April 4, 2023

Justice Centre Reports & Analysis | Luke A. Neilson

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

Justice Centre for Constitutional Freedoms

Abstract

Information technologies with data-tracking and/or user-profiling capabilities generate significant privacy concerns. Proposals for Canadian digital identification frameworks often make accommodations for those frameworks to have data-tracking and user-profiling capabilities and do, therefore, generate privacy concerns. Furthermore, technologies with such capabilities may generate additional concerns surrounding freedom, mobility, security, equality, access, autonomy, consent, and human dignity. These concerns sometimes engage the *Canadian Charter of Rights and Freedoms*, to which Canadians should appeal in any contest between privacy rights and government intrusions into properly private spheres of human life.

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 legal research and advocacy because of your generosity and vision.

Updates to this report

This is Version 1.0 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

Canadians care about privacy. Canadian governments and their partnering agencies care about implementing digital ID programs at the provincial, federal, and international levels. Both privacy and digital ID programs are thought to be necessary for human improvement and flourishing. In certain cases, however, emerging information technologies like digital ID appear to have negative impacts on the enjoyment of privacy. There exists a tension between protecting private spheres from government surveillance and providing Canadians with convenient and secure access to goods and services.

Some analyses suggest that all digital ID programs are privacy harming or that there are no features of digital ID that are privacy-neutral or privacy-enhancing. This does not appear to be the case. Certain programs appear to be mere digital counterparts to the physical identification documents with which Canadians are already familiar, e.g., driver's licenses, passports, or healthcare cards. In fact, some programs appear to be privacy-enhancing. In France and the United Kingdom, digital ID users can exchange only whatever information about themselves is necessary for transactions to occur. This is an improvement on the physical identification documents familiar to Canadians, who often cannot avoid disclosing irrelevant private information about themselves (e.g., a home address) when submitting proof of other claims (e.g., claims about age or citizenship).

Not all digital ID programs are privacy-neutral or privacy-enhancing, however. In certain jurisdictions of Italy, China, and Canada, governments and their partnering agencies are developing digital ID programs that are more than mere counterparts to traditional identification documents. Some programs have functionalities that allow governments and their partnering agencies to track the behaviours of their users across time and to develop, thereby, complex profiles of their identities. In Bologna, Italy, users are motivated by their municipality to upload information about their "virtuous" behaviours to their Smart Digital Wallets to gain access to exclusive goods and services. In China, citizens are motivated to perform "virtuous" behaviours and to avoid "non-virtuous" behaviours to avoid significant

social and legal penalties, such as restrictions on mobility or imprisonment. In Canada from 2018 and 2022, the federal government partnered with the World Economic Forum to develop a Known Traveller Digital Identity that would have motivated domestic and international travellers to surrender otherwise private information about their itineraries, reasons for travelling, travelling partners, travel histories, and other personal information in order to access ameliorated goods and services. More recently, the Digital Identification and Authentication Council of Canada recommended a Digital Identity Ecosystem that would capture biological and behavioural data about Canadians, including (e.g.) fingerprints, typing speed, touch pressure, and walking gait as measured by users' mobile devices.[1]

Digital ID programs that capture data about the behaviours, beliefs, and/or personalities of their users across time generate significant ethical and legal concerns. For instance, proposed digital ID programs in Canada generate concerns about whether it is fair for governments to demand that individuals surrender otherwise private information in order to access the goods and services to which they had previously enjoyed access, especially when access to those goods and services is necessary for the enjoyment of *Charter*-protected rights and freedoms. Further, proposed digital ID programs in Canada generate concerns about the appropriateness of governments or state authorities (e.g., post-secondary institutions or healthcare authorities) determining which individuals or organizations count as trustworthy or credible. Finally, proposed programs in Canada generate concerns about the ethics of rating the credibility or trustworthiness of their users; there is a concern that proposed rating systems may be unreliable and arbitrary and that that ratings which arise from them may lead to discrimination or to disproportionate access to goods and services.

[1] We evaluate this Digital Identity Ecosystem in Section II (starting at page 32) of this report. See: "Pan-Canadian Trust Framework Model," Digital Identification Council of Canada, Accessed April 3, 2022, https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf.

Harmful digital ID programs are harmful precisely because they are privacy violating. Unfortunately, the value of privacy has not been adequately articulated in Canadian public policy debates about digital ID or similar information technologies. It is often thought that "privacy is only valuable to those who have something to hide." This is not the case. Privacy is necessary for the enjoyment of important human values, such as security, autonomy, and human dignity. In some cases, privacy is necessary for the prevention of harms. As governments continue to reach for powerful surveillance technologies under the pretense of making the world more efficient and secure, Canadians need to be aware that even the voluntary exchange of otherwise private information for access to goods and services is an extremely *costly* one.[2]

Whatever digital ID programs are implemented in Canada will have to comply with existing privacy laws. Unfortunately, this is no guarantee that implemented digital ID programs will protect the privacy concerns of Canadians. In 2022, the government of Québec passed legislation that will, in effect, permit entities to collect information about the work performance, economic situations, health, personal preferences, interests, or behaviours of Canadians.[3] As new information technologies (e.g., digital ID or AI) emerge, and as governments find new invasive applications for existing technologies (e.g., facial recognition or smartphone tracking technologies), Canadian privacy laws will have to be reinforced and extended to protect the privacy interests of Canadians, to prevent harms to vulnerable groups, and to stem government overreach into what are properly private spheres.

---

[2] In Part Two of this report (to be released before June 30, 2023), we evaluate recent case studies and show that privacy is necessary for the enjoyment of security, autonomy, and human dignity. We also show that privacy violations may equip governments to unreasonably limit the enjoyment of *Charter* Section 2 freedoms, Section 6 mobility rights, Section 7 security rights, and Section 15 equality rights.

[3] "Bill 64: An Act to modernize legislative provisions as regards the protection of personal information," National Assembly of Québec, Accessed April 3, 2023, https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/190120/sq-2021-c-25.pdf, at 65.0.1.

Canadians cannot continue to permit governments to scrutinize the intimate identities of their citizens or to invade every remaining private domain. In some jurisdictions, governments appear to be selling their citizens a mere "digital counterpart to the identification documents with which they are already familiar" as a ruse for the installment of harmful surveillance programs. Canadians need tools for differentiating between tolerable digital identification documents and intolerable surveillance programs.

Introduction

More than 70 countries have implemented digital ID programs of some kind.[4] According to Juniper Research, there were more than 4.2 billion users of digital ID in 2022.[5] Juniper Research predicts that there will be more than 6.5 billion users by 2026 as governments and corporations increasingly move toward digital identity authentication and as users are increasingly expected to be able to authenticate their identities remotely.[6] In 2021, digital ID programs generated $26 billion of revenue; they are expected to generate $53 billion in revenue by 2026.[7] Just as there are positive economic incentives (i.e., wealth creation) for digital ID programs in Canada, there are also negative incentives (i.e., prevention of loss)

[4] "Five reasons for electronic national ID cards," Thales Group, March 29, 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/5-reasons-electronic-national-id-card.

[5] "Digital Identity: Solutions assessment, regional analysis, & market forecasts 2023-2017," Juniper Research, February 27, 2023, https://www.juniperresearch.com/researchstore/fintech-payments/digital-identity-research-report.

[6] The impetus for Digital ID programs has, in many cases, been accelerated by Covid-19 non-pharmaceutical interventions (i.e., lockdowns), which forced people to access goods and services remotely. In many cases, government agencies needed to find ways for users to credibly prove their identities where physical identification documents (e.g., passports and healthcare cards) were insufficient.

[7] Juniper Research, "Digital Identity."

for the same. A Digital Identification and Authentication Council report[8] suggests that Canadians over the age of 19 could collectively save $6.1 billion dollars per year by implementing a federal digital ID program; banks could save $100 million per institution per year; governments could save $482 million per year.

This global trajectory toward the development and expansion of digital ID programs has been motivated by various factors, including the need for governments and corporations to digitize and modernize the delivery of goods and services (e.g., Germany and Japan), to solve security and privacy issues, to combat rising fraud and cybercrime rates, to facilitate intra- and international travel (China, Germany, and Spain), to deliver services remotely, and to reduce harm (Australia and the United Kingdom). In Canada, digital ID initiatives are framed as solutions to increasing rates of identity theft and online fraud, security breaches, and bureaucratic inefficiencies. In China, digital ID initiatives are supposed to help 100 million interprovincially mobile Chinese citizens authenticate their identities and access goods and services when far from home.[9] In Australia and the UK, experts are discussing the possibility of using digital ID programs to prevent minors from illegally accessing online pornographic content, from wagering online, or from accessing social media.[10-11]

Digital ID initiatives are being developed to solve a complex of practical, social, and ethical problems. It is important to recognize this point. Analyses which fixate on the thesis that "all digital ID programs are a ruse for totalitarian surveillance programs" fail to

[8] "The economic impact of digital ID in Canada," Digital Identity Authentication Council of Canada, Accessed April 2, 2023, https://diacc.ca/wp-content/uploads/2018/05/Economic-Impact-of-Digital-Identity-DIACC-v2.pdf.

[9] "China to launch nationwide digital ID card in 2022," Keesing Platform, March 24, 2022, https://platform.keesingtechnologies.com/china-to-launch-nationwide-digital-id-card-in-2022/.

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

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

capture the facts that (a) digital ID programs have emerged in response to real social and economic problems, (b) digital ID programs can be privacy enhancing or can have privacy-enhancing features, and (c) citizens can peacefully engage with their governments to determine the modality, function, and scope of digital ID programs. (We learn later that the citizens of Germany, Japan, and Saskatchewan are exercising their democratic rights to protect against mandatory programs and to ensure that those programs do not have surveillance functionalities.)

