Chapter 19

Now You See Me: Privacy, Technology, and Autonomy in the Digital Age

Valerie Steeves

Learning Objectives

- To become familiar with the range of national and international instruments designed to protect privacy.
- To understand the ways in which the bureaucratic desire to maximize efficiency and the commercial monetization of personal information have constrained human rights protections for privacy.
- To understand current privacy issues around national security surveillance, the corporate collection of data, and social media from a human rights context.

"Privacy Is Over"[1]

As the following examples illustrate, the past few years have been difficult ones for privacy. Edward Snowden's revelations about the Five Eyes[2] disturbed citizens and government leaders alike, especially after it was revealed that the United States was routinely listening in on phone conversations of the heads of state of its allies. German Chancellor Angela Merkel, whose own conversations had been surreptitiously monitored by the US National Security Agency (NSA),

responded by saying that "spying among friends" was "unacceptable."[3] Merkel also compared the NSA to Stasi, the ultra-repressive East German security agency, which had collected detailed dossiers on virtually all its citizens during the Cold War.[4]

Google released its Google Glass[5] for beta testing by eight thousand "explorers." Literally with a blink of the eye, Google Glass wearers can activate a video function and record whatever they happen to see. Moreover, this information can be automatically shared with Google, adding to the growing digital footprint we leave behind us as we surf the Net, interact with various corporations, and – if Google has its way – walk by someone wearing Glass. The first to ban the device was the 5 Point Café, a Seattle dive bar. The bar's owner, Dave Meinert, argued that Glass's ability to constantly record the wearer's experiences violated the expectations of other people in the bar, because a bar was "kind of a private place." Casinos, educational institutions, and some municipalities soon followed suit. As privacy lawyer Timothy Toohey noted, "This is just the beginning ... Google Glass is going to cause quite a brawl."[6]

North of the border, Canada joined a growing number of countries criminalizing "revenge porn," in which disgruntled ex-partners – almost always men – post intimate pictures of their former girlfriends on the Web as a form of social shaming.[7] Tacked on to the Canadian legislation were provisions that greatly expanded the police's ability to collect information about citizens from Internet service providers without a warrant. These so-called lawful access provisions had been defeated in Parliament on three previous occasions, the last time after more than 150,000 Canadians signed a petition condemning police online spying.[8] Both the mother of Amanda Todd, a British Columbia teen who committed suicide after a partially nude picture of her was distributed online, and Ontario's Information and Privacy Commissioner, Ann

Cavoukian, called on the government to stop using child victims of crime as a smokescreen behind which to invade people's privacy.[9] The legislation passed nonetheless.

Developments such as these have led many to conclude that privacy is dead. However, in spite of the recurring obituaries, people continue to push back against new surveillance practices, for a variety of reasons. Critics worry that overzealous national security initiatives such as Five Eyes threaten to upset the democratic balance between citizen and state. Commercial practices such as Google Glass, which collectively record up to 75,000 individual data points on each consumer per day,[10] can constrain our ability to make choices for ourselves, especially when people are sorted into categories for preferential or discriminatory treatment based on their demographics. And constant monitoring of the intimate and mundane details that we post on social media challenges the traditional divide between our private lives and our public personas. As Canadian teens put it, all this surveillance is just plain creepy.[11]

This chapter examines the ways in which emerging information technologies – and the bureaucratic and commercial agendas behind them – have shaped and constrained our experience of privacy since the United Nations first enshrined a right to privacy in the Universal Declaration of Human Rights (UDHR) in 1948. We explore how, with the advent of mainframe computing in the 1960s and 1970s, new methods of collecting, storing, and using personal information raised serious concerns about privacy. However, the same period was marked by growth of government bureaucracy in Europe and the monetization of personal information in North America. I argue that those two factors worked to reframe privacy protection, through the creation of regulatory mechanisms designed to legitimize the ways in which both the public and private sector use increasing amounts of information about us for their own purposes. Privacy was accordingly recast as a matter of individual control over the collection, use, and disclosure of personal

information; and the broader links to human dignity and personality in the UDHR were subsumed in the procedural mechanisms of informational control.

A Brief History of Privacy

Discussions of privacy often start by noting that privacy has been an elusive concept to define. Privacy advocates seek to protect privacy because, as a fundamental human right and an essential part of democracy, it is a good in itself. However, communitarians and information collectors such as governments and corporations often argue that privacy detracts from other legitimate social goals, such as government efficiency, economic growth, and the creation of knowledge. Bennett notes that "over thirty years of semantic and philosophical analysis ... leaves [one] with the overwhelming sense that privacy is a deeply and essentially contested concept," grounded in "questionable assumptions" about the individual, civil society, and the state, and "it is those very assumptions that require careful interrogation if the 'politics' of privacy are to be unearthed."[12]

Certainly over the past century, much of the political struggle around privacy has been triggered by new technologies. Warren and Brandeis, who popularized the classic definition of privacy as "the right to be let alone" in 1890, were writing in response to their concerns that the newspaper industry was using the new technology of photography to capture and publish images of private individuals. By the mid-1960s, concerns about the effect of other new technologies on privacy had again come to the forefront and were generating what Regan calls a "literature of alarm."[13] A plethora of popular literature of the day worried that communication technologies, such as listening devices and telephone taps, enabled the state to eavesdrop on conversations that were previously protected by the physical barriers between private and public spaces. The information management capacities of computerized databases also raised concerns that the

ability of governments and corporations to monitor large populations would inexorably erode democratic governance and individual autonomy.

