Available at: https://www.bbc.co.uk/news/education-53923279.
[25] W Bedingfield, “Everything that went wrong with the botched A-Levels algorithm”, Wired, 19 August 2020. Available at: https://www.wired.co.uk/article/alevel-exam-algorithm.
[26] Ibid.
[27] Evgeny Morozov, “The tech solutions for coronavirus take the surveillance state to the next level”, *The Guardian* (April 15, 2020) - https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt
[28] See, for example, Budd, J., Miller, B.S., Manning, E.M. et al. Digital technologies in the public-health response to COVID-19. *Nat Med* 26, 1183–1192 (2020). https://doi.org/10.1038/s41591-020-1011-4, and, De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, 55, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171
[29] Zuboff *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019)
[30] Cicero, *De Officiis (On Obligations),* translated P. G. Walsh (Oxford, 2008), Book I, sec. 85, p. 30
[31] F. D. Schoeman, *Privacy and social freedom* (1992), 116
[32] Daniel Solove, *Understanding Privacy* (2008), pp. 61-62
[33] Laura K. Donohue, *The future of foreign intelligence: privacy and surveillance in a digital age* (Oxford, NY: 2016), p. 75-76.
[34] John H. Shattuck, *Rights of Privacy* (1977), pp. 3-5
[35] Stanley A. Cohen, *Invasion of Privacy* (1983), pp. 20-21, 34, 52
[36] James Madison, *Federalist Papers*, No. 51 (1788) - https://billofrightsinstitute.org/primary-sources/federalist-no-51; also Louis D. Brandeis and Samuel D. Warren, “The Right to Privacy” *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. - http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C
[37] Georges Duby, ‘Introduction: Private Power, Public Power’, in *A History of Private Life. II: Revelation of the Medieval World*, edited by Georges Duby (Cambridge MA: Belknap Press, 1988)

[38] Diane Shaw, 'The Construction of the Private in Medieval London', *Journal of Medieval and Early Modern Studies*, 26 (1996), p. 450.
[39] David Vincent, *Privacy: A Short History* (Wiley, 2016), p. 2.
[40] SD Warren and LD Brandeis, 'The right to privacy' (1890), 4 *Harvard Law Review* 193-220. In fact, the phrase "right to be let alone" had been coined by Judge Cooley several years earlier. See TM Cooley, *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract,* (2nd ed, Chicago, Callaghan & Company, 1880), p. 29.
[41] Ibid, p. 198.
[42] While Article 8 ECHR has had a wide-ranging impact on privacy protection in Council of Europe Member States, the UN ICCPR has had less impact. A Human Rights Committee (HRC) comprised of independent experts is charged with interpreting and ensuring compliance with the ICCPR. The HRC steers the interpretation of ICCPR provisions by issuing "general comments" on their interpretation. It has already exercised this power to issue a general comment on Article 17 ICCPR. See General Comment 16, issued 23.3.1988 (UN Doc A/43/40, 181–183).
[43] As these State reports, if submitted at all, do not necessarily accurately assess State respect for ICCPR rights, they are often supplemented by "shadow reports" submitted by civil society actors. The Committee discusses these reports with State parties and adopts observations and recommendations. While it is best practice for States to adhere to these recommendations, there is no mechanism for their enforcement. In addition to this oversight mechanism, where a State has signed up to the first Optional Protocol, the Committee can hear complaints or petitions from individuals.
[44] This figure is based on a search of the jurisprudence database of the UN Human Rights Office of the High Commissioner. Database available at: www.juris.ohchr.org (search accurate as of 10 September 2020).
[45] N Sitaropoulos "States are Bound to Consider the UN Human Rights Committee's Views in Good Faith" (OxHRH Blog, 11 March 2015). Available at www.humanrights.dev3.oneltd.eu/states-are-bound-to-consider-the-un-human-rights-committees-views-in-good-faith/.
[46] United Nations OHCHR, "Special Rapporteur on the right to privacy: Annual Thematic Reports" - https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx
[47] See further, www.legal.un.org/ilc/.
[48] In the case of Latin America, consider the cases of Mexico and Brazil. In Mexico, there was constitutional recognition of the right to privacy as early as 1917), while their data protection law followed much later, after constitutional reforms that took place during the 1990s and 2000s which recognized data protection in different ways. Latin America is unique, for example, in codifying the concept of "habeas data" (the express recognition of the right to access and the right to know about the individual´s own information). In contrast, in the Brazilian Constitution, under the term Equality and Non-discrimination, it is stated that "many modern data protection frameworks contain a general principle of "fair" personal processing, which is understood to mean non-discriminatory amongst other things". The point is that non-discrimination in most countries of the region is a value in itself, so that terms of "fair" (or fairness) to not always fully translate. Non-discrimination is a value in itself in Brazil and also, for example, in Argentina, where is expressly recognized in the Constitution as a precondition for the habeas data (art. 43).
[49] See Articles 6.A.II and III and Article 16 of the Mexican Constitution 1917 (as amended); Article 13 of the Swiss Constitution 1999 (as amended); Article 22 of the Belgian Constitution 1831 (as amended); Article 17 of the Constitution of the Republic of Korea 1987 (as amended); Article 2(11) and 3(3) of the Philippine Constitution 1987 (as amended); Article 30 of the Hong Kong Basic Law 1982 (as amended); Article 6 of the Portuguese Constitution 1976 (as amended); Article 15 of the Columbian Constitution 1991 (as amended); Article 4(c) of the Constitution of Trinidad and Tobago 1976 (as amended); Article 1(5) and (12) of the Constitution of Gabon 1991(as amended).
[50] Article 7 of the Bermuda Constitution Order 1968 (as amended).
[51] This includes the States of Brandenburg, Mecklenburg-Pomerania, Saxony, Thuringa, Saxony-Anhalt, Schleswig Holstein, Hesse, North Rhine-Westphalia, Rhineland Palatinate and Saarland.
[52] BVerfGE 35, 202 – Lebach and BVerfGE 65, 1 - Census Act.
[53] *Canadian Charter of Rights and Freedoms*, ss 7 and 8, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
[54] *Nihon-koku kenpō*, 3 May 1947
[55] *Justice K.S.Puttaswamy (Retired). vs Union of India And Ors*., 2017, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1.
[56] EU Charter (n **¡Error! Marcador no definido.** above) Article 51(1).