Most Canadians, however, are uncertain about how information technologies like digital ID will impact their privacy. According to a 2020-2021 survey conducted by the Office of the Privacy Commissioner of Canada, "…almost half of Canadians (47 percent) do not have enough information to know how new technologies might affect their personal privacy…"[12] The same survey found that "[t]he vast majority of Canadians (87 percent) expressed some level of concern about the protection of their privacy…, including 32 percent of Canadians who said they are extremely concerned about the protection of personal privacy."[13] Most Canadians already feel that they do not possess adequate control over their personal information.[14] At the same time, Canadians and their governments care to implement technologies that solve social, economic, financial, and healthcare problems. These technologies often generate privacy concerns. This report investigates the tension between an emerging technology, digital ID, and the enjoyment of privacy in Canada.[15]

---

[12] "2020-21 survey of Canadians on privacy-related issues," Office of the Privacy Commissioner of Canada, 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] Office of the Privacy Commissioner of Canada. According to the cited survey, "The majority of Canadians also feel they have not very much or no control at all over how their personal information is used by companies (61%) or by government (65%)."

[15] It is important to note that many of the tensions and concerns identified in this report are applicable to surveillance programs understood more broadly and not just to whatever Digital ID programs function as surveillance programs. The conclusions of this report may, therefore, enjoy applications in other related domains.

On June 2, 2022, Privacy Commissioner of Canada Daniel Therrien noted that "Digital ID, like all technologies, can be helpful and privacy protective or harmful to privacy depending on how it is designed."[16] This report makes some progress in discovering the line between privacy-neutral and privacy-harming digital ID initiatives. The distinction between them has not been adequately explored. Further, this distinction should be of some use to Canadian voters and public policy designers. While no government fails to proclaim that privacy protections are at the heart of their digital ID initiatives, few governments say more about privacy than this. It is therefore unclear how proposed initiatives will impact the enjoyment of privacy.

Report structure

In Part One (presented here), this report provides an analysis of the digital ID initiatives of six comparator jurisdictions (C6). This analysis indicates that digital ID programs vary in their modality, their intended functionality, and the scope of the data captured by them. It seems that not every digital ID program generates privacy concerns.[17] In fact, some digital IDs may be more privacy-preserving than the physical identification documents they are designed to replace or complement. Notwithstanding this, it also seems that some digital ID programs do generate significant privacy concerns. We would like to understand why some programs generate privacy concerns while others do not. From another perspective, we would like to understand why some programs are harmful while others are non-harmful. *This report advances a loose but nonetheless helpful distinction between non-harmful and harmful programs based on the scope and kind of data captured by the programs.*

---

[16] Anthony Murdoch, "Canadian gov't looking to implement digital ID program despite concerns of privacy experts," *Life Site News,* August 12, 2022, https://www.lifesitenews.com/news/canadian-govt-looking-to-implement-digital-id-program-despite-concerns-of-privacy-experts/.

[17] Or, it seems that some Digital ID programs have privacy-enhancing features. Such features should be implemented whenever possible.

Programs that capture more data than is necessary for users to credibly authenticate their identities (or specific claims about their identities) to others are harmful digital ID programs, on this analysis. More specifically, *programs that track data pertaining to the biology, behaviours, personalities, and/or beliefs of their users across time* are harmful, and we suggest that such programs are harmful precisely because they violate the privacy of their users.[18-19-20] Or, whenever such information must be collected and stored by digital ID programs for the authentication of users' identities, there should be strong justifications for collecting and storing this information; the collection and storing of such data should not be the default state. Finally, whatever information is collected should not be used to profile (i.e., to "get at" the intimate identities of) digital ID users.

---

[18] We suggest later that, even where users consent to the tracking and profiling of their identities across time, the exchange of otherwise private information for access to goods and services sometimes constitutes an *unfair* exchange.

[19] We note that Digital ID programs can capture more data than is required for proof-of-identity without thereby being tracking or profiling programs. There is a "conceptual" or "possible" space between the harmful and non-harmful programs described above. Our understanding is that this space is "merely possible" and is not being occupied by Digital ID programs, which tend to either be modest proof-of-identity programs (e.g., mere digital counterparts to the traditional physical identification documents with which Canadians are familiar) or fully fledged *tracking/profiling programs.*

[20] Importantly, this report is not an analysis of the *technology* of Digital ID. We are not positioned to address the security or privacy implications of biometric, cryptographic, distributed ledger, or blockchain technologies, to name but a few of the many complex technologies powering Digital ID programs today. In other words, this is not a software engineer's analysis of Digital ID. Rather, this is a face-value analysis of what governments and their partnering agencies are saying about their Digital ID programs. Any recommendations or evaluations advanced in this report are therefore qualified by the following: whether any program is ultimately privacy-enhancing, privacy-neutral, or privacy-harming will depend on factors that fall beyond the scope of this analysis. This report is nonetheless helpful. Any program that appears to be privacy-harming on a face-value analysis will probably be privacy-harming, whatever the underlying technology happens to be. For instance, whenever a government publicly states or suggests that their Digital ID program has the capacity to track the behaviours of their users across time, this program will be privacy-harming (on our analysis), whatever the underlying technology happens to be. However, programs that appear to be privacy-enhancing or privacy-neutral on a face-value analysis may, in fact, be privacy-harming, depending on the underlying technology. Accordingly, this report is a starting place for future research on Digital ID programs.

This report then applies this distinction to the digital ID initiatives of the six comparator jurisdictions (C6) and finds that the digital ID initiatives of Italy, China, and Canada count as harmful precisely because they have the capacity to track the behaviours of their users across time and to develop, thereby, complex profiles of their users. Once again, this report suggests that such programs lead to a violation of privacy or (in cases where individuals voluntarily consent to exchanging otherwise private information to access promised goods or services) to an unfair exchange of otherwise private information for access to goods and services.

This report then evaluates the World Economic Forum's (WEF) Known Traveller Digital Identity (KTDI) program–a program with which Canada had partnered between 2018 and 2022. We suggest that the KTDI functions as a kind of tracking and profiling program and that it would have generated significant concerns about access, consent, fairness, and privacy had it been implemented. While it is unclear whether Canada will pursue a partnership with the WEF around the KTDI going forward, an analysis of the tracking capabilities of the KTDI is a fascinating look at "where Canada might have gone" and the importance of protecting private spheres from government overreach. This report then evaluates the proposed Pan-Canadian Trust Framework of the Digital Identity Authentication Council of Canada (DIACC). We suggest that his program is harmful insofar as it recommends that government and private entities capture data about the biology and behaviours of users across time as a requirement of participation.

We conclude Part One by looking at how the citizens of Germany, Japan, and Saskatchewan have peacefully engaged with their governments to (a) determine how (and even whether) digital ID programs are implemented in their jurisdictions and to (b) stem the incursions of governments into properly private spaces.[21]

[21] Part Two of this report will be released before June 30, 2023.

I Digital ID in six comparator jurisdictions (C6)

We want to gain a clearer picture of what all digital ID programs have in common, what differentiates those programs from each other, and why it is that some programs generate practical, social, and ethical problems. Before evaluating their differences, this report investigates what all digital ID programs appear to have in common. In its simplest form, digital ID is a technology that allows users to credibly authenticate their identities (or claims about their identities) to other agents, such as governments, corporations, or individuals, especially within the domains of financial services, online e-commerce, health, and government services.[22] What makes an authentication document *credible* is usually the endorsement of some state agency (e.g., a government, a healthcare agency, a post-secondary institution, etcetera). Of digital ID, the Government of Canada states,

> In the physical world, your driver's licence or health card allows you to provide information about yourself, what you can do, or what services you can access; digital credentials would be the digital equivalent of these documents. These credentials would make services faster, easier, and safer for Canadians.[23]

According to this definition, digital ID can be thought of as a digital counterpart to the physical identification documents with which Canadians are already familiar. Beyond this simple definition, however, digital ID takes many different forms and therefore generates different kinds and degrees of privacy concerns. We explore these different forms in the next section.

---

[22] Digital Identity Authentication Council of Canada, "The economic impact of digital ID."

[23] "Digital Credentials," Government of Canada, Accessed April 3, 2023, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html.

In this section, we describe key features of the digital ID programs of six comparator jurisdictions (C6): France, the United Kingdom, Germany, Japan, Bologna (Italy), and China. While many jurisdictions have adopted digital ID programs of some kind, the C6 represents a diversity of programs and shows that any analysis of the merits or demerits of digital ID programs should take this diversity into consideration. Different kinds of programs give rise to different kinds and degrees of privacy considerations.

France

On April 26, 2022, French President Emmanuel Macron signed the *Service de garantie de l'identité numérique* or the Digital Identity Guarantee Service (SGIN) into law.[24] SGIN is a smartphone application extension of the *Carte Nationale d'Identité* or the National Identity Card of France.[25] This microchipped electronic identification (eID) card authorizes users to access public and private services and to prove their identities online. Whenever users want to prove their identities online, they can simply place their eID on the back of their smartphones, whereupon they will be prompted to enter their PIN.[26] Once this PIN is successfully entered, the smartphone application securely reads and authenticates the data attributes contained within the eID.[27] Notably, users are able to control what information about them is shared with the service providers to whom they are required to prove their identities.[28] According to the Government of France website,

[24] "President Macron signs digital ID guarantee service decree," Keesing Platform, June 5, 2022, https://platform.keesingtechnologies.com/president-macron-signs-digital-id-guarantee-service-decree/. See also: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825?datePubli=.

[25] Frank Hersey, "France announces user-controlled mobile digital identity app for use with national ID," BiometricUpdate.Com, April 28, 2022, https://www.biometricupdate.com/202204/france-announces-user-controlled-mobile-digital-identity-app-for-use-with-national-id.

[26] "Keep control of your identity data," French Republic website, Accessed April 3, 2023, https://france-identite.gouv.fr/.

[27] French Republic website.

[28] French Republic website.