Privacy protection accordingly took to the legislative stage in most developed countries in the 1970s. Legislators sought to enact a set of procedural protections based on Alan Westin's popularization of privacy as individuals' right "to determine for themselves when, how and to what extent information about them is communicated to others."[14] Westin's definition was subsequently taken up by more than eighty-five countries,[15] and his set of data-protection principles[16] now dominates privacy law worldwide.[17]

However, the concerns of the time were rooted not in technological change but in the events that had occurred twenty-five years earlier. Europeans in particular were sensitive to the ways in which central recordkeeping had facilitated the identification and exportation of Jewish people during the Nazi occupation of Europe. Accordingly, the promise of faster, more efficient computerized recordkeeping raised the spectre of mass deportation and oppressive social control. [18] In his seminal work on the history of data protection, Flaherty provides an interesting window on the attitudes of the day: "the development of computer and data banks has aroused elemental anxieties. In England in particular, such sentiments are fuelled by the presence of individuals who have lived under totalitarian regimes and who fear the potential abuse of data banks by governments or invading forces ... [Abuse of population registries] is a common fear in European countries that suffered under Nazi occupation, or were seriously threatened by it."[19]

Because of the legacy of the Second World War, the postwar international community concluded that "disregard and contempt for human rights ... resulted in barbarous acts which have outraged the conscience of mankind,"[20] and came together through the United Nations to adopt the Universal Declaration of Human Rights, on 10 December 1948. The Declaration

expressly provides for protection of privacy. Article 12 declares: “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.”

Privacy is also indirectly protected through provisions guaranteeing the right to life, liberty, and security of the person and to freedom of thought, conscience, and religion. The right to freedom of religion expressly includes the right to practise a religion or belief in public or private. The Declaration also lays the groundwork for respect of privacy as a social right tied to the right to free development of personality.

When the Council of Europe first passed the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1950, it incorporated similar privacy rights in articles 8 and 9, subject to such limitations “as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.” And when the United Nations adopted the International Covenant on Civil and Political Rights in 1966, once again protections for privacy that mirrored the provisions of the UDHR were included.

The language used in these instruments created a broad legal right to privacy and cast that right as an essential element of human dignity, freedom, and the democratic process. Thus legal protections for privacy that flowed from the experiences of the Second World War recognized privacy as a fundamental human right, and protected it accordingly.

When legislators again picked up the privacy portfolio in the 1970s, they placed their concerns about new information technologies in this context. The 1973 report of the US

Department of Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems is typical:

> Most of the advanced industrial nations of Western Europe and North America share concerns about the social impact of computer-based personal data systems ... The discussions that have taken place in most of the industrial nations revolve around themes that are familiar to American students of the problem: loss of individuality, loss of control over information, the possibility of linking databases to create dossiers, rigid decision making by powerful, centralized bureaucracies.[21]

Accordingly, early interest in privacy legislation on the part of the public, the United Nations, and the Council of Europe focused on socio-democratic issues, such as the impact of new technologies on individuality and freedom, and on the exercise of bureaucratic or governmental power. These concerns were shared by scholars who were "motivated by a desire to build institutional and cultural barriers against the comprehensive monitoring of private life that appeared – before the Second World War and later, during the Cold War years – as a necessary condition for the functioning of totalitarian or authoritarian regimes."[22]

However, data protection was not necessarily a good fit with broader concerns about dignity, autonomy, and the promotion of human rights. In fact, the first jurisdiction to enact data protection legislation, the German state of Hesse, was motivated by a very different set of concerns. Under German constitutional law, state and federal laws are administered by local authorities. State governments were using computers to centralize their information gathering and processing, and local governments worried that this centralization would in effect transfer the power and influence traditionally held by local authorities to the state bureaucracy. For its

part, the state legislature was concerned that data processing would enhance the executive's power, especially if the legislature were cut off from information held in computers owned and operated by the state bureaucracy.[23]

Data-protection laws were accordingly introduced in Hesse in 1970, not to protect privacy but to settle an ongoing dispute between bureaucrats and politicians over which level of government would enjoy the power that came with computerized control of citizens' information. Data protection was accordingly seen as a tool to enhance state power and control; the various levels of government competed for access to data processing to enhance their own effectiveness and wished to set out basic ground rules to protect administrative turf.

Citizen concerns about confidentiality and privacy remained an important thread as the fabric of the legislative program was woven. However, the Hesse act demonstrates that data protection laws were enacted because they are consistent with bureaucratic and political interests in safeguarding their respective spheres of power. The rights of a citizen to access and correct his or her data are also consistent with the administrative need for data integrity: citizen oversight of records safeguards the data itself and helps ensure that the information used for policymaking and administration is indeed accurate.

