Justice Centre Reports and Analysis | Luke A. Neilson

Digital ID, Surveillance, and the Value of Privacy | Part Two

Justice Centre for Constitutional Freedoms

August 9, 2023

Abstract

Digital ID (and other technologies with tracking and profiling capabilities) may be used by governments and partnering agencies to collect data about citizens. Among other problems, these technologies may threaten the privacy of their users. Personal informational privacy matters because it is necessary for the enjoyment of security, autonomy, and human dignity. When privacy is violated, users are exposed to data hacking and harmful state interventions, to a loss of expressive and investigative capacity, and to a loss of dignity. Privacy matters. Canadian law and public policy should protect personal privacy from the potential negative impacts of information technologies and from government overreach.

Acknowledgements

We thank our Justice Centre team of litigators, researchers, and communicators for contributing their insight and expertise to this report. We also thank the thousands of Canadians who have supported the Justice Centre with their financial resources. The Justice Centre is leading Canada in public policy and advocacy because of the generosity and vision of donors.

Updates to this report

This is Version 1.0 of Part Two of this report, which may be updated at any time with notice to the public via the Justice Centre website and social media channels.

Table of Contents

Executive Summary

Digital Identification has been described by governments as the digital or electronic counterpart to traditional identification documents, such as physical driver's licenses, passports, and healthcare cards.[1] There are approximately 2.3 billion digital ID apps in use today; this number is expected to rise to 4.1 billion by 2027.[2-3] Governments in Canada and across the globe would have these users believe that their smartphone, desktop, or micro-chipped digital IDs expose them to no more risks than familiar identification documents. Digital ID users are told that there are no risks (or that whatever risks exist can be managed effectively by the state) and immense benefits: security for individuals, inter- and intra-organizational efficiency, economic profitability, and a future of better and new partnerships between individuals, corporations, governments, and international entities.

There are benefits to digital ID, but there are also serious potential harms, which have not been adequately investigated or understood by governments or policy designers. Some governments use digital ID to limit access to information, track personal data, and develop complex profiles of users' personalities. Digital ID programs with tracking and profiling capabilities may expose Canadians to serious harms, including harms to privacy, security, freedom of expression, mobility, and equality. Many digital ID programs being proposed in Canada today will not be developed in Canada but instead through partnerships with entities that are neither accountable to Canada nor transparent about how those programs will be

[1] "Digital Credentials," Government of Canada, Accessed August 4, 2023, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html#:~:text=Digital%20credentials%20in%20Canada&text=Digital%20credentials%20offer%20Canadians%20the,interacting%20with%20government%20in%20Canada.

[2] "Active Digital Identity Apps to Surpass 4.1 Billion by 2027, As Third-Party Platforms Look to Leverage Civic Identity Systems," Juniper Research, February 27, 2023, https://www.juniperresearch.com/pressreleases/active-digital-identity-apps-to-surpass-4-1bn.

[3] Other sources say that there are currently 1.7 billion digital IDs in circulation but that the number is expected to grow to 5 billion by 2024. See: "Governments Digital Identity Credentials to Reach 5 billion by 2024 Backed by Mobile Biometrics," Biometric Update, June 9, 2019, https://www.biometricupdate.com/201907/governments-digital-identity-credentials-to-reach-5-billion-by-2024-backed-by-mobile-biometrics.

designed or how Canadian data will be managed. In many cases, information technologies like digital ID (including facial recognition, biometrics, Artificial Intelligence, and even social credit) structurally disadvantage individuals when they do not know when their information is collected, where it is stored, or how it is used, which erodes the possibility of informed consent. When such technologies are combined with (a) insufficiently robust privacy laws and (b) institutional apathy about the value of informational privacy, Canadians stand to lose. These technologies may be used to invade the privacy of Canadians, prioritize government interests, and create structural power imbalances between states and the citizens they are meant to serve.

Contemporary discussions about digital ID should centre around privacy. Unfortunately, the value of privacy has not been carefully articulated or defended in modern public policy debates or in the Canadian education system. Canadians do not, therefore, have an adequate response to governments when governments attempt to capture personal information about individual citizens. Some believe that privacy is valuable only to those with something to hide. This ignores the fact that privacy is necessary to preserve many important human values, including the possibility of intimacy and openness between spouses and family members, between friends, between counsellors and those they help, between lawyers and their clients, and between many other personal and professional relationships. But most importantly, privacy is necessary for the enjoyment of security, autonomy, and human dignity.

Every Canadian acknowledges the value of security,[4] which might be described as *freedom from threat*.[5] When governments collect unnecessary data about Canadians, that data is

[4] As a state of being. See: Jonathan Herrington, "The Concept of Security," 2012, https://jherington.com/docs/Herington_Ashgate-2012.pdf.

[5] Buzan, Barry. *People, States and Fear: The National Security Problem in* 21 *International Relations*, Sussex, Wheatsheaf Books, 1983.

exposed to illegal hacking, which imperils the security of Canadians. It is a truism that, if data exists, it can be hacked. It is also a truism that governments and their administrators sometimes use what they know about citizens to threaten their security (e.g., by violating rights). Further, every Canadian acknowledges the value of autonomy–the capacity to be independent, to pursue a self-determined course of action, and to be free from external manipulating forces. Sometimes, information technologies like digital ID are used to limit access to information, which undermines the capacity of individuals to make informed decisions. Technologies with surveillance capabilities may also have a negative impact on expression and may cause self-censorship to occur. When people know that their behaviours are being monitored (even when those behaviours are not illegal), people tend to be less expressive or honest and, therefore, less autonomous. Finally, every Canadian recognizes the value of human dignity–the inherent goodness and complexity of being human, a being which cannot and should not be captured or predicted by even the most sophisticated profiling technologies. When governments invade privacy, they undermine the possibility of the inviolate personality.