> The [digital ID] application will load the identification information contained in the chip of the identity card (last name, first name(s), date and place of birth, nationality, sex, postal and email addresses, photograph), except for fingerprints. This information will then allow authentication and connection to the desired services, but you will decide which data you agree to communicate via this application, after entering the PIN code attached to the identity card.[29]

Regulators regard the SGIN as an improvement over its predecessor, *Alicem.* According to the Alliance Vita website,

> In France, the regulator of personal data is known as the *National Commission for Information Technology and Civil Liberties* or the "*CNIL*". Previously, the *CNIL* was wary about *Alicem,* but last December the commission gave its approval to the new SGIN project, but stressed that it should not be compulsory, and should be user-friendly "for the general public, including those unfamiliar with digital technology". The commission also pointed out that, unlike *Alicem*, the application does not make it necessary to record more information than the one used to create an identity card.[30]

The modality of the SGIN of France, then, is a combination of a microchipped national identity card and a smartphone application. The intended functionality of the SGIN is for users to be able to authenticate claims made about their identities to online public and private service providers. Finally, the scope of the data captured by SGIN does not range beyond the scope of the data captured by the national identity card, if reports from Alliance Vita, the CNIL, and other sources are correct.

---

[29] "A digital identity mobile app coming soon," French Republic website, Accessed April 3, 2023, https://www.service-public.fr/particuliers/actualites/A15658?lang=en.

[30] "France creates a national digital identity service," Alliance Vita, May 13, 2022, https://www.alliancevita.org/en/2022/05/france-creates-a-national-digital-identity-service/.

The United Kingdom

Unlike France, the United Kingdom is determined to operationalize digital ID without the use of physical eID cards.[31] The UK is currently developing a smartphone or website digital ID and intends to make digital passports and licenses as credible as their physical counterparts.[32] Notably, the UK program purports to enhance privacy protections for its users by allowing users to exchange only the type and amount of personal information about them that is necessary to prove their identities or eligibility to service vendors.[33] For example, suppose a British user needed to prove her age to a service vendor to be eligible for the service; her digital ID allows her to prove her age without also having to disclose any other non-relevant information about herself, such as her address or weight. In this case, users appear to have more control over their data than when using traditional, physical identification documents. With traditional documents, users normally cannot help but share more information than is necessary when proving their identities or eligibility for services. Of this feature, the UK Government website states,

> There will also be more opportunities for "data minimisation". This is when information is only shared if it's needed to give a user access to a service. For example, when buying age-restricted products, a retailer only needs to know that a user is over a certain age e.g., "over 18". They do not need to see the rest of the information on their identity document. Making sure personal information is shared and managed securely will put users, services, and organisations at a lower risk of identity fraud.[34]

---

[31] Sebastian Skelton, "Cabinet Office looks to expand public data sharing for digital ID," *Computer Weekly*, January 13, 2023, https://www.computerweekly.com/news/252529178/Cabinet-Office-looks-to-expand-public-data-sharing-for-digital-ID.

[32] Emma Woollacott, "UK announces initial steps for national digital identities," Forbes, March 14, 2022, https://www.forbes.com/sites/emmawoollacott/2022/03/14/uk-announces-initial-steps-for-national-digital-identities/?sh=22e454e322e6.

[33] Woollacott.

[34] "Plans for governing body to make digital identities as trusted as passports," GOV.UK, July 19, 2021, https://www.gov.uk/government/news/plans-for-governing-body-to-make-digital-identities-as-trusted-as-passports.

Further, the United Kingdom appears to be committed to removing whatever barriers are preventing potential users from becoming actual users while, simultaneously, making enrollment voluntary. They note,

> To ensure digital identity products are available to as many people as possible, businesses will be required to report annually to the governing body on which users are excluded from using their services and outline what is being done to mitigate this. Equally, digital identity use will not be mandatory, and people will retain the option to use available report documentation.[35]

Another release from the UK Government states,

> Digital identity use will not be mandatory, and people will retain the option to use available paper documentation. Just as the government is committed to not making digital identities compulsory in the UK, it also wants to ensure that people in the future are not forced to use traditional identity documents if these are not strictly required.[36]

The modality of the digital ID of the United Kingdom, then, is a smartphone or website application. The intended functionality of the application is for users to be able to authenticate their identities (or claims made about their identities) to online public service providers. Finally, the scope of the data captured by the ID does not appear to be different than the scope of the data captured by traditional identification documents, such as licenses or passports, if cited sources are correct.

[35] GOV.UK.

[36] BiometricUpdate.Com, "UK plans to make digital ID."

Germany

The German government and the Deutsche Telekom Security firm recently launched a digital ID program that allows users to store their National ID on their smartphones as an electronic identification document (eID).[37] Using "near field communication" (NFC) technology, users will be able to tap their microchipped National ID cards on the back of their phones, whereupon the information from the National ID card will be uploaded to and securely stored on their eID. (Microchipped national identity cards have been mandatory in Germany since 2017.)[38] With an eID, German users can authenticate their identities, open bank accounts, confidentially send and receive medical records, access eGovernment services, and even vote from mobile devices.[39] The German government has promised that users will be able to use their eIDs to access more than 575 government services.[40] According to the Government Global Forum website,

> Similar to contactless payments a few years ago, consumers will quickly realise the benefits of having key credentials including their driving license, national health insurance cards, or even their car and apartment keys available on their mobile phone, securely stored at all times. Soon, they may also be able to remotely verify their identity to access and send confidential medical records, open a bank account, or vote using their smartphone.[41]

Some hope that this eID program will modernize Germany, which is, reportedly, "digitally shy" and behind the times in terms of the digitization of government and private services.[42]

---

[37] "Important information on the new electronic German ID card," German Missions in the United States, Accessed April 3, 2022, https://www.germany.info/us-en/service/02-PassportsandIDCards/id-card-important-information/917866.

[38] German Missions in the United States.

[39] Munyaradzi Makoni, "Germany to launch digital ID smartphone service," Global Government Forum, April 2, 2022, https://www.globalgovernmentforum.com/germany-to-launch-digital-id-smartphone-service/.

[40] Kate Connolly, "New ID law aims to help reduce 'digital shyness' in Germany," *The Guardian*, May 22, 2021, https://www.theguardian.com/world/2021/may/22/new-id-law-aims-to-help-reduce-digital-shyness-in-germany.

[41] Global Government Forum, "Germany to launch digital ID."

[42] Global Government Forum.

The German government is simultaneously participating in an international initiative to make international travel within Europe more efficient and secure. Spain and Germany are now developing a cross-border digital ID program that will allow the citizens of both countries to prove their identities and to access public and private services when travelling to the other country.[43] This is part of a broader initiative by the European Union to create a European Digital ID, which would allow European citizens to associate their national identifications with other personal documents like driver's licenses, qualifications, and bank accounts and to access goods and services beyond the confines of their own borders.[44]

The modality of the digital ID of the Germany, then, is a smartphone extension of the microchipped national ID card. The intended functionality of the application is for users to be able to authenticate claims made about their identities to online public service providers. Finally, the scope of the data captured by the ID does not appear to be different than the scope of the data captured by traditional identification documents, such as licenses or passports, if cited sources are correct.[45]

Japan

In 2022, the Government of Japan expedited its transformation toward modernization and digitization by making enrollment in the My Number Digital ID program a precondition of access to public health insurance.[46] Like the Social Insurance or Social Security Numbers of Canada and the US, the My Number program assigns a unique numeral of 12 numbers to

[43] Alessandro Mascellino, "Spain and Germany to test cross-border digital ID," BiometricUpdate.Com, August 2, 2021, https://www.biometricupdate.com/202108/spain-and-germany-to-test-cross-border-digital-id.

[44] Mascellino.

[45] If the German eID will contain digital car and apartment keys, the scope of the data captured by the eID will range beyond the scope of the data captured by traditional identification documents.

[46] Laura Dobberstein, "Japan to citizens: get a digital ID or health insurance gets harder," The Register, October 27, 2022, https://www.theregister.com/2022/10/27/japan_digital_id_push/.

each of its users.[47] My Number cards are microchipped and linked to documents such as drivers' licenses, tax accounts, and health insurance profiles.[48] Cardholders may use PINs to access online public services via the Mynaportal–an online system for registering and changing bank accounts, viewing health insurance information, checking pension info, and accessing other related services.[49] On digital ID, Minister for internal affairs and communications, Terada Minoru, stated,

> Through the response to Coronavirus it became clear that the delay in digitalization is a social issue, and there is a strong need for the digitalization of society as a whole. Under these circumstances, My Number Card is a key tool for the digitalization of public administration. In the future, a policy aiming to abolish health insurance cards has been indicated.[50]

The modality of the digital ID of Japan, then, is a microchipped card. The intended functionality of the application is for users to be able to authenticate claims made about their identities to online public service providers. Finally, the scope of the data captured by the ID does not appear to be different than the scope of the data captured by traditional identification documents, such as licenses or passports. Notably, however, enrollment in the My Number program was (for a time) a precondition of access to the health care system.[51] The government has since stated that citizens paying into a public health insurance plan will be able to access health care without a My Number card.[52]

---

[47] "Individual Number Card: My Number Card," The Japan Agency for Local Authority Information Systems, Accessed April 3, 2023, https://www.kojinbango-card.go.jp/en/.

[48] The Japan Agency for Local Authority Information Systems.

[49] The Japan Agency for Local Authority Information Systems.

[50] Dobberstein, "Japan to citizens."

[51] Dobberstein.

[52] Dobberstein.