When Sweden became the first national government to pass data protection legislation, three years later, it was both the most computerized country in the world and the country with the most extensive routine surveillance in Europe. Flaherty called it "the model surveillance society in the Western world, because of its high degree of automation, the pervasiveness of personal identification numbers to facilitate record linkages, and the extent of data transfers between the public and private sectors."[24] He concluded: "Sweden illustrates the kind of surveillance society

that results when record linkages are so easy to accomplish that the power holders cannot resist using them to try to solve real and alleged social problems."[25]

Although citizen concerns about automation of the 1970 census raised questions about privacy, the Swedish government's interest in data protection was rooted in a desire to protect Sweden's national sovereignty against the possibility of its automated population registers falling into the hands of a foreign power. A study published in 1976 by the Swedish Ministry of Defence summarized these concerns well:

> A possible aggressor, who is trying to gain effective and complete control of the population when engaged in acts of war on Swedish territory, may find it necessary to have access to population registers. This assumption is confirmed by experience from the Second World War ... Sweden has ten or so computerized central population registers. In most cases these registers contain very detailed information which would be extremely valuable for a possible aggressor aiming to establish control of Swedish territory.[26]

Moreover, data protection was seen by Swedish authorities as a way to ensure that data would continue to flow to the state, by quelling citizen concerns about the privacy of automated census data. As the National Tax Board put it, "coming under surveillance is a privilege,"[27] and "the population should themselves feel that there is a good reason for being recorded in the population registration system ... that [it] simplifies life for them and is an efficient support in achieving a correct distribution of social rights and obligations."[28] From this perspective, data protection was a tool to legitimize state collection of information – to advance ongoing state surveillance more than to protect privacy.

When the Council of Europe (COE) enacted privacy rules two months after Sweden passed its legislation, it returned to the human rights roots underlying citizen concerns. The Resolution of the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector (the "Private-Sector Resolution") was its response to an earlier report by the Council's Committee of Experts on Human Rights, which concluded that the law of the time did not provide sufficient protection for citizens against intrusions by technical devices, especially because international covenants applied only to public authorities and did nothing to restrict intrusive practices on the part of private organizations. Although the COE resolution adopted a set of data-protection principles, those principles were contextualized by broader statements rooted in the Council's commitment to human rights. For example, the annex to the Private-Sector Resolution states that information about intimate private life should not be collected, because it might lead to unfair discrimination, and the explanatory report suggests that member states should enact provisions to limit the types of data that can be collected.The COE's primary interest in filling the gap in the law to restrict the negative effects of surveillance technologies was bracketed by competing interests in greater political integration across Europe and administrative modernization. Nonetheless, the Private-Sector Resolution subordinated managerial imperatives – to collect and use large amounts of information to manage risk – to the need to protect individual privacy and autonomy.

Interestingly, when the COE passed its Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector (the "Public-Sector Resolution") the next year, concerns about privacy as a human right were notably absent. The preamble to the Public-Sector Resolution did not mention the need to protect individuals from potential abuses. Instead it expressly stated that the Resolution was intended to promote greater political

integration among member states, by contributing to "public understanding and confidence with regard to new administrative techniques which public authorities in the member states are using in order to ensure the optimal performance of the tasks entrusted to them." The "problems" the Resolution sought to resolve were no longer grounded in historical memory of the Holocaust; instead it was intended to allay public anxiety about new technologies so that governments could continue to use these technologies as they emerged:

> Public anxiety has arisen not because many abuses of information technology have actually been discovered but rather from the possibility of abuse ... the discussion is apt to flare up on the occasion of each new project for the use of information technology. In this connection, it should be kept in mind that the success with which computers can be used to public affairs will depend very much on the degree of confidence the public is willing to give to their use.[29]

The Public-Sector Resolution accordingly took on a pedagogical role, seeking to allay public concerns by "sufficiently informing" citizens about new technologies in order to manufacture public trust in emerging administrative practices. In other words, data-protection laws were less about protecting people from growing surveillance and more about legitimizing that surveillance through the adoption of procedural rules. As the Preamble stated, data surveillance "should be regarded as a positive development. The purpose of the present resolution is not to oppose such use but to reinforce it with certain guarantees."

This shift away from a human rights perspective of privacy, to a focus on managerial efficiency and the legitimacy of surveillance practices, did not occur in a vacuum. As Burkert writes, "Right from the outset, the concept of data protection in Europe was not merely a European affair. American international companies and their subsidiaries ... conveyed the

American view on regulation and on privacy regulation in particular."[30] From the American perspective, any restriction on the flow of personal information constitutes a trade barrier. American policy is accordingly shaped less by the managerialism evident in the European Union and more by a desire to free technological innovation and trade from cumbersome regulatory mechanisms.

Subsequent international efforts to protect privacy have been heavily influenced by this position. For example, the influential Organisation for Economic Co-operation and Development's Guidelines on the Protection of Personal Privacy and Transborder Flows of Personal Data, passed in 1980, contains a set of data protection principles. The Guidelines also ask member states to "take all reasonable and appropriate steps to ensure that transborder flows ... are uninterrupted and secure" and to avoid passing domestic legislation "in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

The importance of the uninterrupted flow of information in the international marketplace was later underlined in the OECD's Declaration of Transborder Flows in 1985. The Declaration states that these flows are "an important consequence of technological advances and are playing an increasing role in national economies." Since "computerized data and information now circulate, by and large, freely on an international scale" and this circulation brings "social and economic benefits resulting from access to a variety of sources of information and of efficient and effective information services," OECD member states agreed to "promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information."

Thus the OECD Guidelines were at least in part intended to promote the flow of personal data between states to enhance trade and promote efficiencies. Again data protection was perceived to be consistent with these goals. Indeed, the admonition in section 18 – to avoid laws "in the name of the protection of privacy and individual liberties" that would obstruct the flow of personal data – implies that data protection was adopted because it minimizes the risk to economic and bureaucratic goals that could be posed by privacy legislation based on a perspective other than data protection.