Digital ID is a clever ruse in most (but not all) cases. While the mere digitization of physical documents is a modest and beneficial proposal, governments will use digital ID for more than facilitating interactions between individuals, organizations, and governments. Digital ID (or related technologies) may be used to monitor the behaviours and personalities of millions within Canada and billions across the world. Privacy, and what depends on it–security, autonomy, and human dignity–will be the cost.

Introduction

In Part I of this report on digital ID, we explored the digital ID programs of Canada and six comparator jurisdictions across the world. Digital ID is a reality for the citizens of more than 70 countries today;[6] the number of adopters grows every year. This technology has been received with widespread enthusiasm by governments and private industry. Canadians hear promises that digital ID technologies and frameworks[7] will grow economies, efficiently facilitate partnerships between governments, industry, and individuals, and provide a higher degree of security and convenience for users than traditional identification documents could ever provide. Nonetheless, there are concerns about how digital ID programs (and the legal and economic frameworks in which these programs are embedded) will impact important human values, including the value we place on personal and informational privacy.

In Part I, we demonstrated that some digital ID programs may have a negative impact on the enjoyment of rights, freedoms, and privacy in Canada. Governments and partnering agencies within and beyond Canada are eager to see the adoption of digital ID, which they describe as a mere digital counterpart to traditional identification documents, e.g., physical licenses, passports, and healthcare cards. We showed, however, that there is a meaningful distinction between digital IDs that are (a) mere digital counterparts to traditional identification documents and (b) programs with tracking and profiling capabilities. The proposed programs surveyed in Part I (e.g., the Known Traveler Digital Identity program or the Pan-Canadian Trust Framework)

[6] "5 reasons for Electronic National ID Cards," Thales, March 29, 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/5-reasons-electronic-national-id-card.

[7] There is a distinction between "digital ID," "digital ID programs or frameworks," and "information technologies." The term "information technologies" refers to a set of hardware (e.g., computers, smartphones, or eye-scanners) and software (e.g., databases, applications, or networks) that are used to create, store, manage, and share electronic information. The term "digital ID" refers to an electronic identification document belonging to an individual user. The terms "digital ID program" or "digital ID framework" refer to the information technologies, policies, laws, and institutional behaviours that come together to make each individual digital ID work.

would allow governments and partnering agencies to capture unnecessary data about Canadians, including data about (e.g.) their behaviours, histories, transactions, bodies, and personalities. These programs generate significant concerns about rights and freedoms, the proper domain of government, and the value of privacy. Canadians should be wary of any technology (however convenient) that reduces their capacity to enjoy privacy. Privacy matters.

Why does privacy matter? The answer to this question is the focus of Part II of this report. Whereas Part I focused on key features of digital ID, and whereas Part I applied a suite of public policy analysis tools to the digital ID programs being proposed in Canada today, Part II focuses on why Canadians should be concerned about the findings of Part I. The fact that digital ID proposals present a threat to the privacy of Canadians is only concerning *if privacy is valuable*. What follows is a defense of *the value* of privacy. We argue that, when weighing the value of privacy against the values of boosting economic profitability, building new information pathways between government, industry, and individuals, and providing more convenient service experiences for Canadians, the value of privacy should be afforded more weight. Unfortunately, the value of privacy in a modern world has not been carefully articulated in debates about the appropriate use of technologies like digital ID. This report is designed to repair that gap in the conversation. It is also designed to equip ordinary Canadians with conversational tools for reasonably defending the value of their privacy against unreasonable invasions.

We advance a definition of privacy and suggest that privacy matters (where digital ID is concerned, at least) because privacy is necessary for the prevention of harm and the protection of important human values. We suggest that, when privacy is violated, the security, autonomy, and human dignity of Canadians is jeopardized. In other words, the enjoyment of privacy is linked to the possibility of enjoying security, autonomy, and dignity. Security is explicitly protected by Section 7 the *Canadian Charter of Rights and Freedoms*, and it is clear that many

other sections of the *Charter* (including Sections 2, 6, 7, and 15) have the preservation of autonomy and human dignity in mind.

Regarding security, we show that privacy violations expose Canadians to security concerns in two ways. First, we observe that any data collected about Canadians is susceptible to illegal hacking. When data is illegally hacked, Canadians are exposed to various harms, including information loss, identity theft, service disruption, and financial distress. It is worth pausing to consider whether the collection of Canadian data is sufficiently advantageous to warrant the risks associated with possessing that data in the first place. Second, we observe that governments sometimes use what they know about Canadians to expose them to various harms, including the harm of being illegitimately restricted from accessing essential goods and services. We consider various case studies in which Canadian provincial and federal governments have used (what should otherwise have been) private data of Canadians to intervene in their affairs and jeopardize their security. Regarding autonomy, we show that tracking and profiling digital ID programs (as with any surveillance technologies) have the potential to dampen the autonomy and expressiveness of Canadians. We suggest that surveillance programs (like some proposed digital ID programs) have a quieting effect on freedom of expression. We suggest that Canadians should be free from the oversight of overbearing states that collect data for their own purposes and not for any worthy benefit to Canadians. We also suggest that digital ID programs may be used to restrict citizens' access to information, which may prevent those citizens from accessing diverse viewpoints or information deemed harmful to state interests. Regarding human dignity, we show that tracking and profiling Digital ID programs have the potential to violate human dignity by treating the individual as a specimen or object of analysis rather than as a unique and inscrutable person. In other words, tracking and profiling programs have the potential to disrupt our ethical and constitutional notions that citizens are unique individuals whose beliefs and behaviours cannot (or ought not to) be studied, modelled, or predicted by their governments. Like many in the

information technology and ethics literature, we suggest that governments have a negative ethical obligation *not* to violate the human dignity of Canadians.