Bologna, Italy

The Smart Citizen Wallet of Bologna, Italy, was released to the citizens of Bologna on March 29, 2022.[53] Smart citizen wallets are digital wallets that allow users to securely store digital identification documents such as government-issued documents, financial information, health care information, and more. Unlike the other digital ID programs surveyed thus far, this program is designed for more than authenticating the identities of their users. It is part of a more ambitious plan to improve the lives of the citizens of Bologna, according to government officials.[54] Bologna Mayor Matteo Lepore has said that the Smart Citizen Wallet is like a "supermarket points collection" program that rewards its users for behaviours deemed by the municipality to be virtuous. Virtuous actions may include recycling, using public transportation, managing energy efficiently, and avoiding fines.[55] The program does not purport to penalize what are deemed to be non-virtuous behaviours; instead, users with sufficiently high scores for virtuous behaviour are rewarded with goods, such as access to cultural events and discounts. Versions of this program are being used elsewhere in Italy already.[56]

The modality of this program, then, is a digital wallet stored on smartphones and web-based applications. The intended function of the program is for users to be able to authenticate their identities to others *and to motivate enrolled citizens to behave virtuously in order to gain access to exclusive goods and services*. Because citizens are encouraged to upload information about their virtuous behaviours, the scope of the data captured by this program is more expansive than the scope of the data captured by programs in countries like France, the UK, Germany, and Japan. This program allows the municipality of

[53] Kirsten Valeur, "Italy introduces an app, which rewards model citizens," May 19, 2022, https://www.trykkefrihed.dk/italy-introduces-an-app-which-rewards-model-citizens.htm.

[54] Valeur.

[55] Valeur.

[56] E.g., Rome

Bologna to know about (some of) the behaviours of their citizens across time and to build profiles of their identities.

China

In a briefing before the National People's Congress in May 2022, China Premier Li Keqiang stated that China would be implementing a national digital ID card by the end of that year. Chinese citizens are increasingly inter-provincially mobile, and many need to access goods and services beyond the provinces where their IDs are issued.[57] In some cases, citizens must return to their home provinces to access those goods or services. While the Chinese government had been testing digital ID in several major cities since 2018, the IDs were not operable beyond these cities, and the new national digital ID would extend coverage across the country.[58]

Most analyses of China equate social credit systems with digital ID. The two are related but distinct. Whether the social credit systems of China will be made interoperable with a national digital ID program remains to be seem. It is reasonable to assume that they will be. In many provinces of China, citizens are already embedded within social credit systems that reward them for good behaviour and penalize them for (what is thought to be) bad or criminal behaviour. For violating what many would consider to be unjust norms and laws (e.g., norms and laws against purchasing too many video games, having too many children, protesting the government, or behaving rudely toward others), participating citizens may experience a decline in their social credit score and may, therefore, be (e.g.) excluded from travelling or from qualifying for a mortgage, be publicly shamed, or be criminally prosecuted.[59] Such systems rely on sophisticated surveillance technologies that

[57] Keesing Platform, "China to launch nationwide digital ID."

[58] Keesing Platform.

[59] Canada's road to Beijing," Justice Centre for Constitutional Freedoms, August 9, 2022, https://www.jccf.ca/wp-content/uploads/2022/08/Canadas-Road-to-Beijing_FINAL.pdf.

are designed to capture the intimate identities of their participants. This is a case in which governments are using information technologies not only to prevent harms (or their conception of harms) but also to advance some positive vision of morality or the good.[60]

What can we learn from the C6?

Even this brief survey of digital ID initiatives in the C6 is informative. We have seen that some digital ID programs are (at least for now) non-mandatory (e.g., France, UK, Germany, Japan, and Bologna). Other programs are (or were) mandatory, or citizens faced significant social and financial penalties for failing to enroll. Further, we have seen that digital ID is presented to their users in different modalities: the plastic microchipped card, the smartphone application, the website-based application, or the Smart Citizen Wallet. Further, some programs allow users to control how much information about them is disclosed in transactions. In the UK and France, users can exchange only whatever information is required for them to access a good or service. In other countries, users do not appear to have this kind of control over their information. From another perspective, some programs capture only as much information about their users as is required to credibly prove the identities of their users. Some programs (e.g., the Smart Citizen Wallet of Bologna, Italy, or the digital ID programs of China) might be described as a tracking or profiling programs insofar as they capture data about the behaviours of their users across time (or, at least, insofar as their users are motivated, in the case of the Smart Citizen Wallet, to upload information about their behaviours to the program).

[60] Simina Mistreanu, "Life Inside China's Social Credit Laboratory," *ForeignPolicy.com*, April 3, 2018, https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.

II Digital ID initiatives in Canada

Canada is pursuing digital ID initiatives at the provincial, federal, and international levels. Most provinces have adopted digital ID programs of some kind. In 2018, the Canadian Bankers Association (CBA) released a white paper called *Canada's Digital ID Future – A Federated Approach*[61] in which the CBA called for a federated approach to a digital ID program that would coordinate every provincial digital ID within a federal framework. This ambition falls within the scope of Canada's Digital Ambition 2022,[62] developed by the Treasury Board of Canada Secretariat. According to this document, Canada's digital ambition is "[t]o enable delivery of government in the digital age for all Canadians. This will be done by providing modernized and accessible tools to support service delivery that expresses the best of Canada in the digital space."[63] digital ID is one dimension of the ambition to modernize service delivery in Canada. Between 2018 and 2022, Canada partnered with the World Economic Forum to deliver a pilot Known Traveller Digital Identity program to Canadian domestic and international travellers. More recently, the Digital Identity Authentication Council of Canada has been developing recommendations for a digital ID program that would change the way Canadians interact.

[61] "White Paper: Canada's Digital ID Future - A Federated Approach, Canadian Bankers Association, May 30, 2018, https://cba.ca/embracing-digital-id-in-canada.

[62] "Canada's Digital Ambition 2022," Government of Canada, Accessed April 3, 2022, https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html.

[63] Government of Canada.

The Known Traveler Digital Identity program

In this section, we provide an analysis of the pilot Known Traveler Digital Identity (KTDI) program of Canada and the World Economic Forum (WEF).[64] While it is unclear whether the federal government will continue to pursue this partnership or program, an analysis of the program is informative for three reasons. First, an analysis of the KTDI provides helpful material for the project of distinguishing between harmful and non-harmful programs. Second, an analysis of the path Canada *might have taken* (and still might take) illustrates what the federal government and the WEF are capable of and may help Canadians ask the right kinds of questions about any national program going forward. Finally, an analysis of the KTDI gives rise to interesting questions about consent, privacy, the conditions necessary for fair exchanges of information, access, equality, and the potential harms of surveillance programs.

According to a Government of Canada news release from January 25, 2018,

> The Government of Canada will collaborate with the World Economic Forum and partners to test emerging digital technologies and how they can improve security and the seamless flow of legitimate air travellers, with the launch of the Known Traveller Digital Identity prototype…
>
> The Known Traveler Digital Identity system takes emerging digital technologies such as advanced biometrics, cryptography, and distributed ledger technologies to give travellers control over, and the ability to share their information, via personal mobile devices, with governments and travel providers to facilitate and expedite progress from departure to destination airports, and beyond.[65]

[64] The purpose of this section is not to describe every Canadian Digital ID program; rather, the purpose of this section is to illustrate the ways in which some Digital ID programs are harmful or likely to be so.

[65] "The Government of Canada to test cutting-edge technologies to support secure and seamless global travel for air passengers," Government of Canada, January 25, 2018, https://www.canada.ca/en/transport-canada/news/2018/01/the_government_ofcanadatotestcutting-edgetechnologiestosupportse.html.

The modality of the program is the mobile device, and the KTDI is supposed to allow users to digitally authenticate their identities to travel authorities.[66] In its modality and intended function, therefore, the KTDI is not dissimilar from most of the programs encountered in the previous section. *In terms of the scope and kind of data captured by the program, however, the KTDI is importantly different than most of those programs.* The following statement from the WEF is worth quoting at length:

> The Known Traveller Digital Identity concept is designed to enable the voluntary sharing of information whereby the individual builds up trust in their digital identity. To build a trusted "Known Traveller" status, travellers need attestations–authenticated claims as declared by a *trusted* entity–to be added to their Known Traveller Digital Identity each time a trusted entity–such as a post office or a governmental or educational institution–verifies a claim. *In this concept, these attestations are the backbone of trust and the basis of reputation and, ultimately, how security decisions can be made.* Examples of attestations are proof of citizenship in country X, an educational degree from college Y, and proof of vaccination for viral disease Z. In the future, country A might authorize a traveller to enter the nation based on a previous risk assessment and the resulting attestation by country B. (emphasis added)
>
> Importantly, as it is currently proposed, travellers will consolidate attestations into a Known Traveller *profile* and increasingly strengthen their claim to *compliance*, trust, and legitimacy as a traveller. People continue to build the Known Traveller status by

[66] The application of the KTDI could range beyond the regulation of interactions between individuals and travel agencies. The following excerpt from the KTDI website suggests that the program could also be used to regulate interactions between individuals and governments, other "consortium parties", hotels, rental car agencies, and other agencies in the travel and tourism sectors. See: https://ktdi.org.

> acquiring more attestations, thereby contributing to a more secure and seamless traveller journey for all stakeholders.[67] (emphasis added)

Under the KTDI, the degree to which travellers are considered by travel authorities and state authorities to be compliant, trustworthy, and legitimate (and, therefore, eligible for travel or for access to ameliorated travel-related goods and services) depends on the degree to which otherwise private information about travellers is submitted to authorities. This information can be submitted to authorities in two ways. First, trusted agencies (e.g., post offices, post-secondary institutions, health agencies) can submit attestations or "credible claims" about travellers. Second, travellers can submit attestations about themselves on their own behalf. The following chart enumerates the information that travellers could submit about themselves and others in order to be perceived as being more trustworthy by travel authorities. Sections A, B, and C enumerate the information to which authorities have access already. Section D enumerates information that could be captured under the KTDI. For instance, travellers who submit information about their travel itineraries (past and present), purposes for travelling, identities of travel partners,[68] or medical information would be perceived by the program to be more trustworthy than those who did not (all else being equal).