In 1981 the Council of Europe opened its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data for ratification. Although the Convention applies only to the automated processing of personal data, its provisions are very similar to the OECD Guidelines. In addition, both processes were influenced by the American perspective. As a member of the OECD, the United States took an active role in drafting the Guidelines, and the COE Convention "received special wording to provide for the unlikely event that the US would join."[31]

The Convention again enacts a set of data protection principles in an express attempt to "reconcile" the "fundamental value" of privacy with the "fundamental value of ... the free flow of information" (preamble). Although the Convention does not suggest that an organization has a right to access an individual's personal information that is co-equal with the individual's right to privacy, it does imply that organizational access is a competing interest of equal importance. This is inconsistent with the COE's strong statements in 1973 against managerial practices that create dangers to privacy, and shows how the Council's original concerns about the potential negative impact on individual autonomy and human rights had been eclipsed by managerial demands and commercial imperatives to access data, regardless of citizen expectations of privacy.

This "process of forgetting" is also evidenced by the priority that the Convention gives to the free disclosure and exchange of personal information. Article 12(2) provides that "[a] party shall not, *for the sole purpose of the protection of privacy,* prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party" (emphasis added). This is a surprising statement from a human rights perspective, as it implies that a state is prohibited from restricting the flow of data to a fellow signatory to the Convention solely because the restriction is required to protect privacy. And, like the other instruments we have examined, the Convention builds in significant exceptions to data protection requirements for the purposes of security, public safety, crime control, statistics, and scientific research. However, the Convention's list of exceptions in article 9 also includes data required to promote "the monetary interests of the state." It is difficult to conceive of restrictions being placed on other human rights – such as the right to free speech or security of the person, for example – justified solely on the basis of fiscal benefits.

The importance of commercial surveillance continued to shape privacy policy after the 1981 Convention. By the late 1980s the European Union had become concerned that lack of a uniform approach to privacy across Europe could impede the free flow of personal data across borders and make trade more difficult, both within Europe and between Europe and North America. Accordingly, when the EU enacted its Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data in 1995, it called on member states to adopt data protection laws as a way of promoting trade.

The Directive was also a key part of a policy structure developed to support the "information superhighway," and as such it sought to create social and political conditions conducive to the adoption and mass implementation of new technologies. Like the Council of

Europe before it, the EU was concerned that consumers would not adopt e-commerce unless they were confident that there were rules protecting their personal information. The Directive reflected the "perception, enunciated from the highest circles of government and inter-governmental policy-making, that trust and trustworthiness were key elements of the climate in which [e-commerce] initiatives would flourish."[32] Once again privacy policy took on a pedagogical role; instead of reflecting citizen concerns about the protection of privacy as an essential part of human dignity and autonomy, it became a tool with which to reconstitute those concerns and make them conducive to the prerogatives of bureaucratic efficiency and technological innovation.

As we see below, both of these trends – promoting managerial efficiency and freeing up trade and innovation – have influenced Canada's approach to privacy. They have, in turn, constrained the full protection of privacy as a human right.

Privacy in the Canadian Context

Although Canada played a key role in the drafting of the UDHR, human rights protections for privacy within Canada have been patchy at best. Canada is a signatory to the UN conventions discussed above, but the Canadian Charter of Rights and Freedoms does not contain a specific provision protecting privacy. The Supreme Court of Canada has attempted to fill the gap by using section 8 of the Charter (the right to be free of unreasonable search and seizure) to protect citizens from police surveillance when they have a "reasonable expectation of privacy." For example, the police cannot place a hotel room under surveillance unless they first obtain a warrant, because a warrantless search would violate the occupant's reasonable expectation of

privacy. On the other hand, the police may use video surveillance in a public washroom because the courts have said that people using the washroom do not have an expectation of privacy.

Part of the problem lies in the fact that, with the advent of new technologies, the police do not need to watch what occurs in private spaces; they can instead collect data about those spaces and use that data as a proxy to determine what is happening inside. For example, in *R. v. Tessling* (2004), the Supreme Court allowed the police to fly over Walter Tessling's house and use a forward-looking infrared camera to take a picture of heat escaping from the house. Although the police would not have been able to obtain a warrant to enter the house, because they only suspected that Tessling was operating a grow op, they were able to "look into" the house to see how many lights were on and where they were located. The Court allowed this because the heat pattern was only "information" about the house. Unlike bodily and territorial privacy, which are given a high level of protection by the courts, informational privacy is protected only if it involves a biographical core of personal information that the citizen would not wish the state to have access to. Information about heat escaping from lights does not meet that test, even though the house itself and the activities within it would have been protected if the police had entered the house.

But privacy has also lost ground. As data protection legislation diffused throughout many parts of the world, Canadian legislators also created laws that privileged managerial efficiency and trade over the broader meaning of privacy as a human right.