While the intangible value of privacy does not appear to rank highly among the more tangible values so often mentioned by governments and industry today (e.g., convenience, safety from domestic and international threats, etcetera), this is not to say that privacy is valueless. On the contrary, privacy is necessary for the enjoyment of much that is best and finest in our world and relationships with each other. *Today, the* value of privacy *has no advocate in modern public policy debates. Its value is unappreciated and, therefore, undefended.*

The value of privacy

It would be difficult to find a Canadian who did not value privacy to some extent. Most Canadians hold the intuition that "privacy is valuable." After all, most people prefer that the details of their intimate relationships, conversations, and thoughts remain hidden (at least to some extent) from public discovery. Most Canadians would like to be able to control information about themselves and believe that failure to control that information may result in harms to themselves or others. In this report, we adopt the common-sense understanding of informational privacy that first appeared in Warren and Brandeis' 1980 essay, "The Right to Privacy," where privacy is defined as "control over information about oneself" and as "the right to be left alone."[8] Do Canadians care about control over information about themselves or about the right to be left alone by the state?

[8] Myers, Cayce. "Warren, Samuel & Louis Brandeis. The Right to Privacy," 4 Harv. L. Rev. 193 (1890)." *Communication Law and Policy*, vol. 25, no. 4, 2020, pp. 519–22, https://doi.org/10.1080/10811680.2020.1805984.

A survey conducted for the Digital Identification and Authentication Council of Canada (DIACC) confirms this, finding that 91 percent of Canadians want control over their personal data collected by governments and that 86 percent of respondents want control over personal data collected by private organizations.[9-10] Further, Canadians care now more than ever about maintaining their privacy online. According to survey data collected by The Office of the Privacy Commissioner of Canada,

> Approximately nine in 10 Canadians (89%) are at least somewhat concerned about people using information available about them online to attempt to steal their identity, including almost half (48%) who said they are extremely concerned about identity theft. The proportion of Canadians concerned about identity theft has not changed since 2018. The vast majority of Canadians also are at least somewhat concerned about social media platforms gathering personal information that they (88%) or someone else (89%) posted online to create a detailed profile of their interests and personal traits. In addition, 88% of Canadians are at least somewhat concerned about how companies and organizations might use information available about them online to make decisions about them, such as for a job, an insurance claim or health coverage.[11]

Most Canadians are concerned about the security of their online identities, about companies and organizations developing sophisticated profiles of their traits, and about those profiles being cited as justification for limiting access to essential services or opportunities.

Not all Canadians are concerned about protecting personal information, however. One survey found that 38 percent of Canadians are willing to consent to organizations accessing their

[9] DIACC, "Digital ID and Authentication Council of Canada Research Finds Canadians Want Digital ID that is user-centric and aligns with their values," April 4, 2022, https://diacc.ca/2022/04/04/privacy-security-and-choice-drive-canadians-desire-for-digital-id/.

[10] These survey results may suggest that Canadians are more sceptical of private industry use of personal data than of government use of personal data. While industry use of Canadian data is not an object of study in this paper, many of the findings of this paper (and certainly the main ones) apply as well to industry as to government.

[11] Office of the Privacy Commissioner of Canada, "2020-21 Survey of Canadians on Privacy-Related Issues," March 10, 2021, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/.

private data whenever those organizations promised desirable goods or services in return.[12] The same survey found that 13 percent of Canadians are unconcerned about protecting their personal privacy.[13] We suggest that, even in cases where privacy is not violated *because the user has consented to that information being accessed*, the protection of privacy is still valuable. So, why is privacy valuable?

The question has generated many responses since privacy became a topic of legal, political, and academic discussion in the nineteenth century. Not everyone agrees with the premise of the question, and some believe that privacy is not valuable.[14] Others regard the concept *privacy* to be so fuzzy that no meaningful account of its value can be articulated.[15] Still others think that, however valuable privacy may be, the "ship has sailed," and privacy cannot be protected in our quickly evolving world of (e.g.) biometrics, facial recognition, smart phones, smart homes, and AI.[16]

Nonetheless, many within this literature hold that privacy is valuable because of a cluster of underlying values, such as property rights, autonomy, intimacy, democracy, liberty, dignity, or economic value. In other words, this approach is compatible with the view that privacy is valuable because privacy is necessary for maintaining our other values, or that we could not enjoy our other values without privacy. We are not able to explore all of these in this paper, but, with respect to harmful digital ID programs, we suggest that privacy is valuable because

[12] Office of the Privacy Commissioner of Canada, "2020-21 Survey of Canadians on Privacy-Related Issues," March 10, 2021, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/.

[13] Office of the Privacy Commissioner of Canada.

[14] van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, "Privacy and Information Technology", *The Stanford Encyclopedia of Philosophy* (Summer 2020 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/sum2020/entries/it-privacy/.

[15] van den Hoven.

[16] The view that "what is lost cannot be recovered" is both false and dismal. Many domains that are currently private could yet be invaded; in other words, not all is yet lost. Further, one should not despair that, because they have lost their keys once, they will never recover them again.

security, autonomy, and human dignity are *prima facie* valuable.[17] Privacy, in this context, then, can be regarded as a *safeguard* against harm and against the loss of other important values.

In what follows, we explore how tracking and profiling digital ID programs (and similar information technologies) could have a potential negative impact on security, autonomy, and dignity. This is, in one sense, a picture of what Canadians stand to lose whenever they do not prioritize their privacy over the perceived convenience and safety of digital ID.