---

[67] "The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel," World Economic Forum, January 2018, https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf, at page 14.

[68] This generates a host of privacy concerns. The KTDI motivates travellers to disclose their own personal information but also the personal information of others. Travellers are free to disclose whatever information they like about themselves. However, when travellers disclose the personal information of others, they may not have their consent to do so. The KTDI motivates travellers to violate the consent of others in order to be perceived as more trustworthy by the program. This program is rather radical, then. It allows for governments and the WEF to track the behaviours of consenting users *and non-users* (who are therefore non-consenting) across time.

Section A	Section B	Section C	Section D
Core data elements found in the Machine Readable Zone of the Official Travel Document (OTD)	**Additional data elements normally found in airline systems**	**Additional data not normally found in airline systems and which can be collected by, or on behalf of, an airline**	**Additional information that passenger could provide through the Known Traveller Digital Identity (as recommended by law-enforcement stakeholders)**
– OTD number – Issuing state or organization of OTD – OTD type – Expiration date of OTD – Surname/given name(s) – Nationality – Date of birth – Gender	– Seating information – Baggage information – Traveller's status – Place/port of original embarkation – Place/port of clearance – Place/port of onward foreign destination – Passenger name record locator number (or unique identifier)	– Visa number – Issue date of the visa – Place of issuance of the visa – Other document number used for travel – Type of other document used for travel – Primary residence – Destination address – Place of birth	– Contact number – Contact email – Countries visited on this trip prior to arrival – Flight number – Travel itinerary – Purpose of trip – Duration of trip – Extended travel history – People with whom travelling – Currency being brought into the country – Recent interactions with agriculture or livestock – Health information (e.g. vaccinations) – Criminal history (positive declarations) – Driving licence number

[69]

We suggest that the Known Traveller Digital Identity program generates four significant concerns. Each concern arises when Canadians exchange otherwise private information about themselves (or when trusted agencies submit that information on their behalf) in order to access ameliorated goods and services.

The classification problem

We recall that individuals can make themselves appear to be more trustworthy to travel authorities whenever "trusted entities" make attestations about their identities to those authorities. What we call *the classification problem* is the problem of determining what counts as a trusted entity or organization, i.e., an entity or organization whose attestations

[69] World Economic Forum, "The Known Traveller," at page 17.

matter. It is interesting to note that only state entities (e.g., post-secondary instutitions or public health agencies) are listed as examples of trusted entities. Charitable organizations, churches, unions, or corporations do not appear to count as entities that could make credible claims about the trustworthiness of Canadian travellers. Of course, entities that are not counted as trustworthy by governments or the WEF may nonetheless be able to make reliable attestations about the characters or reputations of individuals. Why should governments, the WEF, or state authorities be the only organizations capable of making credible claims about travellers, and why are many kinds of otherwise credible organizations precluded from making these claims on behalf of Canadians? This is a powerful shift. The KTDI appears to afford state institutions an immense amount of influence over determinations about the perceived trustworthiness of travellers.[70]

The relevance problem

What we call *the relevance problem* is the problem of determining whether attestations from (e.g.) healthcare agencies or post-secondary institutions say anything meaningful, relevant, or reliable about the trustworthiness of Canadians or about their eligibility for

[70] It could be argued that, *even now*, whether someone is eligible for domestic or international travel depends entirely on the attestations of state authorities and of no other entities or organizations. To board a plane today, Canadians must submit government-issued identification documents; documents from non-government entities do not count as proof-of-identity. It could be argued, then, that the classification problem is not a genuine problem or that, if it is, it is a problem that applies equally to traditional proof-of-identity requirements. In response, we say that it is not problematic for governments to be the only entities whose attestations about the kinds of facts captured by traditional identification documents (e.g., name, date of birth, address, etcetera) are accepted as proof-of-identity. For, the kinds of facts captured by traditional identification documents are usually non-controversial and are not facts with which alternative entities (e.g., charities, churches, or corporations) could reasonably disagree. The KTDI, however, proposes to capture facts about individuals that may be controversial. Facts about the reputations, characters, or trustworthiness of individuals normally do (and should) arise from a balance of sources and perspectives. For this reason, the classification problem applies only to the KTDI (and to similar Digital ID programs) but not to traditional proof-of-identity requirements as described in this report.

travel. It is difficult to see how attestations from one's university or post office could be relevant to determining the degree of risk one poses to others before, during, or after take-off. That the KTDI considers this kind of otherwise private information to be relevant to risk assessment suggests that the KTDI is something closer to (e.g.,) the Smart Digital Wallet of Bologna or the social credit systems of China than to mere digital counterparts to traditional identification documents.

The access problem

What we call *the access problem* is the problem that arises when individuals are excluded from accessing ameliorated goods and services (or goods and services of any kind) because they will not submit otherwise private information to travel authorities or because they do not have (e.g.) the kinds of academic credentials or vaccination records others may have. Under the KTDI, individuals who do not attend recognized academic institutions or who have not been vaccinated against relevant viruses will not be able to have attestations from those academic institutions or health agencies made on their behalf. They will not, therefore, be considered as trustworthy as those who do pursue higher education or who receive vaccinations for relevant viruses. As a result, they may not be eligible for access to ameliorated goods and services (or to goods and services of any kind).

The access problem is especially problematic for three reasons. First, it is unclear how (e.g.) possessing an academic degree could make one less of a liability to the travel industry than not possessing one. (This is the relevance problem restated.) If it cannot be shown that (e.g.) those who do not possess academic credentials pose more risk to the travel industry than those who do, then it seems unfair to restrict access to goods and services from those who do not possess academic credentials. Second, those who do not attend recognized academic institutions or who do not receive relevant vaccinations may have reasons for doing so *that do not reflect negatively on their characters or trustworthiness*. Further, some people experience prohibitive barriers to accessing these

kinds of credentials and should not thereby be excluded from accessing goods and services. Finally, the KTDI would inappropriately motivate Canadians not just to *be who they say they are* but to *be the right kind of person* (according to the government's conception of *the right kind of person*) in order to access goods and services. Canadians should not feel any pressure to attend academic institutions or to become vaccinated against relevant viruses in order to enjoy access to the goods and services to which they have always enjoyed access. There may be other, fine motivations for pursuing higher education or for being vaccinated, but access to domestic and international travel should not be one of them.[71]

The consent problem

Finally, what we call *the consent problem* arises when individuals consent to an exchange (e.g., an exchange of otherwise private information for access to goods and services) that is nonetheless unfair. According to the KTDI website,

> It is important to note that in order to be allowed to travel, the traveller must share all information required by the relevant entity (such as a border agency). However, the sharing of information is consent-based, and the traveller retains the right to decide which information to share and with whom.[72]

Some people hold the intuition that an exchange is fair whenever the parties to the exchange consent to it. If this is correct, then individuals who consent to exchanging otherwise private information for access to goods and services under the KTDI have participated in a fair exchange. In the case of digital ID and the KTDI, we think that this intuition is incorrect or that it only gets at part of the conditions that must be met for an

[71] The access problem here described may engage *Charter* Section 15 equality rights.

[72] "Unlocking the potential of digital identity for secure and seamless travel," Known Traveller Digital Identity, Accessed April 3, 2022, https://ktdi.org.

exchange to be fair. There appear to be many reasons for which an exchange that is consensual could be unfair. In this context, a consensual exchange may be unfair if:

> (1) one party cannot reasonably avoid the exchange,
> (2) one party demands something of greater value (e.g., the disclosure of private information) for something of lesser value (e.g., access to expedited airport security lanes), or
> (3) failure to consent to the terms of the exchange results in the unreasonable curtailment of any liberties protected by the *Charter*.

Whether the KTDI generates unfair exchanges depends on whether (a) submitting otherwise private information to the KTDI is necessary for access only to *ameliorated* travel-related goods and services or (b) submitting otherwise private information to the KTDI is necessary for access to domestic and/or international travel *of any kind*.[73]

Even if the KTDI asks Canadians to do no more than submit otherwise private information to access mere ameliorated goods and services, the KTDI would still be asking Canadians to submit sensitive personal information about themselves and others just to access a better airport experience. In this case, we think that the KTDI is asking for more than it is giving in return, and, therefore, is unfair for reason (2)–listed above. If, however, the KTDI is asking Canadians to submit private information about themselves and others to be eligible for domestic and/or international travel *as such*, then the KTDI is asking Canadians to enter into exchanges that are unfair for reasons (1), (2), and (3). Canadians who refuse to submit otherwise private information will be excluded from domestic and international travel and will have available to them no reasonable air travel alternatives. This would likely motivate Canadians to consent to an unfair exchange in order to access (what could be considered) an essential service. Further, requiring Canadians to disclose

[73] The language of the KTDI does not make clear whether (a) alone or (a) and (b) together is the case. This itself is problematic.

otherwise private information to be eligible for domestic and/or international travel would constitute an unreasonable curtailment of the right of all Canadians to enter and leave Canada as protected by Section 6 of the *Charter.*[74] Here, we have advanced a stricter requirement on the conditions for fair exchange. Even when parties consent to an exchange, the exchange itself may not be fair. When governments offer to exchange mobility rights for access to otherwise private information, we suggest that governments are acting unfairly.

The future of the KTDI is unknown in Canada. Whatever its future, an analysis of the program suggest that federal governments intend to implement digital identification programs that have significant profiling capacities and that generate significant problems surrounding consent, access, and the appropriateness of government's determining who is trustworthy. The KTDI would have motivated Canadians to engage in consensual but unfair transactions with their governments and the WEF. It would have caused conditions that discriminate against both organizations not perceived to be trustworthy and individuals unable to disclose (for various reasons, including non-consent or barriers-to-access) attestations about their trustworthiness. Even on the most charitable view, the KTDI is a kind of rewards program designed (in part) to profile Canadian travellers and to present significant barriers-to-access to non-compliant travellers.