Canada's Privacy Act, which was passed in 1982, governs collection, use, and disclosure of personal information by the public sector. Although the Act gives Canadians rights to access and correct information held about them, section 4 indicates that information can be collected for any purpose that "relates directly to an operating program or activity of the [government]

institution." Moreover, the ability to control the collection is limited by vague language and exceptions to the general rules. Under section 5, the individual must be advised of the purpose for collection, but only when the information is collected directly; indirect collection is allowed whenever direct collection is not possible. However, neither requirement applies when it *might* "result in the collection of inaccurate information" or "defeat the purpose or prejudice the use for which information is collected." Thus the government can legally collect personal information without the individual's knowledge or consent, and the test to determine whether or not it even has to notify the individual is the mere possibility that notice might prejudice the use of the data as defined by the government.

The case of *Smith v. Attorney General of Canada* (2001) is a good example of how this can defeat a broader understanding of privacy as a human right and the link between privacy and human dignity and autonomy. Smith was accused of committing fraud because her data showed up in both the employment insurance database and the customs database. The government was routinely matching the data between the two in an attempt to catch "cheaters" who were travelling outside the country while collecting employment insurance benefits. The Privacy Commissioner of Canada argued that this constituted unreasonable search and seizure because it treated every Canadian traveller like a criminal suspect, in effect allowing the state to place citizens under surveillance on the off-chance that they were committing an offence. The Supreme Court disagreed and held that any reasonable expectation of privacy on the part of a traveller did not outweigh the government's need to ensure that people are complying with the law.

The most interesting aspect for our purposes is that the government had consulted with the Privacy Commissioner before beginning the data-matching program. The Commissioner had indicated that the practice would have serious implications for privacy, because that kind of

"fishing expedition" – traditionally viewed as an abuse of power – potentially impairs the citizen's dignity and autonomy. The government rejected the Commissioner's advice because the matching program was a highly efficient tool for bureaucrats administering the employment insurance program and complied with the narrow data protection provisions included in the Privacy Act. This, in effect, privileged the government's desire to access personal data because it was an efficient way of administering a government program and ignored broader concerns about privacy as a human right.

The same concerns about bureaucratic efficiency drove much of the discussion when Canada passed its data protection legislation for the private sector. However, the Personal Information Protection and Electronic Documents Act (PIPEDA), which was enacted in 1999, was also a direct response to the EU's Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of Such Data. The absence of data protection rules was seen as a barrier to trade with Europe, and PIPEDA was pursued as a way to both open up trade and build consumer trust on the part of Canadians. For example, the discussion paper that preceded the legislation argued that data protection laws were needed to "strike the right balance between the *business need* to gather, store, and use personal information and the *consumer need* to be informed about how that information will be used." Data protection was accordingly seen as an essential element "of building the consumer trust and the market certainty needed to make Canada a world leader in electronic commerce."[33] In addition, PIPEDA itself was based on the results of negotiations among industry, government, and consumer group stakeholders. Like the Privacy Act before it, contains a long list of exceptions to ensure that the data protection rights given to consumers do not reduce the efficiency of conflicting goals, such as policing, research, administration, or e-commerce.

In this chapter I have argued that the desire to promote these conflicting goals has reconstructed the strong protections for privacy first articulated in the UDHR as a set of procedural protections that give individuals limited rights to access and correct the information that governments and corporations use to make decisions about them. The proof may be in the pudding. As the report *Transparent Lives: Surveillance in Canada* makes clear, surveillance has grown exponentially in Canada since PIPEDA was enacted.[34] The report also notes that the line between the public and private sectors is becoming increasingly blurred: information that cannot be legally collected by governments (because to do so would violate section 8 of the Charter) is routinely collected by corporations and then shared with governments, without warrants or any other kind of accountability mechanism. Moreover, our privacy is increasingly constrained by "smart" technologies like the camera that captured the heat patterns of Tessling's house, technologies that record the GPS locations of our cellphones, our use of electronic bus passes, the photos and comments we post on social media, and our faces as they are captured on closed-circuit television security cameras. And all of this information is collected so that others – governments and corporations – can make decisions about the kinds of benefits and services we are entitled to enjoy.

Back to the Beginning: Protecting Privacy as a Human Right

Our brief review of the history of privacy protection indicates that privacy rights as set out in the UDHR were expressly linked to human dignity and autonomy. The UDHR also acknowledged the important role that privacy plays in allowing us to enjoy other human rights; it is hard to

exercise our freedom of speech or association when everything we say and do is routinely and constantly monitored and then shared with governments and corporations.

Ironically, when the government first began talking about the need for PIPEDA in the late 1990s, a parallel process was initiated by the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities (HURAD) that expressed privacy protection firmly in the human rights language of the UDHR. HURAD conducted hearings and public consultations to explore legislative options that could account for the effect of new technologies; it concluded that, although data protection legislation was "clearly a critical part of the spectrum of privacy interest, in a world of increasingly intrusive technologies, it is by no means the only game in town."[35]

HURAD argued that truly effective privacy protection can be sustained only if the value of privacy as a human right is given greater weight than the bureaucratic efficiencies and economic benefits of an unconstrained flow of personal information. To do this, it recommended that the government enact a privacy rights charter with quasi-constitutional status and require all federal laws to respect everyone's "physical, bodily and psychological integrity and privacy; privacy of personal information; freedom from surveillance; privacy of personal communications; and privacy of personal space."[36]

The proposed charter was intended to be "umbrella legislation" that would help guide the development and application of all federal laws, including data protection legislation. By giving the charter precedence over the latter, HURAD hoped to "capture the full breadth of privacy, like a wide angle lens taking in a panoramic view, as opposed to the data protection framework ... that focuses, like a close-up lens, tightly on informational privacy rights."[37] In making its

recommendations, HURAD drew expressly on the early work of the United Nations and the Council of Europe:

"Ultimately, [the privacy charter] is about taking privacy seriously as a human right. To do that, we must invoke recent history and remind ourselves *why* the right to privacy was entrenched in the UDHR and subsequent human rights instruments. Otherwise, we may be seduced into believing that privacy is simply a consumer rights issue that can be fixed by a few codes of conduct and some new, privacy enhancing technologies."[38]

A Privacy Rights Charter modelled on HURAD's recommendations was introduced in the Senate of Canada by Senator Sheila Finestone in 2000. However, the Charter died on the order table after the government refused to support it, because of fears that legal recognition of privacy as a human right would place many of the government's information practices in jeopardy. The Department of Justice's senior general counsel for public law policy, Elizabeth Sanderson, told the Senate Standing Committee on Social Affairs, Science, and Technology at the time, although the government was "sympathetic" to the Charter, legally protecting privacy as a human right "would create a good deal of uncertainty and quite possibly may pose obstacles to many government programs and policy":

> Let me give you a concrete example where the [Charter] could affect departmental legislation and operations. Citizenship and Immigration Canada (CIC) collects a great deal of personal information relating to immigration applications and to the enforcement of deportation orders and immigration offences. [The Charter] would potentially require CIC to defend its information gathering and sharing activities in court ... In conclusion, while [the Charter] can be praised as intending to enhance the privacy of Canadians, the devil may be in

the detail. Changes could come *at the expense of certainty, public safety, operational efficiency and fiscal responsibility.*[39]

Ongoing Conflicts Between Efficiency and Innovation and Privacy

So whither the human right to privacy? Canada remains a signatory to the UDHR, but its domestic legislation largely ignores the human rights impact of new surveillance technologies. Public policy continues to promote bureaucratic efficiency and trade over privacy, and legal reforms to data protection legislation, both PIPEDA and its provincial counterparts, have only added to the long list of exceptions that allow organizations to sidestep the procedural protections that data protection offers.

Most recently, the government proposed changing the law to enable organizations to voluntarily disclose personal information to any other organization for the purpose of investigating a breach of an agreement, and to protect organizations from legal liability for releasing personal information.[40] Both of these changes would make it easier for organizations to share personal information without the individual's knowledge or consent. What is perhaps most perplexing about these amendments is that they were proposed at a time when citizen concerns about privacy were at an all-time high, especially after it was revealed that, even without the amendments, the government asks telecom companies to voluntarily release personal information about their subscribers approximately 1.2 million times each year. As Geist notes, "It is not Canadians who have given up on privacy. It is the Canadian government."[41]

However, a number of advocacy groups continue to challenge these kinds of practices by using human rights language to frame the issues. For example, the International Campaign

Against Mass Surveillance was launched in 2005 by more than a hundred civil-society groups, including the American Civil Liberties Union, the International Civil Liberties Monitoring Group, and Statewatch. The campaign declaration calls on governments to "stop the wholesale, indiscriminate collection and retention of information on citizens, including the acquisition of databanks from private companies," because they "erode or are contrary to existing data protection, privacy and other human rights laws and standards."[42] From this perspective, the fact that data collection conforms to procedural rules is not enough to legitimize it; the test is whether or not it complies with the human rights obligations articulated in international instruments such as the UDHR.

As Ursula Franklin notes, the choice of language is particularly important:

> When human rights informs the language in which the discussion among you and the general public and Parliament takes place, you speak then, rightfully about citizens and all that comes with that. On the other hand, if the emphasis is primarily on the protection of data, one does look at a market model, one does look at an economic model, and all the things you've heard about the new economy. Then it is the language of the market than informs your discourse.[43]

Let's return to the three examples set out at the beginning of this chapter to see how human rights language opens up opportunities for legal responses that go beyond data protection and take human dignity and autonomy into account more fully.

Five Eyes surveillance has been universally condemned in the press as invoking Big Brother politics – precisely the kind of thing the drafters of the UDHR were concerned about – but spy agencies continue to maintain that their practices are legal. The broad exemptions contained in data-protection legislation certainly enable companies to cooperate with government

spying programs. Nonetheless, when Edward Snowden was defending his actions as a whistleblower, he called on:Article 12 of the Universal Declaration of Human Rights, and numerous statutes and treaties [that] forbid such systems of massive, pervasive surveillance. While the US Constitution marks these programs as illegal, my government argues that secret court rulings, which the world is not permitted to see, somehow legitimize an illegal affair. These rulings simply corrupt the most basic notion of justice – that it must be seen to be done. The immoral cannot be made moral through the use of secret law.[44]

Canadian Federal Court Judge Richard Mosley agrees. In November 2013 he lambasted the Canadian Security Intelligence Service (CSIS) for deliberately misleading the Court so it could use Canadian warrants to get other members of the Five Eyes to spy on Canadians on foreign soil. One month later, the General Assembly of the United Nations passed the Resolution on the Right to Privacy in the Digital Age. In it, the Assembly states that it is

> [d]eeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights ... [and] calls upon states to respect and protect the right to privacy, including in the context of digital communications [and] to take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law.