Security

Most Canadians value security, which also happens to be a right that is guaranteed in Section 7 of the *Canadian Charter of Rights and Freedoms*: "[e]veryone has the right to life, liberty, and security of the person, and the right not to be deprived thereof except in accordance with the principles of fundamental justice."[18] Security is not just a desirable thing to have; it is also a right guaranteed to all Canadians by the *Constitution* of Canada.[19] There are different ways to define security. In this report, we define security as *freedom from threat*.[20] We suggest that tracking and profiling digital ID programs are privacy-violating and expose their users to unnecessary threats. In other words, we suggest that privacy violations of this kind *matter* because they may threaten the security of those whose privacy has been violated. We think

[17] Or, in other words, their value is apparent

[18] *Canadian Charter of Rights and Freedoms,* s 7, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

[19] We acknowledge that it is unclear whether the *Charter* Section 7 right to security, as understood by Canadian courts, encompasses the right to informational privacy or to control over/access to personal information. Security of the person has been interpreted to refer to control over one's physical or psychic integrity, and Section 7 has been interpreted to be engaged whenever the state interferes with personal autonomy or the ability of an individual to control that integrity. (See: https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art7.html) Nonetheless, we think that informational integrity is an important dimension of human well-being. Harms to the digital identities of persons, or invasions of the informational privacy of persons, do seem to engage a common-sense understanding of security and the right to security.

[20] Buzan, Barry. *People, States and Fear.*

that this threat can be experienced either as an *indirect* or *direct* effect of governments capturing otherwise private information about their citizens.

So, what is the link between security, privacy, and digital ID?

Security concerns apply to (a) how information is stored and (b) how information is used by state authorities. First, threats may arise *indirectly* from government action. We note that one cannot hack or gain access to information that does not exist; t is a truism of information technology that nothing is entirely secure. The data collected by tracking or profiling digital ID programs is susceptible to illegal hacking by malicious parties. For example, in 2019, a Desjardins employee accessed the first and last names, dates of birth, social insurance numbers, street addresses, phone numbers, emails, and transaction histories of more than 9.7 million Canadians.[21] In 2019, LifeLabs admitted to having been hacked and having lost the healthcare data of more than 15 million Canadians.[22] In 2020, the Canadian Revenue Agency (CRA) locked more than 800,000 Canadian accounts over privacy concerns; 10,000 CRA accounts were illicitly hacked.[23] In 2022, the Canadian Department of Global Affairs[24] and the IT system used by Members of Parliament and their staff[25] were hacked. Canadians

[21] "Top 15 Cybersecurity Breaches in Canada," Cyberland, Accessed August 4, 2023, https://www.cyberlands.io/topsecuritybreachescanada.

[22] Top 15 Cybersecurity Breaches.

[23] Patrick Brethour, "Thousands of CRA accounts affected by CERB-related hacking," Globe and Mail, March 21, 2021, https://www.theglobeandmail.com/business/article-identity-fraud-complaints-nearly-doubled-in-2020-over-2019/.

[24] Naveen Goud, "Cyber Attack on Canada Foreign Affairs department," Accessed August 4, 2023, https://www.cybersecurity-insiders.com/cyber-attack-on-canada-foreign-affairs-department/.

[25] Irem Koca, "MPs warned to change email passwords after cyber attack on Canadian government," Toronto Star, October 18, 2022, https://www.thestar.com/politics/federal/2022/10/18/mps-warned-to-change-email-passwords-after-cyber-attack-on-canadian-government.html.

experienced an uptick in disruptions to critical infrastructure in 2021 and 2022 because of cybercrime.[26]

It is important to note that governments and corporations are only indirectly responsible for this kind of harm. Nonetheless, by creating databases that *can* be hacked, governments and corporations create the conditions which make hacking a possibility.[27] While governments must capture and store some data about their citizens, they need not capture or store more than is necessary. Whatever benefits may arise from tracking and profiling Digital ID programs, it is not clear that the benefits outweigh the costs associated with the possibility of external breaches to these programs.

Second, where information is concerned, threats to security may arise *directly* from government action. It is possible that governments and corporations will use information acquired via digital ID programs to harm or jeopardize Canadians. Cases like these have already occurred in Canada. During the COVID-19 pandemic, federal and provincial governments made digital proof of COVID-19 vaccination a precondition of access to many

[26] Government of Canada, "National Cyber Threat Assessment 2023-2024," Accessed August 4, 2023, https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.

[27] There is a worry that the data collected by Digital ID programs will be stored in centralized government databases. This worry often generates a "solution": data collected by Digital ID programs should be stored in *decentralized* government databases. In other words, data collected by Digital ID programs should not be stored in one database but in many, and nobody should have access to all the data contained within every database. Those who advocate for this kind of a "solution" generally think that Canadian data stored in this way will be less susceptible to hacking or government abuse. This is likely true, but this is not the "solution" to the problem of tracking and profiling digital ID programs, in our view. This solution ignores what is, in our view, the more fundamental question: is it necessary for governments to acquire the kind of information that could be stored in databases (of any kind) in the first place? We do not think that governments should ever collect unnecessary data about their citizens. After all, Digital ID programs exist for the purpose of helping individuals prove their identities to third parties. We are less concerned with *how* harvested information will be stored than with whether that information needs to be harvested in the first place.

public and private services.[28] In this case, Canadian governments and complicit organizations required Canadians to disclose private medical information about themselves in order to access the goods and services of those organizations. One might argue that these policies did not threaten the security of unvaccinated Canadians (or even vaccinated Canadians who refused to disclose their vaccination status) because being prohibited from dining out or from going to the theatre is not a threat, *per se*. (This may still generate an equality concern, however.) Unfortunately, these same policies also prohibited many Canadians from being eligible for organ transplants and other necessary healthcare services, employment, post-secondary education, financial services, domestic and international travel, and more.[29] Prohibitions on access to preventative or remedial healthcare are obvious instances of exposing Canadians to threats to physical and psychological well-being, and so these mandatory vaccination policies from 2021 can be regarded as threats to the security of affected Canadians.