The Digital Identification and Authentication Council of Canada

While Canada may not pursue a Known Traveler Digital Identity in partnership with the World Economic Forum going forward, prominent voices in government and industry are advocating today for programs that may generate similar privacy and ethics problems. One

[74] *The Canadian Charter of Rights and Freedoms*, Government of Canada, Accessed April 3, 2023, https://www.canada.ca/content/dam/pch/documents/services/download-order-charter-bill/canadian-charter-rights-freedoms-eng.pdf.

such voice is the Digital Identification and Authentication Council of Canada (DIACC), which is "a non-profit coalition of public and private sector leaders committed to developing a Canadian framework for digital identification and authentication".[75] The Board of Directors is composed of government officials and industry leaders from organizations like TD Bank, BMO, Desjardins, Telus, Interac, SecureKey, and Deloitte. The DIACC developed what they call The Pan-Canadian Trust Framework (PCTF) to digitize, secure, standardize, and improve interactions and information sharing between parties across various networks and organizations in Canada and beyond.[76] Such parties include individuals, corporations, and government entities. Trust frameworks are designed to ensure that participating entities can trust the information shared between all parties within the framework. The PCTF provides "consistent and auditable processes for the creation, management, and use of digital representations [of the identities] of people and other entities"[77] and "defines conformance criteria necessary for Digital Identity Ecosystem participants and users to interact with assurance".[78] A stated goal of the DIACC for the PCTF is "to facilitate the migration of traditional or complex face-to-face economic interactions to digital interactions"[79-80]

A full analysis of the Pan-Canadian Trust Framework is beyond the scope of this report. The digital ID program recommended by the DIACC may generate privacy or

[75] "Digital ID for Canadians," Digital Identification Council of Canada, Accessed April 3, 2022, https://diacc.ca/the-diacc/.

[76] "Pan-Canadian Trust Framework Model," Digital Identification Council of Canada, Accessed April 3, 2022, https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf.

[77] Digital Identification Council of Canada, at page 5.

[78] Digital Identification Council of Canada, at page 7.

[79] Digital Identification Council of Canada, at page 6.

[80] The DIACC states that the recognition of the existence of analogue processes is likely but not guaranteed. See: Digital Identification Council of Canada, at page 6.

ethical concerns that are not identified here. What follows is an evaluation of the potential privacy impacts of the kind and scope of user data captured by the PCTF of the DIACC.

In order for individuals to participate in the PCTF and, therefore, to access any of the goods or services offered by trusted entities within the PCTF, individuals must count as "PCTF Verified Person[s]",[81] i.e., they must conform to the processes and criteria that allow participating entities to trust that those individuals are "real, unique, and identifiable".[82] The following excerpt from the DIACC PCTF Final Model Recommendation defines processes and conformance criteria for verifying participating persons and for creating and attributing digital identities to them.

> The Verified Person component of the PCTF defines processes and specifies Conformance Criteria for:
>
> 1. **Verifying a person** - The processes that ensure the digital identity of a Person is an accurate representation of that Person and can be relied on for digital service delivery and digital transactions. A Verified Person is a real, unique and identifiable human being at the moment of Verification; and within the PCTF context such a person can be subject to legislation, policy, or regulations within a context. These processes ensure that a Person has been properly verified, and that they are the Person who initiated, directly or through a legally authorized representative, the request for a service or a transaction.
> 2. **Creating a trusted digital identity for a person** - The processes used to establish and maintain a digital record for a Verified Person in order to uniquely distinguish them from other Persons. The processes ensure that a digital record of a Person is properly created, used exclusively by that same Person either directly or aided by their legally authorized representative, and can be relied on for online transactions. This is also referred to as a Verified Person record.
>
> [83]

Digital records of Verified Persons will include two types of information (evidence) about those persons: foundational and contextual. Foundational evidence (e.g., the digital equivalents of driver's licenses or birth certificates) will be generated only by entities in the public sector, such as "Vital Statistics organizations of the provinces and territories,

[81] Digital Identification Council of Canada, at page 10.

[82] Digital Identification Council of Canada, at page 10.

[83] Digital Identification Council of Canada, at page 10.

Immigration, Refugees, and Citizenship Canada".[84] Whatever information about Canadians is collected by public-sector entities can count as foundational evidence and can, therefore, be captured by the PCTF in compliance with existence laws and regulations. What is meant by contextual evidence is less clear, but non-public-sector entities, such as "public and private and non-profit identity providers" can generate contextual evidence about individuals, and the PCTF can capture whatever contextual evidence about individuals is generated by these entities in compliance with existing laws and regulations.[85]

What kind of data could count as contextual evidence? The DIACC suggests that the verification of biological or behavioural data could count as the kind of evidence necessary for the verification of the identities of participating individuals. Listed examples of biological data include fingerprints.[86] In another place, listed examples of behavioural data include smartphone typing speed, touch-screen pressure, or walking gait as determined by a smartphone or mobile-device accelerometers.[87] In another place, the DIACC suggests that confirmation of digital identities may depend on "[t]he dynamic confirmation that a subject has a continuous existence over time (i.e., 'genuine presence')."[88] Of course, one cannot prove that a subject has a continuous existence across time unless there is evidence of that subject existing across time. Such evidence will likely not be (or will not be limited to) the kind of evidence currently captured by public-sector entities, e.g., evidence of bankruptcy, of change-of-address, or of the registration of a business. Such events normally occur with insufficient frequency to prove the continuous existence of a subject across time. The language of the DIACC's recommendation opens the door for the

[84] Digital Identification Council of Canada, at page 21.

[85] Digital Identification Council of Canada, at page 21.

[86] Digital Identification Council of Canada, at page 27.

[87] "PCTF Verified Person Component Overview," Digital Identification Council of Canada, Accessed April 3, 2023, https://diacc.ca/wp-content/uploads/2020/09/PCTF-Verified-Person-Component-Overview-Final-Recommendation_V1.0.pdf, at pages 4 and 5.

[88] "Pan-Canadian Trust Framework Model," Digital Identification Council of Canada, at page 27.

gatekeepers of digital ID programs to capture and store evidence about the *behaviours* (which, when taken all together, are sufficient to prove continuity of existence) of subjects across time.

Like the Known Traveler Digital Identity program of the previous pages, the PCTF of the DIACC describes criteria to which individuals and entities must conform to be considered sufficiently trustworthy for transactions to occur. And, like the KTDI, the PCTF would capture data about Canadians that ranges far beyond the scope of data captured today by traditional identification systems. Future approaches to digital ID programs will likely capture and store biological and behavioural data about Canadians unless Canadian privacy laws are amended to prohibit this. Unfortunately, Canada does not appear to be moving in this direction. For instance, on September 22, 2022, the Québec government adopted Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, which regulates (and, therefore, conditionally allows for) the profiling of the citizens of Québec. According to Section 65.0.1 of the *Act*, "profiling" refers to "the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests, or behaviour."[89]

[89] "Bill 64: An Act to modernize legislative provisions as regards the protection of personal information," National Assembly of Québec, Accessed April 3, 2023, https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/190120/sq-2021-c-25.pdf, at 65.0.1.

III Drawing a distinction between digital ID programs

We must share something of ourselves with others to establish a sufficient degree of trust to conduct transactions with others. This is an unavoidable cost of living in communities with others who are unknown (or insufficiently known) to us. Identification documents of any kind (whether physical or digital) allow their users to credibly authenticate claims about their identities to others. Ordinary identification documents contain information about their users, such as their age, sex, weight, eye-colour, or place of residence. Notably, the identification documents with which most Canadians are familiar (provincial IDs, driver's licenses, or passports) do not contain reference to any information about the behaviours, personalities, or preferences of their users. Drivers' licenses do not track the mobility habits of their possessors. Passports do not, in the usual cases, track where you travel.[90] In the usual cases, your physical identification documents contain just enough information about you to allow you to credibly authenticate specific claims made about your identity (e.g., "I am 18 years old,") or to differentiate you from other individuals.

There is a significant degree of variation between the digital ID programs being implemented across the world today. Regarding their modality, most programs are delivered to users in the form of smartphone or web-based applications, and some are delivered in the form of microchipped, plastic cards. Regarding the scope of the captured data, most programs capture only the kind and amount of data captured by traditional identification documents. Notably, some programs (i.e., the Known Traveller Digital Identity) are described as capturing only the kind and amount of data contained on traditional identification documents *but do, in fact, capture much more than that.* Some programs track the behaviours of their users across time (either with or without consent)

[90] In some cases, traditional identification documents *do* track (or contain record of) the mobility behaviours of their possessors across time. Canadian passports may be stamped by the border officials of Canada or other countries, thereby leaving a record for others to see of your mobility behaviours across time.

and use whatever information is collected to build profiles of their users. In the case of Canada's Known Traveller Digital Identity program, theoretical users are motivated to submit unnecessary information about themselves and their travel itineraries in order to build credibility or trust with the governments and travel authorities with whom they interact. The digital ID of the Pan-Canadian Trust Framework could capture data about the bodies and behaviours of their users.

There are many ways to distinguish between or classify digital ID programs. In many analyses, whatever distinctions are drawn tend to fixate on the modality of the digital ID program. In other words, many regard the distinction between physical identification documents and digital identification documents as "getting at" the distinction between non-harmful and harmful digital ID programs. We suggest that drawing the distinction in this way is problematic; certain digital ID programs appear to be privacy-neutral (i.e., no more harmful than their counterpart physical identification documents) or even privacy-enhancing.