Google Glass continues to be a subject of controversy, especially because it underlines how pervasive commercial data collection has become. Google Glass illustrates how “smart”

environments, replete with sensors, create a leaky environment. The platforms on which we play, work, and shop and the devices we carry share information about us promiscuously on an ongoing basis, often in the background and outside our control. Moreover, private-sector interests in marketing and the commodification of online social interactions, on the one hand, and public-sector concerns about efficiency and risk reduction, on the other, have combined to create a system in which decisions about us are routinely made on the basis of data collected about us. These "data shadows" are used to profile us, both for benefits and as risks, in essence automating discrimination in new and disturbing ways.

Data protection rules have been insufficient to curb this because they fail to examine the purposes of the collection. Although organizations are required to collect and use data only for the purposes they specify, broad and largely meaningless "purposes" such as "optimizing your user experience" have consistently been accepted by data protection regulators. Once collection is legitimated by a transparent goal of this type, any discrimination based on how the data is used to profile the individual recedes into the algorithm; it becomes increasingly difficult to challenge the kinds of disadvantages that are reinforced by the sort.

In order to challenge this practice, in May 2014 a group of privacy advocates issued the Ottawa Statement on Mass Surveillance in Canada. They noted "[t]hat there is extensive targeting and profiling of individuals and groups on grounds of race and ethnicity, political and religious views, social class, age, gender, sexual preference and disability; [and that] Canadian privacy and data protection laws and regulations are regularly bypassed, undermined or broken, and are inadequate for dealing with information and privacy rights in the age of big data and ubiquitous surveillance."[45]

To rectify the situation, they called upon government to "fully respect the Canadian Charter of Rights and Freedoms including the right to privacy, freedom of thought and expression, freedom of association and peaceful assembly, and security against unreasonable search and seizure."[46]

"Revenge porn" illustrates how information available on networked media can cause harm to a person's reputation, even when the information is true. Online providers such as Google typically resist deleting this kind of content. However, in 2014 the Court of Justice of the European Union held in favour of a Spanish man who was embarrassed by online references to social security debts he had incurred in 1998. The Court determined that individuals are entitled to have irrelevant or excessive information about them excluded from the Internet giant's search results, unless there is a public interest that militates against it.[47] Within one day of making the service available, Google received twelve thousand requests to block information.

Conclusion

In each of the above cases, the language of human rights was used to expand upon the protections offered by data protection and to reassert the importance of privacy to the democratic process and to human dignity and autonomy. Human rights instruments were referenced to challenge the bureaucratic and commercial imperatives that lie at the base of many government and corporate information practices.

Meeting the challenges posed by networked technologies will not be easy. However, the "panoramic lens" of human rights can help us move beyond narrow procedural rules and consider more deeply the kind of society we want to be. Data protection is a part of the puzzle, but it is privacy as a human right that will provide the big picture.

Takeaway Messages

• Privacy rights are central to individual autonomy and dignity.

• Effective privacy protection must go beyond data protection and interrogate the impact of surveillance practices on privacy as a human right.

Study Questions

• Privacy has been variously defined as the right to be let alone, the right to control what personal information others know about you, and the right to a private life. Which definition is the most compelling to you, and why?

• Google collects every email you send or receive through Gmail and uses it for a variety of purposes, including selling information about you to advertisers. Does this practice violate your privacy? Why or why not?

Issues for Debate or Roundtable

• Given the popularity of social media, is privacy something that people continue to value?

• The right to ask a search engine to delete links to irrelevant or excessive information about oneself is sometimes called "the right to be forgotten." Is there a public interest in providing people with ongoing access to such information? Does deleting the links to the information violate the poster's right to free expression?

Additional Reading

Humphreys, Stephen. *Navigating the Dataverse: Privacy, Technology, Human Rights*. Geneva: International Council on Human Rights Policy, 2011.

<bok>Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.</bok>

Websites

Canadian Internet Policy and Public Interest Clinic. https://www.cippic.ca/.

Electronic Privacy Information Centre. https://epic.org/.

OpenMedia. https://openmedia.ca/.

Privacy International. https://www.privacyinternational.org/.

Notes

1. T.L. Friedman, "Four Words Going Bye-Bye," *New York Times*, 20 May 2014, http://mobile.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html?from=mostemailed&_r=0.

2. "Five Eyes" refers to the United States, the United Kingdom, Canada, Australia, and New Zealand, which have signed a multilateral agreement to cooperate in signals-intelligence gathering. Edward Snowden released documents indicating that the Five Eyes countries circumvent laws that restrict their ability to spy on their own citizens by asking one of the other members to do it for them, and that American and Canadian intelligence agencies routinely collect telephone and Internet records en masse from corporations such as Google, Facebook, and Verizon.

3. L. Baker and A. Rinke, "Merkel Frosty on the U.S. over 'Unacceptable' Spying Allegations," Reuters, 24 October 2013, http://news.yahoo.com/germany-france-unite-anger-over-u-spying-accusations-094005929.html.

4. I. Traynor and P. Lewis, "Merkel Compared NSA to Stasi in Heated Encounter with Obama," *The Guardian*, 17 December 2013, http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama.

5. A pair of glasses without lenses but with a tiny computer attached to the frame that can access networked media and record sound and video.

6. D. Streitfeld, "Google Glass Picks Up Early Signal: Keep Out," *New York Times*, 6 May 2013, http://www.nytimes.com/2013/05/07/technology/personaltech/google-glass-picks-up-early-signal-keep-out.html.