[57] See, in Austria, BGBl. Nr. 59/1964, after signing and ratifying the Convention itself in 1958, see BGBl. Nr. 210/1958 and, in the UK, Human Rights Act 1998 (HRA). Despite the UK being one of the co-founders and original signatories of the ECHR, until the adoption of the HRA, claimants had to exhaust all domestic remedies before they could raise fundamental right issues before the European Court of Human Rights in Strasbourg. It should be noted, however, that even after the HRA came into force, the constitutional principle of parliamentary sovereignty meant that the courts cannot invalidate Acts of Parliament. They can merely issue a "declaration of incompatibility" of those Acts with the ECHR. It is then up to the legislator to amend or repeal the relevant Act, see s. 4, HRA.
[58] Datenschutzgesetz of 7 October 1970 (HDSG), GVBl. I, 625.
[59] See, for example, the Datalagen in Sweden in 1973 (Datalagen, 11 May 1973), the first German Federal Data Protection Act in 1977 (Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung, Bundesdatenschutzgesetz (BDSG 1977), BGBl. I, 201), and other national laws in France (Loi n8 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés), Denmark (Lov nr 294 af 8 juni 1978 om offentlige myndigheders register), Norway (Lov om personregistre mm av 9 juni 1978 nr 48) and Austria (Bundesgesetz uber den Schutz personenbezogener Daten BGBl. 565/1978) in 1978, and Luxembourg (Loi du 31 mars 1979 reglementant l'utilisation des donnees nominatives dans les traitements informatiques) in 1979.
[60] As a matter of historical fact, it could therefore be argued that data protection law was initially a creature of primary rather than constitutional law. Relevant laws might have a private law or a public law focus, depending on the type of data users they intended to regulate. However, it seems clear that, in itself, the right to the protection of an individual's personal information was not initially perceived as a self-standing fundamental right.
[61] In EU parlance "secondary law" is equivalent to first rank non-constitutional law as the term "primary law" is reserved for the EU treaties.
[62] Recital 11 of Directive 95/46 "Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data"
[63] At the time, the varied nature of those national frameworks meant the EU member states were at risk of establishing trade barriers between each other because of the different levels of protection they provided and the increasing unwillingness of individual member states to allow cross-border transfers of personal information to countries that provided lower levels of protection.
[64] Article 1(1) 1995 Directive (n 2).
[65] An earlier version of the Charter was first drafted and solemnly proclaimed on 7 December 2000 with the intention that it should eventually become part of the EU's binding constitutional instruments. A modified version of the original text formed part of the proposed European Constitution, which was intended to replace the existing EU treaties with a single text. However, although the Constitution was signed by all of the then members states, its failure to be ratified by all of them meant that it never came into force. It was ultimately abandoned in 2004. A right to data protection is also set out in Article 16 of the Treaty on the Functioning of the European Union (TFEU), which includes an obligation on the EU legislature to adopt rules governing the processing of personal data by EU institutions and member states when carrying out activities that fall within the scope of EU law.
[66] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Exchanging and Protecting Personal Data in a Globalised World COM/2017/07 final – Point 3.3.1 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN
[67] Guidelines for the Regulation of Computerized Personal Data Files, final report submitted by Louis Joinet, Special Rapporteur, 21 July 1988 (E/CN.4/Sub.2/1988/22).
[68] C Kuner, "An International Legal Framework for Data Protection: Issues and Prospects" (2009)25 *Computer Law and Security Review* 307, p. 309.
[69] European Union, Charter of Fundamental Rights of the European Union [2012] OJ C 326/02, Article 8.
[70] See 27th International Conference of Data Protection and Privacy Commissioners, "The protection of personal data and privacy in a globalised world: a universal right respecting diversities" (2005), www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf. To this end, the Commissioner's also appealed: to every Government in the world to promote the adoption of legal instruments of data protection and privacy according to the basic principles of data protection and also to extend it to their mutual relations; to the Council of Europe to invite, in accordance with article