Accordingly, we suggest that the most interesting and productive distinction between digital ID programs pertains to the scope and kind of captured data. Specifically, we suggest that digital ID programs should be classified into the following categories:

(a) Digital ID programs that track data pertaining to the biology, behaviours, personalities, and/or preferences of their users
(b) Digital ID programs that do not track data pertaining to the biology, behaviours, personalities, and/or preferences of their users[91]

[91] We suggest that programs that do not track data pertaining to the biology, behaviours, personalities, and/or preferences of their users do not (*ceteris paribus*) generate significant threats to the fundamental rights and freedoms of Canadians. Or, whatever threats are generated by these programs are not unique to those programs; they are no more a threat to the rights and freedoms of Canadians than the physical identification documents with which Canadians are already familiar.

The above distinction can be regarded as the (imperfect but nonetheless helpful) distinction between:

(a) Tracking and/or profiling digital ID programs
(b) Digital counterparts to traditional identification documents

Digital ID programs that capture more data about their users than is necessary for authentication or proof-of-identity can be regarded as *something more than* mere digital counterparts to traditional identification documents. Such programs are designed to perform functions over and above the credible authentication of their users. They are designed to capture data about the bodies and behaviours of their users and, in some cases, to use this captured data to develop sophisticated profiles of their users. In some cases, users are invited to contribute that data themselves to access faster and more convenient services.

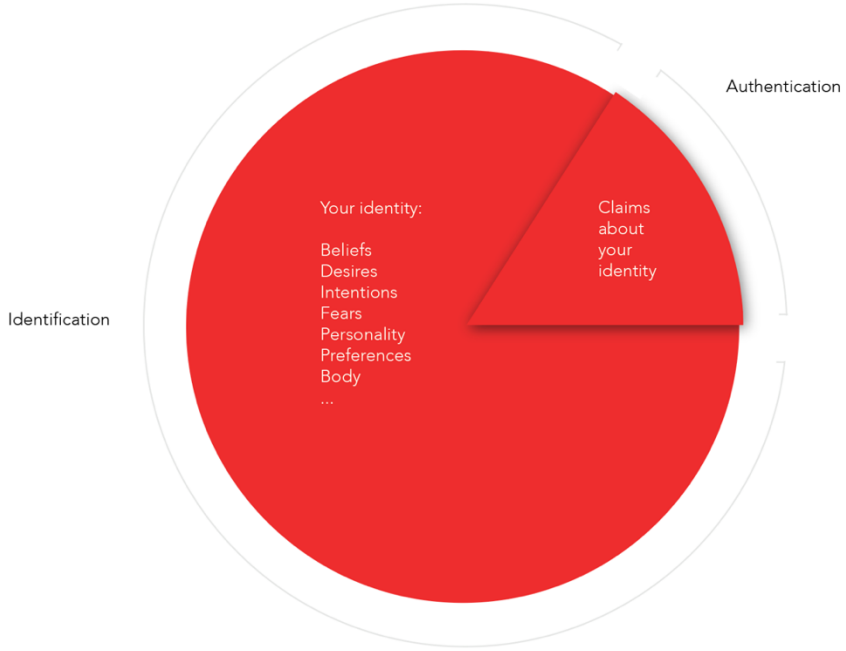
The above distinction can also be regarded as the distinction between authentication and identification programs. According to the Canada Banker's Association's (CBA) 2018 white paper on "Canada's Digital ID Future–A Federated Approach," there is an important difference between the identity of a person (understood as a whole or totality) and the subset of facts about the identity of a person that must be shared with others to establish a sufficient degree of trust for a transaction to occur. The CBA writes,

> *Identity* is the representation of who you are…It is important to differentiate between digital *identification* and digital *authentication*. Digital authentication is something most of us do every day–logging on to our favourite social media site, signing into an account with our preferred ecommerce retailer, or even accessing our mobile device through a thumb scan. Authentication is the act of proving that the person accessing my account or device is me, usually through a PIN, password, biometric identifier, or other form factor. Authentication is designed to answer the question "*Is that you?*" Identification, by contrast, is more complex. Identification is intended to answer the question "*Who are you?*" Digital

> ID is the challenge of answering "Who are you? With a high degree of certainty, without resorting to face-to-face interaction and the exchange of physical documents.[92]

There is a distinction, then, between identification and authentication, and it is a distinction that even a proponent of a national digital ID program acknowledges. This distinction is helpfully compatible with the distinction between harmful and non-harmful digital ID programs advanced in this report. Tracking and profiling programs attempt to understand the identities of their users. In addition to allowing users to authenticate specific and limited claims about their identities, these programs have the (theoretical) capacity to capture or model information about who their users *really* are: (e.g.) information about their beliefs, desires, intentions, fears, personality, preferences, bodies, and histories. On the other hand, mere authentication programs capture only enough information about their users to allow service providers sufficient reason to think that their users are who they say they are. Of course, mere authentication programs must capture some information about the identities of their users: (e.g.) their height, weight, address, age, etcetera. Nonetheless, mere authentication programs are modest about how much information is needed to establish that degree of trust and do not peer too deeply into the intimate lives of their users.

[92] "White Paper: Canada's digital ID future–A federated approach," Canadian Bankers Association, May 30, 2018, https://cba.ca/embracing-digital-id-in-canada.



With this distinction in mind, we claim that neither governments nor their partnering agencies have any business knowing about the intimate identities of their citizens. Not only is it unnecessary for governments to know this information, governments knowing this information gives rise to intolerable practical and ethical problems that exposes citizens to unnecessary risks and harms. What these risks and harms are will be the focus of Part Two of this report.[93]

[93] Part Two will be released before June 30, 2023.

Conclusion

This report identified a tension between digital ID and privacy. In Part One, we suggested that digital ID programs have the potential to threaten the enjoyment of privacy in Canada. After surveying and identifying problems with the KTDI and PCTF, we suggested that the distinction between non-harmful and harmful digital ID programs is really the distinction between:

(a) Digital ID programs that track data pertaining to the biology, behaviours, personalities, and/or preferences of their users
(b) Digital ID programs that do not track data pertaining to the biology, behaviours, personalities, and/or preferences of their users

Further, we believe that an awareness of this distinction is helpful for potential and actual users of digital ID. This distinction may help Canadians to understand where the line between non-harmful and harmful identification programs lies and to be vigilant "in the right direction". Whether or to what extent a federal Canadian digital ID limits the enjoyment of privacy in Canada will depend on the following: how Canadian governments and partnering agencies design a federated digital ID, how robust legislative protections are, and how invested Canadians are in the protection of private spaces against government surveillance and overreach.

In closing, it is encouraging to note that peaceful citizen activism has affected how governments implement digital ID programs in Germany, Japan, and Saskatchewan. In Germany, where a national digital ID program is non-mandatory, many citizens are refusing to enroll in the program as a result of their experiences with authoritarian regimes and their concern that government agencies will have excessive access to their personal information. As Connolly of *The Guardian* writes,

> [A] lack of joined-up technology, together with bureaucrats' own reluctance and a general mistrust of identity cards–often due to the experience of the Nazi and GDR dictatorships–led to the so-called eID hardly being used in the way it was intended…Some data protection experts have weighed in, insisting Germans are being forced to digitise their lives against their will and arguing that the eID will give law enforcement agencies and tax officials too much access to citizens' information and photo IDs.[94]

In Japan, where a national digital ID was initially required for access to the public health care system, 100,000 citizens signed a petition demanding that enrollment in the program not be mandatory for accessing the health care system. The petition was successful. According to *CTV News*,

> On Monday [October 24, 2022], Prime Minister Fumio Kishida acknowledged concerns about *My Number* cards. He told lawmakers in Parliament that the old health insurance cards will be phased out, but the government will arrange for people to continue to use their public health insurance if they are paying into a health plan.[95]

Interestingly, Japanese citizens appear to share similar concerns with German citizens. Both appear to draw from their experiences with authoritarian regimes and recognize the relationship between surveillance and the violation of private spaces, moral wrongness, and social harms. According to Kageyama of the *Associated Press,*

> But the [Japanese] reluctance to go digital extends beyond the health care system. After numerous scandals over leaks and other mistakes, many Japanese distrust the government's handling of data. They're also wary about government overreach, partly a legacy of authoritarian regimes before and during World War II.[96]

---

[94] *The Guardian,* "New ID law."

[95] Yuri Kageyama, "Japan steps up push to get public buy-in to digital IDs," *The Associated Press*, October 24, 2022, https://www.ctvnews.ca/sci-tech/japan-steps-up-push-to-get-public-buy-in-to-digital-ids-1.6123460.

[96] Kageyama.

The story of digital ID in Saskatchewan is an interesting case study about data capture, privacy, and the power of provincial governments and their citizens to determine the appropriateness and kind of provincial digital ID programs that are implemented. In April 2022, the Saskatchewan government halted the development of its digital ID program. Saskatchewan Minister of SaskBuilds and Procurement Jim Reiter stated that the government "was working closely with the information and privacy commissioner on any issues the ID would cause, and that it was still quite early in the planning stages," according to *CBC*.[97] The Saskatchewan government later stated, "At this time we think it is reasonable to observe the uptake in other provinces to see if people are using it, understand the benefits, and to identify the best ways to protect citizens' privacy and security."[98] This kind of caution is, in our view, appropriate. In June 2022, the Saskatchewan Information and Privacy Commissioner tabled a report on digital ID with the provincial legislative assembly, calling for a provincial digital ID that would meet the province's needs, maximize benefits, and reduce risks. The Commissioner noted that a digital ID would allow users to virtually authenticate their credentials to health authorities and would reduce the rate at which faxes containing private information were misdirected.[99-100]

While Saskatchewan is making progress to implement a provincial digital ID, the government has simultaneously refused to surrender private medical information to Ottawa via a national digital ID program in exchange for additional healthcare funding under the

[97] "Saskatchewan quashes digital ID plan–for now," *CBC*, April 1, 2022, https://www.cbc.ca/news/canada/saskatchewan/sask-digital-id-1.6405362.