These examples are cited because they demonstrate how Canadian governments and corporations can use information about the behaviours and medical histories of Canadians (e.g., vaccination status) to develop harmful policies that exclude people from vital services and opportunities. Even if one agrees with the mandatory vaccination policies imposed in 2021, this does not change the fact that Canadian governments have set a precedent of using personal information collected from individuals through tracking and profiling technologies (whether Digital ID or otherwise) to harm Canadians. Personal information should not be used against its owners (in all the usual cases). Privacy is shelter from state power. Invasions of freedom begin with invasions of privacy, for the arms of the state cannot grip a people it does not know.

[28] The Justice Centre has reported extensively on this policy and its impacts elsewhere. See: https://www.jccf.ca/published-reports/.

[29] See Justice Centre news releases here: https://www.jccf.ca/category/news-releases/.

Autonomy

Autonomy generally refers to the ability of rational, free agents to regulate their own lives, to be free from unnecessary or coercive forces, and to decide for themselves how to live.[30] Even if information captured by digital ID programs (or other information technologies) is stored securely, and even if that information is never used by governments or corporations to prevent Canadians from accessing public and private goods and services, it is nonetheless true that the very existence of surveillance programs threatens the autonomy of those being monitored.

Most Canadians would agree that autonomy is valuable. Nonetheless, the notion of autonomy is less understood than the notions of privacy or security. A helpful understanding of autonomy may be found from John Christman, who notes,

> Put most simply, to be autonomous is to govern oneself, to be directed by considerations, desires, conditions, and characteristics that are not simply imposed externally upon one but are part of what can somehow be considered one's authentic self. Autonomy in this sense seems an irrefutable value, especially since its opposite–being guided by forces that are external to the self and that cannot be authentically embraced by the self–seems to mark the height of oppression.[31]

The autonomy of persons has been a foundational value in most western democracies and in classical liberal traditions.[32-33] We now suggest that privacy violations threaten the capacity to

---

[30] Christman, John. "Autonomy in Moral and Political Philosophy", *The Stanford Encyclopedia of Philosophy* (Fall 2020 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/>.

[31] Christman, John.

[32] It is, further, a founding value of the Justice Centre, the vision of which is to realize "a free society where governments uphold human dignity by respecting fundamental rights and freedoms, and where Canadians can realize their potential and fulfil their aspirations".

[33] Of course, individual autonomy is not an absolute or unqualified value; most Canadians would prefer not to live in a country in which harmful behaviours are allowed to be expressed. Laws exist (in part) to limit the ability of individuals to engage in behaviour that harms other people. Despite these necessary limitations, most Canadians

govern oneself, decide upon a course of action, and pursue goals that arise from motivations considered to be one's own, free from disturbing external forces.

So, what is the link between autonomy, privacy, and digital ID?

Tracking and profiling digital ID programs (and any similar surveillance systems) threaten the ability of their users to experience and express their own autonomy. It is well established that surveillance programs have a chilling or quieting effect on expression, creativity, and civic engagement. When people know that their behaviours and speech are being monitored, they tend to avoid speaking about, writing about, or researching subjects that would put them at odds with the state, with institutionalized norms, or even with majority opinion. This is true in most places and not just in countries normally associated with mass surveillance or with routine state invasions of personal privacy.

We see this in the aftermath of the 2013 disclosure of National Security Agency surveillance operations in the United States. According to a 2013 survey of American writers conducted by Pen America and the FDR Group, 85 percent of survey participants (all of them writers) stated that they were concerned with government surveillance.[34] Sixty-six percent stated that they disapproved of the government collecting internet and telecommunications data as part of their war on terrorism.[35] After it was discovered, in 2013, that the National Security Agency (NSA) had been conducting mass surveillance operations on millions of American phones, email accounts, online behaviours and transactions, and chat forums, many writers reported self-censoring in order to avoid unnecessary attention from the state. According to the survey, 16 percent of participants reported having avoided writing or speaking about certain topics in

would prefer to live in a country in which behaviours that are not incompatible with the principles of fundamental justice are given space to become reality.

[34] "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor," PEN America, November 12, 2013, https://pen.org/wp-content/uploads/2022/08/2014-08-01_Full-Report_Chilling-Effects-w-Color-cover-UPDATED.pdf

[35] "Chilling Effects.

order to avoid negative repercussions. This expressive reluctance was particularly pronounced among writers and researchers who were inclined to criticize the government or address sensitive topics, including topics like the Middle East, state security, and foreign perceptions of America. The Canadian context is, of course, different; but the causal relationship between mass surveillance and self-censorship is not. Self-censorship that is caused by external forces, such as the presence of mass surveillance programs, is incompatible with human autonomy. According to van den Hoven, Blaauw, Pieters, and Warnier,

> Lack of privacy may expose individuals to outside forces that influence their choices and bring them to make decisions they would not have otherwise made. Mass surveillance leads to a situation where routinely, systematically, and continuously individuals make choices and decisions because they know others are watching them. This affects their status as autonomous beings and has what sometimes is described as a "chilling effect" on them and on society.[36]

A second concerning feature of digital ID programs is that they may be used to limit access to information. Consider the digital ID programs being proposed in Australia and the United Kingdom, which will be used to restrict what people can access online or the minimum age at which they can access online information, including social media content.[37-38] While content limitations may be appropriate in some cases (e.g., to prevent minors from accessing pornography), content limitations may not be appropriate in others. In China, information technologies are used to prevent Chinese citizens from accessing the media of democratic states, along with other content which the state considers damaging to its interests.[39] It is

[36] "Privacy and Information Technology," Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/it-privacy/.