23 of the Convention for the protection of individuals with regard to automatic processing of personal data, non- member-states of the Council of Europe which already have a data protection legislation to accede to this Convention and its additional Protocol.
[71] Ibid, para. 12.
[72] Ibid, p. 3.
[73] ICDPPC, Madrid Resolution (November 2009) - http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf
[74] See, respectively: Agencia Espanola de Proteccion de Datos, "Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data" (unpublished draft, January 2009; updated drafts dated 24 February and 24 April 2009); International Conference of Privacy and Data Protection Commissioners, "Resolution on anchoring data protection and the protection of privacy in international law" (2013), available at: www.globalprivacyassembly.org/wp-content/uploads/2015/02/International-law-resolution.pdf.
[75] If such cooperation is perceived to be ineffective, this may lead to resistance to entrenching international legal protection and giving it more impact over domestic data protection standards. For instance, the existing UN instruments receive little recognition on the international stage.
[76] KM Yilma, "The United Nations data privacy system and its limits" (2019)33 *International Review of Law, Computers & Technology* 224, p. 230.
[77] See, P de Hert and V Papakonstantinou, "Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency" (2013)9 Journal of Law and Policy 271, p. 282.
[78] European Parliamentary report on the Commission Evaluation report on the implementation of the GDPR two years after its application (March 17, 2021) - https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.pdf; Access Now, *Two Years Under the EU GDPR: An Implementation Progress Report* (May 2020) - https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf; Nathan Eddy, "How EU Authorities See GDPR Effectiveness Two Years In", *e-Week* (June 17, 2020) - https://www.eweek.com/security/how-eu-authorities-see-gdpr-effectiveness-two-years-in/
[79] I/A Court H.R, Case of *Fontevecchia and D'Amico v. Argentina*, judgment of 29 November 2011 (Merits, Reparations and Costs, Series C No. 238), para. 49
[80] See, for instance, joined Cases C-92/09 and 93/09, *Volker und Markus Schecke and Eifert* EU: C: 2010: 662, para. 89.
[81] One area of continued contention is whether and how the benefits of innovation can be reconciled with the protection of fundamental rights. Division on this issue was already evident in the 1970's when the UN General Assembly adopted a 'Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefits of Mankind'. UN Countries in the Global North and West boycotted this declaration and abstained from voting on subsequent resolutions as these more industrial nations were keen to have emphasis placed on the potentially negative impact of technological developments on human rights. See Yilma (n **¡Error! Marcador no definido.**), pp. 227 and 228.
[82] Kuner (n **¡Error! Marcador no definido.**), p. 310.
[83] González Fuster G. (2014) "Privacy and the Protection of Personal Data Avant la Lettre." In: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Law, Governance and Technology Series, vol. 16. Springer, Cham. https://doi.org/10.1007/978-3-319-05023-2_2
[84] However, as Gonzalez Fuster and Hijmans note, their co-existence has triggered many questions, very few of which have "been answered since in a clear, consistent, or consensual manner". G Gonzalez-Fuster and H Hijmans, 'The EU rights to privacy and personal data protection: 20 years in 10 questions', Discussion Paper, Brussels Privacy Hub. Available at: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_González_Fuster_Hijmans.pdf.
[85] As a general rule, it seeks to enable individuals ("data subjects") to control access to information about them by making the processing of personal data subject to their consent or to the existence of laws that authorise such processing. A right to data protection commonly grants data subjects a number of legal rights, including most notably the right to access their data where it is held by others. It also imposes on data users ("controllers") a number of corresponding legal obligations.
[86] For instance, in order to accede to Convention 108+, States must have an independent supervisory authority in place (Article 15(5), Convention 108+, n 1 above). Article 8(2) of the EU Charter of Fundamental Rights and Article 16 of the Treaty on European Union and the Treaty on the Functioning of the European Union (Consolidated version, Official Journal C 326 , 26/10/2012 P. 0001

– 0390) both provide that compliance with data protection rules must be subject to control by an independent authority.

[87] For example, see rules and procedures detailed by the US Congressional Research Service in their report, *Data Protection Law: An Overview* (March 2019). Available at https://fas.org/sgp/crs/misc/R45631.pdf

[88] W Veil, "The GDPR: The Emperor's New Clothes - On the Structural Shortcomings of Both the Old and the New Data Protection Law" (2018), p. 22. Available at SSRN: https://ssrn.com/abstract=3305056

[89] O Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015), pp. 91-105.

[90] P de Hert and S Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in Claes et al (eds), *Privacy and the criminal law* (Intersentia, 2006) 61, pp. 66-67

[91] D Solove, *The Digital Person: Technology and Privacy in the Information Age* (NYU Press, 2004), p. 8.

[92] G Gonzalez-Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2004), p. 257.

[93] O Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal
Order" (2014) 63 *International and Comparative Law Quarterly* 569, pp. 584-585.

[94] Mark Chinen, "Complexity Theory and the Horizontal and Vertical Dimensions of State Responsibility", *European Journal of International Law*, Volume 25, Issue 3, August 2014, Pages 703–732, https://doi.org/10.1093/ejil/chu048

[95] Corrin, Jennifer. "From Horizontal and Vertical to Lateral: Extending the Effect of Human Rights in Post-Colonial Legal Systems of the South Pacific." *The International and Comparative Law Quarterly* 58, no. 1 (2009): 31-71. Accessed July 30, 2021. http://www.jstor.org/stable/20488273.