7. Bill C-13, *Protecting Canadians from Online Crime Act*, 2nd Session, 41st Parliament, 62–63 Elizabeth II, 2013–2014.

8. OpenMedia, https://openmedia.ca.

9. M. Geist, "From Toews to Todd: The Unravelling of the Government's Online Privacy Laws," *Huffington Post*, 26 May 2014, http://www.huffingtonpost.ca/michael-geist/carol-todd-privacy-bill_b_5393244.html.

10. J. Gerstein and S. Simon, "Who Watches the Watchers? Big Data Goes Unchecked," Politico, 14 May 2014, http://www.politico.com/story/2014/05/big-data-beyond-the-nsa-106653.html.

11. V. Steeves, *Young Canadians in a Wired World, Phase III: Experts or Amateurs? Gauging Young Canadians' Digital Literacy Skills* (Ottawa: MediaSmarts, 2012), 64.

12. C. Bennett, "The Political Economy of Privacy: A Review of the Literature," paper prepared for the DOE Human Genome Project, Center for Social and Legal Research, University of Victoria, BC, 1995, 2.

13. P. Regan, *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995), 13.

14. A. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 7.

15. G. Greenleaf, "Global Data Privacy Laws: 89 Countries, and Accelerating," *Privacy Laws and Business International Report* 115 (February 2012).

16. Data-protection principles require that organizations collecting personal information be accountable for their handling of the information; identify the purpose for collection and use; obtain the information with the data subject's knowledge and/or consent; collect only information that is relevant to the purpose; use the information only for the stated purpose; retain the information only for as long as is needed for the stated purpose; ensure that the information is accurate; keep the information secure; be open about their information practices; and provide the data subject with access to the information it has collected about him or her. Data-protection laws require organizations to comply with some or all of these practices; C. Bennett and C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2006).

17. Bennett and Raab, *Governance of Privacy*.

18. D. Flaherty, *Privacy and Government Data Banks: An International Perspective* (London: Mansell, 1979), 44; H. Burkert, "Privacy – Data Protection: A German/European Perspective," in *Governance of Global Networks in the Light of Differing Local Values*, ed. C. Engel and K.H. Keller (Baden-Baden: Nomos, 2000), 60.

19. Flaherty, *Privacy and Government Data Banks*, 44.

20. United Nations, Universal Declaration of Human Rights, preamble.

21. US Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (Washington, DC: HEW, 1973), appendix B.

22. Bennett and Raab, *Governance of Privacy*, 23.

23. Burkert, "Privacy – Data Protection," 44–45.

24. Flaherty, *Privacy and Government Data Banks*, 4.

25. Ibid., 94.

26. Sweden, Ministry of Defence, Secretariat for National Security Policy and Long Range Defence Planning, *Report* (Stockholm, 1976).

27. G. Persson, "Computerized Personal Registers and the Protection of Privacy," *Current Sweden* 344 (1986): 2.

28. Sweden, National Tax Board, "Population Registration in Sweden," brochure (Stockholm: National Tax Board, 2003).

29. Council of Europe, Resolution on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, (74) 29, Explanatory Memorandum, para. 5.

30. Burkert, "Privacy – Data Protection," 65–66.

31. Ibid., 66.

32. Bennett and Raab, *Governance of Privacy*, 79.

33. Industry Canada and Department of Justice, Task Force on Electronic Commerce, *Building Canada's Information Economy and Society: The Protection of Personal Information* (Ottawa: Public Works and Government Services Canada, 1998): 3 (emphasis added).

34. C.J. Bennett, K.D. Haggerty, D. Lyon, and V. Steeves, *Transparent Lives: Surveillance in Canada* (Edmonton: Athabaska University Press, 2014).

35. Canada, House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where Do We Draw the Line?* (Ottawa: Public Works and Government Services Canada, 1997), 24.

36. Ibid., 45.

37. Ibid, 44–45.

38. Ibid., 72.

39. Canada, Proceedings of the Standing Senate Committee on Social Affairs, Science and Technology, Issue 25: Evidence, 20 September 2001, 25 (emphasis added).

40. See Parliament of Canada, Bill S-4, *Digital Privacy Act*, and Bill C-13, *Protecting Canadians from Online Crime Ac*t, 2nd Session, 41st Parliament, 62–63 Elizabeth II, 2013–2014.

41. M. Geist, "Why Has the Canadian Government Given Up on Protecting Our Privacy?" *Toronto Star*, 30 May 2014, http://www.thestar.com/business/2014/05/30/why_has_the_canadian_government_given_up_on_protecting_our_privacy.html.

42. American Civil Liberties Union, “Campaign Declaration: International Campaign Against Mass Surveillance,” https://www.aclu.org/technology-and-liberty/campaign-declaration-international-campaign-against-mass-surveillance.

43. Cited in House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy*, 34.

44. E. Snowden, “Edward Snowden’s Statement to Human Rights Groups in Full,” *The Telegraph*, 12 July 2013, http://www.telegraph.co.uk/news/worldnews/europe/russia/10176529/Edward-Snowdens-statement-to-human-rights-groups-in-full.html.

45. Transparent Lives: Surveillance in Canada, Ottawa Statement on Mass Surveillance in Canada,” 10 May 2014, http://www.surveillanceincanada.org/node/32.

46. Ibid.

47. *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, Court of Justice of the European Union, 13 May 2012.