[37] Staff Avision, "Australia considers digital ID age verification for porn," SecureID News, January 14, 2020, https://www.secureidnews.com/news-item/australia-considers-digital-id-age-verification-for-porn/.

[38] Frank Hersey, "UK plans to make digital ID 'as trusted as passports' Biometric Update, July 20, 2021, https://www.biometricupdate.com/202107/uk-plans-to-make-digital-id-as-trusted-as-passports.

[39] Steven Lee Myers, "China's Search Engines Have More Than 66,000 Rules Controlling Content, Report Says," New York Times, April 26, 2023, https://www.nytimes.com/2023/04/26/business/china-censored-search-engine.html.

important that states do not limit the ability of citizens to access information, especially when that information is (a) potentially at cross-purposes with state interests and (b) not illegal. In many jurisdictions across the world, states use technologies like digital ID to prevent their citizens from accessing information considered "undesirable".

Human Dignity

The term "dignity" has referred to different things since it first appeared in literature and law thousands of years ago. Traditionally, "dignity" was applied to persons perceived to be graceful, composed, or beautiful; to persons perceived to adhere with integrity to personal or community codes of conduct; or to persons perceived to have elevated or noble social status.[40] According to these notions, people have dignity whenever they have desirable personal or physical qualities, character, or social status. In other words, dignity is *earned* and is, therefore, non-universal; not everyone has it.

In the twentieth century, the term "dignity" came to mean the value of human beings *as* human beings. Scholars and legal theorists began to think of "human dignity" as a feature of *being human* that does not depend on the possession of beauty, principledness, or rank (or any other *earned* feature). Rather, it was thought that human beings are valuable as such; they have inherent value or goodness. Because all human beings have inherent value or goodness, no human being can be considered more or less dignified (or more or less valuable) than any other human being. All human beings enjoy the status of having human dignity to the same degree.

On this more contemporary definition, the *fact* all human beings are inherently dignified generates an obligation to *recognize* the fact that all human beings are inherently dignified.

[40] Remy Debes, "Dignity", *The Stanford Encyclopedia of Philosophy* (Spring 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/spr2023/entries/dignity/.

The innate dignity of human beings generates for us moral and/or legal reasons to ensure that the dignity of all human beings is preserved. In other words, we have an obligation to treat ourselves and others in ways that are appropriate to the kinds of beings we are, according to scholar Suzy Killmister.[41] This is, for many scholars, the link between (a) human dignity and (b) human rights.[42]

According to scholar Teresa Iglesias,

> The connection [between dignity and rights] is essential. It is rooted in the concept of the human person, in human self-understanding as constituted by the bedrock truths about what and who we are…The universal meaning of the concept of *dignity,* as inherent to every human being, expresses the *intrinsic good that the human being is.* The distinct *human rights* articulate those basic *intrinsic goods* proper to, and expressive of, each one's dignity, individually and in community relationships—as dimensions of our very being. These basic goods—guaranteed as rights—must be recognized, respected, and promoted so that the intrinsic good that the human being is himself or herself, personally and as an individual, may be preserved and assured. Thus, the ground for advocacy and defense of human rights resides on what and who the human being is, *as* a human being, namely on his or her dignity.[43]

The idea that human rights guarantee basic goods (e.g., freedom of expression, guaranteed by *Canadian Charter of Rights and Freedoms* and by many other constitutional documents across

[41] Suzanne Killmister, *Contours of Dignity*, Oxford/New York: Oxford University Press. doi:10.1093/oso/9780198844365.001.0001 at page 23.

[42] Other scholars (e.g., Waldron 2012) think that there is no need to appeal to the "innateness" or "inherentness" of human dignity to explain the link between human dignity and rights. We can remain quiet about whether or not dignity is an innate feature of being human. Instead, we might think that people of lower social rank successfully captured for themselves (at various points throughout history, but especially since the 18th century), through political movements and legal developments, the rights and privileges previously enjoyed only by those of higher ranks. Whatever we think explains the link between human dignity and rights, however, most agree that such a link exists. In other words, most agree that having human dignity generates rights and obligations. (See: Waldron, Jeremy, 2012, *Dignity, Rank, and Rights*, Meir Dan-Cohen (ed.), (Berkeley Tanner Lectures), New York: Oxford University Press. doi:10.1093/acprof:oso/9780199915439.001.0001 at pages 57-61.)

[43] Teresa Iglesias, 2001, "Bedrock Truth and the Dignity of the Individual," *Logos: A Journal of Catholic Thought and Culture*, 4(1): 114–134. doi:10.1353/log.2001.0005, at page 130.

the world) and that these goods are necessary for the preservation and assurance of human dignity is a long-standing value of western democracies. The scholar Immanuel Kant, writing in the 18th century, argued that all human beings have innate value or dignity because they are rational and autonomous. Because of our rational autonomy, we have moral value, according to Kant, and we must abide by certain limitations in our treatment of each other. In other words, people must not violate the rights and freedoms that are owed to us as human beings. An implication of this is that human beings are "ends in themselves", according to Kant. They are not "means to the ends of others". When we treat people as though they are ways of getting what we want (e.g., by deceiving them or by violating their privacy), we undermine their rational autonomy; we undermine their ability to have genuine self-motivated desires, to evaluate what is best for themselves, or to make long-term plans for themselves. (We can see here a link between autonomy and human dignity.) On this notion of human dignity, human beings have the right to exist for themselves and not for the interests of others, their community, or the state.[44]

So, what is the link between human dignity, privacy, and digital ID?