[96] P De Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S Gutwirth et al (eds), Reinventing Data Protection? (Springer 2009) 5, p. 8.

[97] Lynskey (n **¡Error! Marcador no definido.**) pp. 586-587.

[98] AF Westin, *Privacy and Freedom* (1967, Atheneum), pp.324-325.

[99] Gavison, Ruth E., Privacy and the Limits of Law (May 16, 2012). *The Yale Law Journal,* Vol. 89, No. 3 (Jan., 1980), pp. 421-471, Available at SSRN: https://ssrn.com/abstract=2060957, or Zuboff, Shoshana, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization (April 4, 2015). *Journal of Information Technology* (2015) 30, 75–89. doi:10.1057/jit.2015.5, Available at SSRN: https://ssrn.com/abstract=2594754

[100] For an elaboration of this distinction see Gonzalez-Fuster and Hijmans (n **¡Error! Marcador no definido.**) p. 6.

[101] R Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere" (2018)67 *Duke Law Journal* 980, 1011.

[102] CJ Hoofnagle, B van der Sloot & FZ Borgesius, "The European Union general data protection regulation: what it is and what it means" (2019)28 *Information & Communications Technology Law* 65.

[103] L Dalla Corte, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' in D Hallinan et al (eds), *Data Protection and Privacy: Data Protection and Democracy* (Hart, 2020) p. 27; See also Veil (n **¡Error! Marcador no definido.**) p. 22.

[104] H Hijmans, *The European Union as Guardian of Internet Privacy* (Springer, 2016), para. 2.13.

[105] N Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights", p. 7. Available at: www.hal.inria.fr/hal-01559453.

[106] A Rouvroy and Y Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in S Gutwirth et al (eds), Reinventing Data Protection? (Springer 2009), p. 45.

[107] Andrade suggests, for instance, that it is 'only after the weighing and balancing of substantive interests and rights in question, that procedural rights come into play, laying out the legal conditions and procedures through which those substantive rights are to be effectively enforced'. Andrade (n **¡Error! Marcador no definido.**) 6.

[108] In US Constitutional Law, debates persist regarding whether due process is a substantive or procedural right. Nevertheless, its status as a constitutional right is never in doubt. The same could be said for the right to a fair trial, recognised in multiple international legal instruments. More recently,

procedural environmental rights have been introduced into national constitutional documents and international legal agreements.

[109] UN High Commission on Human Rights, *General Comment on Article 9 of UN CRPD (Accessibility*) -https://www.ohchr.org/EN/HRBodies/CRPD/Pages/GC.aspx

[110] Article 1, EU Charter (n **¡Error! Marcador no definido.**). Although an express right to human dignity is not included in the ECHR, its Protocol No. 13 for the Protection of Human Rights and Fundamental Freedoms concerning the abolition of the death penalty in all circumstances refers to need for "the full recognition of the inherent dignity of all human beings".

[111] I Kant, *Groundwork for the Metaphysics of Morals* (Abbott Thomas K. tr, 2005), 88 (emphasis omitted).

[112] D Lyon, *The Electronic Eye: The Rise of Surveillance Society* (University of Minnesota Press, 1994), p. 109.

[113] D Keats Citron and F Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1, 3.

[114] Colin J. Bennett, "In Defence of Privacy: the concept and the regime" from *Surveillance and Society* 8(4) 2011, pp. 485-496 - https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/4184/privacy_debate

[115] Frederik J. Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International 2015), p. 43.

[116] Justin Sherman, "Data Brokers Are A Threat To Democracy", *Wired* (April 2021) - https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/

[117] Lyon (n 112), p. 13.

[118] K Crawford and J Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 *Boston College Law Review* 93, p. 111.

[119] Lyon (n 112), pp. 70-71. See also A Spina, 'Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?' (2014) 2 *European Journal of Risk Regulation* 248, p. 251.

[120] J Raz, *The Morality of Freedom* (Oxford University Press 1986), p. 369.

[121] "Invictus", WE Henley in "A Book of Verses" (D. Nutt, 1888), pp. 56–57.

[122] Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature*, 54 (2):442-92 - https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442

[123] For example, see Fred H. Cate's "The Failure of Fair Information Practice Principles" from *Consumer Protection in the Age of the Information Economy* (2006) - https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf

[124] TI Emerson, *The system of freedom of expression* (Random House Trade, 1970), p. 549.

[125] Regan, Priscilla M. Legislating Privacy: Technology, Social Values and Public Policy. Chapel Hill, NC: University of North Carolina Press, 1995; or,

[126] On commodification see: C Prins, "When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter" (2006)3 SCRIPTed 270.

[127] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021) (February 11, 2021). (2021) 169 *Privacy Laws & Business International Report.* 6-19, Available at SSRN: https://ssrn.com/abstract=3836261 or http://dx.doi.org/10.2139/ssrn.3836261

[128] Graham Greenleaf, A*sian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, 2014) and *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) - https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia

[129] One example would be Singapore and its human rights policy which is informed by overriding state objectives and national development goals, which actively prioritise economic growth and social order. The scope and application of human rights is qualified by the imperatives of economic development and cultural reference to Neo-Confucian communitarianism. See Prof Thio Li-Ann, "Pragmatism and realism do not mean abdication: a critical and empirical inquiry into Singapore's engagement with international human rights law" in *Singapore Year Book of International Law* (2004) 8, p. 41-91 - http://www.asianlii.org/sg/journals/SGYrBkIntLaw/2004/4.pdf

[130] For example, some of the oldest data protection laws in the world originate in Asia-Pacific jurisdictions such as Hong Kong, New Zealand, Australia, South Korea, and Japan. As effective and solid as these laws are, they have at their core organizational obligations and rights for data subjects, as opposed to human rights concerns.