[98] *CBC.*

[99] "Saskatchewan Information and Privacy Commissioner Tables 2021-2022 Annual Report," Office of the Saskatchewan Information and Privacy Commissioner, June 28, 2022, https://oipc.sk.ca/saskatchewan-information-and-privacy-commissioner-tables-2021-2022-annual-report/.

[100] This is another case in which digital ID may be privacy-enhancing (or in which digital ID overcomes a privacy-harming feature of traditional identification systems).

recently proposed Canada Healthcare Transfer agreement.[101] According to the *Western Standard*, Premier Scott Moe stated,

> The Government of Saskatchewan will not share any personal medical information with the federal government. This information is protected under *The Health Information Protection Act* and will remain so…The only information the Saskatchewan government reports publicly is healthcare statistics, and Moe is willing to do that. But [Moe is willing to share] only publicly available statistics, such as surgical wait times.[102]

This case demonstrates that provincial governments can appeal to robust privacy laws (whenever these laws exist) to legally protect Canadian information. This case also demonstrates that the disappearance of private spaces is often the result of voluntary exchanges of those spaces for promised benefits, such as increased healthcare funding (or, in the case of Japan, access to the public healthcare system). These cases demonstrate that Canadians can negotiate with their governments on the conditions of access to public goods and services and can protect properly private spaces from the incursions of state surveillance.

Looking ahead to Part Two

In Part Two (forthcoming), we explore why surrendering otherwise private spaces to government oversight *matters*. Part Two explores and defends the (commonly held) intuition that privacy is valuable. That privacy is valuable is not a universal belief, however, and its value will have to be carefully and forcefully articulated in future public

[101] Christopher Oldcorn, "Moe says no to healthcare digital IDs after public outcry," *Western Standard,* February 2, 2023, https://www.westernstandard.news/news/moe-says-no-to-healthcare-digital-ids-after-public-outcry/article_c47a30ee-a337-11ed-b551-6f4bccdddfcb.html.

[102] Oldcorn.

policy debates, especially when so many participants in those debates *devalue* privacy and o*vervalue* the convenience and safety that supposedly arises from the implementation of surveillance technologies.

This report follows many in the information technology ethics and privacy literature in saying that privacy is necessary (where surveillance technologies are concerned) for the enjoyment of security, autonomy, and human dignity. In Part Two, we will evaluate case studies and show that digital ID initiatives may undermine the security of both those who enroll and do not enroll in those initiatives; personal data can be hacked by external actors or used by government or corporate agencies to unjustifiably curtail liberties. Further, we show that surveillance initiatives (whether in the form of digital ID or otherwise) may undermine autonomy and expressive freedoms. That is, surveillance programs tend to have a chilling or quieting effect on expression, and this can be regarded as a harm. Finally, we show that profiling programs undermine human dignity. The human being is not a specimen or object of study, and governments commit an "epistemic immodesty" whenever they attempt to know the "deep" or "intimate" identities of their citizens.

Bibliography

Alliance Vita. “France creates a national digital identity service.” May 13, 2022. https://www.alliancevita.org/en/2022/05/france-creates-a-national-digital-identity-service/.

Canadian Bankers Association. “White Paper: Canada’s digital ID future–A federated approach.” May 30, 2018. https://cba.ca/embracing-digital-id-in-canada.

CBC. “Saskatchewan quashes digital ID plan–for now.” April 1, 2022. https://www.cbc.ca/news/canada/saskatchewan/sask-digital-id-1.6405362.

Connolly, Kate. “New ID law aims to help reduce ‘digital shyness’ in Germany.” *The Guardian*. May 22, 2021. https://www.theguardian.com/world/2021/may/22/new-id-law-aims-to-help-reduce-digital-shyness-in-germany.

Digital Identification Council of Canada. “Digital ID for Canadians.” https://diacc.ca/the-diacc/.

--- “PCTF Verified Person Component Overview.” https://diacc.ca/wp-content/uploads/2020/09/PCTF-Verified-Person-Component-Overview-Final-Recommendation_V1.0.pdf.

--- “The economic impact of digital ID in Canada.” https://diacc.ca/wp-content/uploads/2018/05/Economic-Impact-of-Digital-Identity-DIACC-v2.pdf.

--- “Pan-Canadian Trust Framework Model.” https://diacc.ca/wp-content/uploads/2020/09/PCTF-Model-Final-Recommendation_V1.0.pdf.

Dobberstein, Laura. “Japan to citizens: get a digital ID or health insurance gets harder.” The Register. October 27, 2022. https://www.theregister.com/2022/10/27/japan_digital_id_push/.

French Republic website. “A digital identity mobile app coming soon.” https://www.service-public.fr/particuliers/actualites/A15658?lang=en.

--- "Keep control of your identity data." https://france-identite.gouv.fr/.

German Missions in the United States. "Important information on the new electronic German ID card." https://www.germany.info/us-en/service/02-PassportsandIDCards/id-card-important-information/917866.

Government of Canada. "*The Canadian Charter of Rights and Freedoms*." Government of Canada. https://www.canada.ca/content/dam/pch/documents/services/download-order-charter-bill/canadian-charter-rights-freedoms-eng.pdf.

--- "Canada's Digital Ambition 2022." https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html.

--- "Digital Credentials." https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html.

--- "The Government of Canada to test cutting-edge technologies to support secure and seamless global travel for air passengers." January 25, 2018. https://www.canada.ca/en/transport-canada/news/2018/01/the_government_ofcanadatotestcutting-edgetechnologiestosupportse.html.

GOV.UK. "Plans for governing body to make digital identities as trusted as passports." July 19, 2021. https://www.gov.uk/government/news/plans-for-governing-body-to-make-digital-identities-as-trusted-as-passports.

Hersey, Frank. "France announces user-controlled mobile digital identity app for use with national ID." BiometricUpdate.Com. April 28, 2022. https://www.biometricupdate.com/202204/france-announces-user-controlled-mobile-digital-identity-app-for-use-with-national-id.

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

The Japan Agency for Local Authority Information Systems. "Individual Number Card: My Number Card." https://www.kojinbango-card.go.jp/en/.

Juniper Research. “Digital Identity: Solutions assessment, regional analysis, & market forecasts 2023-2017.” February 27, 2023. https://www.juniperresearch.com/researchstore/fintech-payments/digital-identity-research-report.

Justice Centre for Constitutional Freedoms. “Canada’s road to Beijing.” August 9, 2022. https://www.jccf.ca/wp-content/uploads/2022/08/Canadas-Road-to-Beijing_FINAL.pdf.

Kageyama, Yuri. “Japan steps up push to get public buy-in to digital IDs.” *The Associated Press*. October 24, 2022. https://www.ctvnews.ca/sci-tech/japan-steps-up-push-to-get-public-buy-in-to-digital-ids-1.6123460.

Keesing Platform. “China to launch nationwide digital ID card in 2022.” March 24, 2022. https://platform.keesingtechnologies.com/china-to-launch-nationwide-digital-id-card-in-2022/.

--- “President Macron signs digital ID guarantee service decree.” June 5, 2022. https://platform.keesingtechnologies.com/president-macron-signs-digital-id-guarantee-service-decree/. See also: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825?datePubli=.

Mascellino, Alessandro. “Spain and Germany to test cross-border digital ID.” BiometricUpdate.Com. August 2, 2021. https://www.biometricupdate.com/202108/spain-and-germany-to-test-cross-border-digital-id.

Makoni, Munyaradzi. “Germany to launch digital ID smartphone service.” Global Government Forum. April 2, 2022. https://www.globalgovernmentforum.com/germany-to-launch-digital-id-smartphone-service/.

Mistreanu, Simina. “Life Inside China’s Social Credit Laboratory.” *ForeignPolicy.com*. April 3, 2018. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.

Murdoch, Anthony. “Canadian gov’t looking to implement digital ID program despite concerns of privacy experts.” *Life Site News.* August 12, 2022. https://www.lifesitenews.com/news/canadian-govt-looking-to-implement-digital-id-program-despite-concerns-of-privacy-experts/.

National Assembly of Québec. “Bill 64: An Act to modernize legislative provisions as regards the protection of personal information.” https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/190120/sq-2021-c-25.pdf.

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/.

Office of the Saskatchewan Information and Privacy Commissioner. “Saskatchewan Information and Privacy Commissioner Tables 2021-2022 Annual Report.” June 28, 2022. https://oipc.sk.ca/saskatchewan-information-and-privacy-commissioner-tables-2021-2022-annual-report/.

Oldcorn, Christopher. “Moe says no to healthcare digital IDs after public outcry.” *Western Standard.* February 2, 2023. https://www.westernstandard.news/news/moe-says-no-to-healthcare-digital-ids-after-public-outcry/article_c47a30ee-a337-11ed-b551-6f4bccdddfcb.html.

Secure ID News. “Australia considers digital ID age verification for porn.” January 14, 2020. https://www.secureidnews.com/news-item/australia-considers-digital-id-age-verification-for-porn/.

Skelton, Sebastian. “Cabinet Office looks to expand public data sharing for digital ID.” *Computer Weekly*. January 13, 2023. https://www.computerweekly.com/news/252529178/Cabinet-Office-looks-to-expand-public-data-sharing-for-digital-ID.

Thales Group. “Five reasons for electronic national ID cards.” March 29, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/5-reasons-electronic-national-id-card.

Woollacott, Emma. “UK announces initial steps for national digital identities.” Forbes, March 14, 2022,. https://www.forbes.com/sites/emmawoollacott/2022/03/14/uk-announces-initial-steps-for-national-digital-identities/?sh=22e454e322e6.

World Economic Forum. “The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel.” January 2018. https://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

Valeur, Kirsten. “Italy introduces an app, which rewards model citizens.” May 19, 2022. https://www.trykkefrihed.dk/italy-introduces-an-app-which-rewards-model-citizens.htm.