We suggest that the tracking and profiling digital ID programs referenced in Part One of this report are concerning because they pose a threat to human dignity. From another perspective, privacy matters because it is necessary for human dignity. When digital ID programs peer into intimate and personal spaces, the human being is treated as an object for study, analysis, and

[44] Articulations of fundamental rights and freedoms in codes of law, charters, and declarations are designed, therefore, to protect human beings from being treated in ways that undermine their dignified status as human beings. One of the first legal recognitions of the conceptual and legal link between human dignity and rights appears in the United Nations' *Universal Declaration of Human Rights*, (1948), the preamble to which mentions "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice, and peace in the world…" While the *Canadian Charter of Rights and Freedoms* does not mention the term "dignity", it is clear that this document seeks to protect human dignity. In other words, it is clear that the rights and freedoms guaranteed by the *Charter* are guaranteed because they are considered necessary for the preservation and assurance of human dignity, among other related goods.

prediction. She is, in a word, treated as a specimen, not as a being dignified and rightly hidden from the gaze of the state.

The scholar Edward J. Bloustein (1964) argues that privacy invasions undermine the possibility of an "inviolate personality" (or of a "person that ought not to be harmed or violated"). Legal and social protections for personal privacy safeguard the inviolate personality of human beings, which includes their individual dignity and integrity, their autonomy and independence.[45] These are all dimensions of what it means to have human dignity, according to Bloustein. Other scholars point out that privacy violations caused by surveillance technologies and treat individuals as specimens or objects of study–objects that can be perfectly modelled and predicted across time. It is, however, an epistemic[46] and moral immodesty to regard individuals as objects of study. First, we argue that governments do not have a right or need to know the kind of information collected by privacy-invading digital ID programs. Their attempt to know more than they should is an epistemic (or knowledge-related) overreach. Second, we argue that governments have no moral justification for collecting the kind of information collected by privacy-invading digital ID programs, in normal cases. The claim (whether made explicitly or implicitly) that governments have a moral justification for accessing unnecessary information is an overreach.

Harms to human dignity generate real-world harms. When sophisticated information technologies are used to track and profile citizens, sensitive information about citizens (e.g., sexual preferences, political affiliation, religious belief, medical history, and race/ethnicity) can be derived and cited as justification for discrimination. Even when citizens are assigned to particular groups only probabilistically, their being assigned to those groups can influence the

[45] Remy Debes.

[46] From the Greek *epistēmē*, meaning *knowledge* or *understanding*

actions of others or the willingness of others to engage with them.[47] According to van den Hoven (et al.),

> [P]rofiling could lead to refusal of insurance or a credit card, in which case profit is the main reason for discrimination. When such decisions are based on profiling, it may be difficult to challenge them or even find out the explanations behind them. Profiling could also be used by organizations or possible future governments that have discrimination of particular groups on their political agenda, in order to find their targets and deny them access to services, or worse.[48]

In both cases, privacy-violating digital ID programs undermine the inviolate personality or human dignity of their users. The intimate or interior lives of human beings cannot be captured be a catalogue of facts about them. Or, even if it were possible to reduce the human being to such a catalogue, the government has no business possessing it, for the individual does not exist for the state.

Conclusion

We can now respond to a common objection to the value of privacy, which reads something like this: *"Privacy is valuable only to criminals."* While it is true that criminals will take advantage of privacy protections to reduce the chance of getting caught and prosecuted, prosecuting criminal behaviour should not serve as a pretext for violating the privacy, security, autonomy and dignity of an on-the-whole law-abiding population. This exposes all citizens to the possibility of state abuse.

[47] Taylor, L., L. Floridi, and B. Van der Sloot (eds.), 2017, *Group privacy: New challenges of data technologies* (Philosophical Studies Series: Vol. 126), Dordrecht: Springer.

[48] van den Hoven.

In this report, we have explored case studies, surveys, and scholarly literature which show that privacy is necessary for the enjoyment of security, autonomy, and human dignity. Regarding security, the state sometimes uses what it knows about its citizens to intervene unjustifiably in their personal affairs. The first and best shelter from unreasonable interventions is privacy–the right to be let alone. Regarding autonomy, surveillance is correlated with a loss of expressive motivation and capacity. We also explored the fact that information technologies can be used to limit access to information, which negatively impacts the ability of potential viewers to become informed and to consider an array of alternatives before setting upon a course of action. Researchers, democratic participants, artists, and others are given strong motivations to self-censor when they know they are being monitored. Finally, human beings enjoy an inherent dignity. Codified rights and freedoms are designed to preserve and assure the enjoyment of that dignity, which demands that the state not regard the individual (or individual data) as mere fodder for state interests. In a word, the motivation to defend privacy is greater than the motivation to hide criminal or immoral behaviours from social or state awareness.

The value of privacy can be defended from several compelling angles. On an international scale, a country with robust legal protections for data and privacy is a safer place to conduct personal and business affairs. On a national scale, such protections service families and partnerships, businesses, and democratic institutions. In this report, we have focused on the value of privacy for individuals, although more could be said about the value of privacy for groups and countries.

States are aware that privacy is valuable. They appeal to the value of privacy to insulate their spending, relationships, and ambitions from democratic accountability. In planning its actions and carrying out its tasks, the state has not lost sight of the value of privacy. Privacy is enjoyed by the state, but not to the same extent by the citizens to whom the state belongs. This report, then, has been a defense of the value of privacy *for individuals*, who must be protected from

the state and from the sophisticated information technologies used by the state to know and control. As scholar Adam Moore says, we must defend "the importance of privacy as a bulwark against the tyrannical excesses of an unchecked state."[49]

[49] DeCew, Judith, "Privacy", *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2018/entries/privacy/.