[131] China, the EU and the US signed on for the Osaka Track, while India, Indonesia and South Africa opted out, signalling a clear divide in the future of e-commerce negotiations and data governance at the WTO.
[132] India's foreign policy vision around data protection norms links closely with conceptions of 'data sovereignty' or more critically 'data colonialism' (akin to Zuboff's notion of surveillance capitalism). See Arindrait Basu, "Sovereignty in a 'datafied' world: A framework for Indian diplomacy" at *Observer Research Foundation* (May 2, 2021) - https://www.orfonline.org/expert-speak/sovereignty-datafied-world-framework-indian-diplomacy
[133] See for example, "Asia's Family Values Give Way to Data Privacy Concerns" https://www.voanews.com/silicon-valley-technology/asias-family-values-give-way-data-privacy-concerns, and IAPP, "Why China's cultural attitudes toward privacy may be in flux" - https://iapp.org/news/a/why-chinas-cultural-attitudes-toward-privacy-may-be-in-flux/
[134] K Kitiyadisai, "Privacy rights and protection: foreign values in the modern Thai context" (2005)7 *Ethics and Information technology* 17, p. 19.
[135] HN Olinger, JJ. Britz, and MS. Olivier "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa" (2007)39 *The International Information & Library Review* 31, p. 34.
[136] Ibid, p.35.
[137] Ibid.
[138] This argument is made, for example, by Shoshana Zuboff, See S Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
[139] *A History of Private Life: from Pagan Rome to Byzantium*, vol. 1, ed. Paul Veyne (Harvard, 1987), 415
[140] Evgeny Morozov, *To Save Everything, Click Here: the folly of technological solutionism* (2013), 346; see also Ursula Franklin, "Liberty, technology and hope" from The Ursula Franklin Reader (2006), 172
[141] John Stuart Mill, *On Liberty* (NY, 1947, 4-5.
[142] Furthermore, in an information context is has proved challenging to identify real detriment to individual interests, never mind the interest of others or the community. However, new forms of data use (and abuse) have shown that such collective interests should not be ignored when contemplating both the need for and the scope of both rights.
[143] See note **¡Error! Marcador no definido.**.
[144] In the past, online advertisers have argued that the mere tracking of internet users through the use of cookies should not be subject to any form of regulation because, they argue, "no harm occurs", and that privacy and data protection rules should only become engaged at the point when users' behavioural data is mined and profiles of users' behaviour are created by them.
[145] In 1962, the United Nations General Assembly recognised the "right of peoples and nations to permanent sovereignty over their natural wealth and resources." It is clear articulation of not only of group interests but also its right to have it say over resources deemed crucial to the collective interests of the group. See Malcolm Shaw, *International Law, Fifth Edition* (2003, Cambridge University Press).
[146] This approach is particularly apparent in the public sector where varieties of entities proclaim a need to access personal data held by other departments or by businesses to advance legitimate public interests like security, public health or the responsible use of public funds.
[147] P Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010)57 UCLA Law Review 1701, p. 2010
[148] J Rauhofer (n 21), pp. 606-617.
[149] J Cohen (n 18), p. 72.
[150] M Adrejevic, "iSpy: Surveillance and Power in the Interactive Era", (University Press of Kansas, 2007), pp. 2-4 and 104-11.
[151] Article 5(1)(c) GDPR.
[152] Zuboff *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019), p. 8.
[153] However, there are also concerns that the profiling and subsequent targeting of individuals could lead to price discrimination and predatory marketing to particular groups of consumers. For a more recent exploration of these issues, see N Newman, "The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google" (2013); available at SSRN: http://ssrn.com/abstract=2310146, last visited on 20 October 2020.

[154] For a detailed exploration of this phenomenon see E Pariser, *The Filter Bubble: What The Internet Is Hiding From You* (Penguin Books, 2011).
[155] It also seems undeniable that this particular use of personal data - to profile and target individuals - has at least been remarkably effective in bringing certain political messages to a wider audience, exploiting existing discontent and connecting the likeminded to each other in ways that was not possible before. Of course, like all technologies those tools are capable of being used for good or ill – and what is considered either may yet lie in the eye of the beholder – but the spread of behavioural surveillance techniques may nevertheless, as Cohen argues, have "produced powerful affordances for volatility, polarization, and public unreason", Cohen (n 18), p. 86.
[156] The use of nuclear power, environmental harm or certain types of research are often cited as comparators.
[157] J Cohen (n 18), p. 90
[158] PM Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995), p.230.
[159] Ibid, p. 233.
[160] S Simitis, "Reviewing Privacy in an Information Society" (1987)135 University of Pennsylvania Law Review 709.
[161] With rare foresight, Simitis also suggested that the question of who can access personal data and what they can do with them should no longer be a primarily individual concern (for example, of celebrities, who wish hide their activities from a curious public) but that the discussion must take into account public or collective interests. This, he felt, was true, in particular, for the kind of ubiquitous data processing that normalises surveillance of the public by those in power and supports their ability to determine and enforce legal and social norms.
[162] Ibid, p, 734.. Also, S Simitis, "Die informationelle Selbstbestimmung—Grundbedingung einer verfassungskonformen Informationsordnung" (1984) Neue Juristische Wochenschrift, 394–405, p. 399.
[163] S Simitis, n 160.
[164] Although it established the right to information self-determination specifically with the aim of granting the individual (qualified) control over their personal data, (one of) the underlying rationale(s) for affording individuals this protection was to equip them to exercise those rights for the benefit of their communities.
[165] See n **¡Error! Marcador no definido.**.
[166] General Comment (n **¡Error! Marcador no definido.**) paras 3 and 7.
[167] Claims that data protection and privacy impede the attainment of other rights and interests therefore often fail to apply this method of reconciliation appropriately, or even to understand that such reconciliation is possible.
[168] UN Office of the High Commissioner for Human Rights, *Article 19: Freedom of Opinion and Expression* - https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23944&LangID=E
[169] See, for example, Article 8(2) ECHR. Based on the notion that national security is designed to protect the right to life, it is often difficult to argue that a balance should nevertheless be struck between the two interests. However, security is also a question of perspective and of the threat model that is used to justify privacy intrusions. Proponents of restrictions on fundamental rights in the interest of security generally argue on the basis of an outward-facing threat model, namely the potential for an attack by an external enemy in the context of terrorism or organised crime. Security measures advocated in this context are generally held out as protecting the very individuals, whose privacy or data protection rights those measures may infringe with the State taking on the role of protector. The balance to be struck in this case is thereby represented as a zero-sum game where an increase in security (provided by the State) will inevitably necessitate an interference with the individual's privacy (perpetrated by the State). However, other threat models exist contemporaneously and deserve to be taken into account when the balance between privacy versus security is struck. One of those threat models is inward-facing, namely the threat to which individuals, alone and collectively, are exposed when faced with an authoritarian or totalitarian governance model. Human rights instruments have largely developed as negative defence rights designed to protect the individual from the overbearing state. Security in this context could therefore be defined as security from the very institutions that seek to justify the need to interfere with the individual's rights and freedoms regardless of the protections afforded by those instruments. In this situation, individuals rely on the right to privacy and data protection precisely to counter the threat that emanates from the State

not just to their own personal security but to the democratic institutions designed to protec their rights and liberty. Whether security requires the infringement or the protection of informational privacy therefore depends on how the threat is framed.

[170] See *Klass v Germany* and *Amann v Switzerland* (n **¡Error! Marcador no definido.**).

[171] See *Judgement of the Court of Justice in Case C-746/18 Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* (n 45).

[172] United Nations, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association to the Human Rights Council* (May 2019) - https://undocs.org/A/HRC/41/41

[173] CJ Benett and CD Raab, *The Governance of Privacy* (2nd ed, MIT Press, 2006) p. 23.

[174] In other areas, this also suggests that the convenience and efficiency that both public and private entities derive from the creation of large data stores (for example, centralized national health records) or methods of ubiquitous surveillance (like CCTV, facial recognition technologies or online behavioural tracking) must be balanced against the possibility of abuse. Effective technical and regulatory security features can prevent the "database state" from becoming the virtual equivalent of Jeremy Bentham's "panopticon", the famous prison model where inmates could be watched from a central point without them knowing when, or indeed if, they were being observed. This is because the "unequal gaze" that characterizes that kind or surveillance carries the risk of causing the internalisation of a disciplinary mind-set in those observed. While, on the one hand, this means that individuals living under that gaze are less likely to break rules or laws, on the other hand, they may be deterred from exercising their individual rights and freedoms or from generally participating in the democratic process.

[175] E Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964)39 *New York University Law Review* 1000.

[176] D Lyon, *Surveillance after September 11* (Polity Press, 2003), p. 27.

[177] This is in fact the premise of the movie "Minority Report" where law enforcement has found a way of predicting the commission of a crime and is therefore able to prevent it. Unfortunately, the method of prediction turned out to be faulty in some cases. Members of "suspected" categories (for example, members of Muslim communities) may internalise that suspicion resulting in a perception of "unwanted observation" and an avoidance of activities and associations that might be misconstrued. This may lead to a loss of political participation by specific minority groups which is likely to damage the political fabric of a democratic society. It may also encourage members of that group to turn to alternative forms of protest and counteraction and, ultimately, their complete alienation from society and its values.

[178] Lyon (n 176) p.142

[179] Ibid.

[180] PM Regan (n 158), p. 227

[181] Benett and Raab (n 173).

[182] UN Special Rapporteur on the right to privacy, *Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic* (July 2020) - https://undocs.org/A/75/147

[183] Another example might be that the Israeli Supreme Court barred the Israeli security service from continuing to access citizen mobile data without specific legislative authorisation. (Non-consensual use). See Reuters, "Israel's top court says government must legislate COVID-19 phone-tracking" (April 26, 2020)- https://www.reuters.com/article/us-health-coronavirus-israel-monitoring-idUSKCN2280RN

[184] B Petkova, "Privacy as Europe's First Amendment" (2019)25 *European Law Journal* 140, p. 152.