Bibliography

Avision, Staff. "Australia considers digital ID age verification for porn." SecureID News. January 14, 2020. https://www.secureidnews.com/news-item/australia-considers-digital-id-age-verification-for-porn/.

Biometric Update. "Governments Digital Identity Credentials to Reach 5 billion by 2024 Backed by Mobile Biometrics." June 9, 2019. https://www.biometricupdate.com/201907/governments-digital-identity-credentials-to-reach-5-billion-by-2024-backed-by-mobile-biometrics.

Brethour, Patrick. "Thousands of CRA accounts affected by CERB-related hacking." *Globe and Mail*. March 21, 2021. https://www.theglobeandmail.com/business/article-identity-fraud-complaints-nearly-doubled-in-2020-over-2019/.

Buzan, Barry. *People, States and Fear: The National Security Problem in* 21 *International Relations*, Sussex. Wheatsheaf Books. 1983.

Christman, John. "Autonomy in Moral and Political Philosophy." *The Stanford Encyclopedia of Philosophy* (Fall 2020 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/.

Cyberland. "Top 15 Cybersecurity Breaches in Canada." Accessed August 4, 2023. https://www.cyberlands.io/topsecuritybreachescanada.

Debes, Remy. "Dignity." *The Stanford Encyclopedia of Philosophy* (Spring 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.). https://plato.stanford.edu/archives/spr2023/entries/dignity/.

DeCew, Judith. "Privacy." *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/spr2018/entries/privacy/.

DIACC. "Digital ID and Authentication Council of Canada Research Finds Canadians Want Digital ID that is user-centric and aligns with their values." April 4, 2022.

https://diacc.ca/2022/04/04/privacy-security-and-choice-drive-canadians-desire-for-digital-id/.

Goud, Naveen. "Cyber Attack on Canada Foreign Affairs department." Accessed August 4, 2023. https://www.cybersecurity-insiders.com/cyber-attack-on-canada-foreign-affairs-department/.

Government of Canada. "Digital Credentials." Accessed August 4, 2023. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html#:~:text=Digital%20credentials%20in%20Canada&text=Digital%20credentials%20offer%20Canadians%20the,interacting%20with%20government%20in%20Canada.

--- *The Canadian Charter of Rights and Freedoms.* Part 1 of the *Constitution Act 1982,* being Schedule B to the *Canada Act 1982* (UK). https://laws-lois.justice.gc.ca/eng/const/page-12.html.

--- "National Cyber Threat Assessment 2023-2024." Accessed August 4, 2023. https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024.

--- "Section 7–Life, Liberty and Security of the Person." Accessed August 4, 2023. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art7.html.

Herrington, Jonathan. "The Concept of Security." 2012. https://jherington.com/docs/Herington_Ashgate-2012.pdf.

Hersey, Frank. "UK plans to make digital ID 'as trusted as passports' Biometric Update." July 20, 2021. https://www.biometricupdate.com/202107/uk-plans-to-make-digital-id-as-trusted-as-passports.

Iglesias, Teresa. "Bedrock Truth and the Dignity of the Individual." *Logos: A Journal of Catholic Thought and Culture*, 4(1): 114–134. 2001. doi:10.1353/log.2001.0005.

Juniper Research. "Active Digital Identity Apps to Surpass 4.1 Billion By 2027, As Third-Party Platforms Look to Leverage Civic Identity Systems." February 27, 2023.

https://www.juniperresearch.com/pressreleases/active-digital-identity-apps-to-surpass-4-1bn.

Killmister, Suzanne. *Contours of Dignity*. Oxford/New York: Oxford University Press. doi:10.1093/oso/9780198844365.001.0001.

Koca, Irem. "MPs warned to change email passwords after cyber-attack on Canadian government." *Toronto Star*. October 18, 2022. https://www.thestar.com/politics/federal/2022/10/18/mps-warned-to-change-email-passwords-after-cyber-attack-on-canadian-government.html.

Myers, Cayce. "Warren, Samuel & Louis Brandeis. The Right to Privacy, 4 Harv. L. Rev. 193 (1890)." *Communication Law and Policy*, vol. 25, no. 4. 2020. https://doi.org/10.1080/10811680.2020.1805984.

Myers, Steven Lee. "China's Search Engines Have More Than 66,000 Rules Controlling Content, Report Says." *New York Times*. April 26, 2023. https://www.nytimes.com/2023/04/26/business/china-censored-search-engine.html.

Office of the Privacy Commissioner of Canada. "2020-21 Survey of Canadians on Privacy-Related Issues." March 10, 2021. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/.

PEN America. "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor." November 12, 2013. https://pen.org/wp-content/uploads/2022/08/2014-08-01_Full-Report_Chilling-Effects-w-Color-cover-UPDATED.pdf.

Resta, Giorgio. "Human Dignity." *McGill Law Journal*, vol. 66, no. 1. 2020. https://doi.org/10.7202/1082043ar.

Taylor, L., L. Floridi, and B. Van der Sloot (eds.). *Group privacy: New challenges of data technologies.* (Philosophical Studies Series: Vol. 126), Dordrecht: Springer. 2017.

Thales. "5 reasons for Electronic National ID Cards." Thales. March 29, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/5-reasons-electronic-national-id-card.

United Nations. *Universal Declaration of Human Rights*. 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier. "Privacy and Information Technology." *The Stanford Encyclopedia of Philosophy* (Summer 2020 Edition), Edward N. Zalta (ed.). https://plato.stanford.edu/archives/sum2020/entries/it-privacy/.

Waldron, Jeremy. *Dignity, Rank, and Rights*. Meir Dan-Cohen (ed.), (Berkeley Tanner Lectures), New York: Oxford University Press. 2012. doi:10.1093/acprof:oso/9780199915439.001.0001.