[185] D Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", Human Rights Council: Twenty-ninth session, agenda item 3, 22 May 2015, p. 15.

[186] NM Richards, *The Dangers of Surveillance*, (2013)126 *Harvard Law Review* 1934, pp. 1945-1952.

[187] Ibid, p. 1935.

[188] Ibid, p. 1948.

[189] *Open Door and Dublin Well Woman v Ireland*, App no 14235/88, [1992] ECHR 68, 29 October 1992.

[190] Ibid, para 81.

[191] UN Committee on the Rights of the Child, *General Comment no. 25 (2021) on children's rights in relation to the digital environment* (March 2021) - https://digitallibrary.un.org/record/3906061?ln=en;

see also Women's Legal Education and Action Fund (LEAF), *De-platforming misogyny* (April 2021) - https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[192] Marie-Claude Landry (Chief Commissioner, Canadian Human Rights Commission), "human rights and privacy rights must develop along with it…. A human rights approach to privacy law reform in this country is needed to address emerging concerns about how technology and the digital world are increasingly affecting our everyday lives. Technology and privacy are fundamental to the next generation of human rights. Everyone in Canada should be able to benefit from technology without fear." (July, 2020) - https://www.chrc-ccdp.gc.ca/en/resources/supreme-court-decision-a-human-rights-victory-protection-genetic-discrimination

[193] UN Committee on the Rights of the Child, *General Comment no. 25 (2021) on children's rights in relation to the digital environment* (March 2021) - https://digitallibrary.un.org/record/3906061?ln=en; see also Women's Legal Education and Action Fund (LEAF), *De-platforming misogyny* (April 2021) - https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[194] UN Committee issues recommendations to protect children's rights in digital environment https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26944&LangID=E

[195] https://www.unicef.org/globalinsight/featured-projects/ai-children

[196] *HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE - AI-and-Human-Rights.Pdf*. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf.

[197] *UN Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression - AI and Human Rights 2018 AI-and-FOE-GA.Pdf*. https://freedex.org/wp-content/blogs.dir/2015/files/2018/10/AI-and-FOE-GA.pdf.

[198] *The OECD Artificial Intelligence Policy Observatory*. https://www.oecd.ai/ ; *EU White Paper on Artificial Intelligence – a European Approach to Excellence and Trust | Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/consultations/white-paper-artificial-intelligence-european-approach-excellence-and-trust. ; *Kung - Building an AI World Report on National and Regio.Pdf*. https://cifar.ca/wp-content/uploads/2020/10/building-an-ai-world-second-edition.pdf. ; "Council of Europe and Artificial Intelligence." *Artificial Intelligence*, https://www.coe.int/en/web/artificial-intelligence/home ; *Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights 1680946e64.Pdf*. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.

[199] *Artificial Intelligence: Governance and Leadership Whitepaper (2019) | Australian Human Rights Commission*. https://humanrights.gov.au/our-work/rights-and-freedoms/publications/artificial-intelligence-governance-and-leadership.

[200] Policy Guidance on AI for Children: *Draft for consultation | Recommendations for building AI policies and systems that uphold child rights* https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children

[201] Krishnamurthy, Vivek. "It's Not Enough for AI to Be 'Ethical'; It Must Also Be 'Rights Respecting.'" *Medium*, 10 Oct. 2018, https://medium.com/berkman-klein-center/its-not-enough-for-ai-to-be-ethical-it-must-also-be-rights-respecting-b87f7e215b97 ; Raso, Filippo A., et al. *Artificial Intelligence & Human Rights: Opportunities & Risks*. SSRN Scholarly Paper, ID 3259344, Social Science Research Network, 25 Sept. 2018. *papers.ssrn.com*, doi:10.2139/ssrn.3259344.

[202] Such as the Open-ended intergovernmental working group on transnational corporations and other business enterprises with respect to human rights, with a mandate to elaborate an international legally binding human rights instrument to regulate the activities of transnational corporations and other business enterprises https://www.ohchr.org/en/hrbodies/hrc/wgtranscorp/pages/igwgontnc.aspx ; https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.pdf

[203] And "AI, ADM and the Justice System." *LCO-CDO*, https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/.

[204] Revised draft U.N. treaty on business and human rights: a few steps forward, a few unanswered questions https://www.accessnow.org/revised-draft-u-n-treaty-on-business-and-human-rights-a-few-steps-forward-a-few-unanswered-questions/

[205] *INFOVEILLANCE | The Royal Society of Canada*. https://rsc-src.ca/en/research-and-reports/infoveillance.

[206] Canada, Office of the Privacy Commissioner *News Release: Commissioner Encouraged by Proposals to Modernize the Public Sector Privacy Act*. 24 Mar. 2021, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210324/.

[207] *Equinet Report: REGULATING FOR AN EQUAL AI: A NEW ROLE FOR EQUALITY BODIES.* *https://equineteurope.org/2020/equinet-report-regulating-for-an-equal-ai-a-new-role-for-equality-bodies/ ;*
[208] O De Schutter and J Ringelheim, "Ethnic Profiling: A Rising Challenge for European Human Rights Law" (2008)71 Modern Law Review 358.
[209] M Veale and R Binns, "Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data" (2017)4 *Big Data & Society*. Available at: https://journals.sagepub.com/doi/epub/10.1177/2053951717743530 .
[210] Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis electronic data banks in the public sector; adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies. Annex, para 3.
[211] G Malgieri, "The concept of fairness in the GDPR: a linguistic and contextual interpretation", FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM, 2020). pp. 154-166.
[212] Dispõe sobre a proteção de dados pessoais e altera a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Article IX.
[213] CNIL, "How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence" (2017), p. 49. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.
[214] According to Greenleaf, writing in 2016, by the completion of each decade, the number of laws has expanded from 10 (1970s) to 20 (1980s), to 40 (1990s), to 80 (2000s), and now to 111 (two-thirds through the 2010s). He notes that the "most striking indicator of the globalisation of data privacy laws is that since 2015, the majority of these laws (57/111) are from outside Europe". G Greenleaf, "Balancing globalisation's benefits and commitments: accession to data protection convention 108 by countries outside Europe" [2016] UNSWLRS 52, p. 1.
[215] Avis n° 934/2018, Commission Européenne pour la Démocratie par le Droit (Commission de Venise), Luxembourg – Proposition de revision portant instauration d'une nouvelle constitution, Strasbourg, le 27 février 2019 (Rapport de la Luxembourg, CDL-REF(2019)006); see also, TA Larsen, C Boulanger and A Vandendriessche, "Luxembourg" in *The New EU Data Protection Regime: Setting Global Standards for the Rights to Personal Data Protection* (The Hague, 2020), 411 and 412.
[216] *Puttaswamy* (n **¡Error! Marcador no definido.** above), para 169.
[217] The Data Privacy Act of 2012 (Act no 10173) in the Philippines, adopted in 2012, is inspired in part by the European Commission's legislative proposal for the GDPR. It contains, for instance, a right to data portability (section 18) which is similar in wording to the right now found in Article 20 GDPR and which is otherwise unique to the GDPR.
[218] Convention 108+ (n 2), Article 37(1) and (2).
[219] Ibid, Article 4(3).
[220] See, presentation of Professor Cécile De Terwangne, "Convention 108+ evaluation and follow-up mechanisms", 1 July 2020. Available at: https://www.coe.int/en/web/data-protection/follow-up-and-evaluation-mechanism.
[221] The non-European signatories of Convention 108 are Argentina; Cabo Verde; Mauritius; Mexico; Morocco; Senegal; Tunisia; and Uruguay (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=TAAIBf9O) . Of these, Argentina, Mauritius, Tunisia and Uruguay have signed Convention 108+ which Mauritius has also ratified (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures).
[222] Non-European States acceding until the amending Protocol enters into force will need to deposit accession instruments for both Convention 108 and the amending Protocol. A list of observers (last updated March 2020) is available here: https://rm.coe.int/list-of-observers-nov-2018-en/1680938538.
[223] Colin J. Bennett, "The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession" CIGI Paper No. 246 (November 30, 2020) - https://www.cigionline.org/publications/council-europes-modernized-convention-personal-data-protection-why-canada-should/
[224] This is indicated in the response of the Council of Europe to the GPA Questionnaire (PSWG3 - Privacy/Data Protection & Other Rights and Freedoms).
[225] For a full list of the non-European states that have ratified the Convention see: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Ryk2y1sX (last accessed on 20 October 2020).

[226] G Greenleaf, “How far can Convention 108+ ‘globalise’? Prospects for Asian accessions” (2020) Computer Law & Security Review. Advance access: https://doi.org/10.1016/j.clsr.2020.105414 .. The thirteen key advantages of Convention 108 accession identified by Greenleaf are: “(i) realistic prospects; (ii) no realistic alternative; (iii) voluntary obligations; (iv) international ‘best practice’ recognition; (v) reciprocal data exports; (vi) moderate standards; (vii) minimum standards; (viii) a ‘whitelist’ substitute; (ix) ‘adequacy’ assistance; (x) development assistance; (xi) business benefits with exports and imports; (xii) individual benefits from minimum protections; and (xiii) assistance to international organisations.”

[227] European Commission, “Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World” COM (2017)7 final, 11-12.

[228] UN Special Rapporteur on the Right of Privacy - Annual Report; Seventy-third session of the UN General Assembly 2018 [2018] UNSRPPub 11 (17 October 2018), para 117(e).

[229] G Greenleaf, “How far can Convention 108+ ‘globalise’? Prospects for Asian accessions” (2020) Computer Law & Security Review. Advance access: https://doi.org/10.1016/j.clsr.2020.105414 .

[230] Ibid, p. 19.

[231] Ibid, p. 19.

[232] Ibid, p. 4.

[233] UN General Assembly, Optional Protocol to the International Covenant on Civil and Political Rights, 19 December 1966, United Nations, Treaty Series, vol. 999, p. 171, Article 2.

[234] For example, the UN ICCPR remains a pertinent Convention to start (or continue) with, but also other Conventions should be taken into consideration, especially when they dialogue or interact with data protection and privacy (even if inferred), such as the Convention on the Rights of the Child, the Convention to Eradicate any Form of Discrimination against Women, among others.