DIGITAL IDENTITY SECURITY FRAMEWORK GUIDE

VERSION OF 12 APRIL 2022

GRIC

UDS Université de Sherbrooke

TABLE DES MATIÈRES

ACKNOWLEDGEMENTS

This guide was funded by the Office of the Privacy Commissioner of Canada under the 2021-2022 Contributions Program. The views expressed herein are not those of the Office of the Privacy Commissioner or the Government of Canada.

THE FOLLOWING PEOPLE CONTRIBUTED TO THE WRITING OF THIS GUIDE:

- Mr. Benjamin Ali Aboudou
- Ms. Samiha Abounouar
- Ms. Marylise Caron
- Pr Daniel Chamberland-Tremblay
- Mr. Félix Gariépy
- Pre Manon Ghislaine Guillemette
- Pr Hugo Loiseau
- Mr. Moumouni Krissiamba Ouiminga
- Professor Arthur Oulaï
- Mr. Claudiu Popa
- Mr. Aboubakar Séhéna Soro
- Pr Pierre-Martin Tardif

THE FOLLOWING PEOPLE CONTRIBUTED TO THE IMPROVEMENT, EDITING, LAYOUT AND TRANSLATION OF THIS GUIDE:

- Pascale Beausoleil

1. SETTING THE CONTEXT

Without a doubt, digital identity is a complex subject that needs to be popularized. Digital identity, its legal frameworks, and its management systems raise questions. The purpose of this guide is to provide answers to questions about the many aspects surrounding digital identity in Canada. Executives and boards of directors are responsible for the digital identity of their customers, employees, and suppliers. The digital identity ecosystem is framed by several laws and regulations and is part of the larger reality of cyber security. In other words, the challenges are great for private sector organizations!

This Guide begins, in section 2, outlining what digital identity is and the multiple approaches that drives it. Section 3 indicates how and why digital identity impacts your organization. Then, in section 4 the Guide outlines why protecting digital identity has become an important factor in an organization's success in Canada. This section describes how to manage the digital identity ecosystem for a private sector organization in Canada. The final section of the Guide examines the benefits and opportunities that good digital identity management can bring to an organization.

1.1. A SHORT STORY

The development of the Internet and the advent of the information society in the early 2000's brought many opportunities, but also many challenges. Among these, the need for organizations to be able to identify and authenticate online with confidence the entities with which they conduct transactions. It is with the objective of responding to this imperative that the concept of digital identity was developed (which we define in section 2.1 of the document). Digital identity is becoming increasingly important in our society, as proved by the Quebec government's announcement in 2019 of the creation and implementation of the Service québécois d'identité numérique (SQIN) aimed at providing each member of the Quebec population with a digital identity. The pandemic has highlighted society's need for a strong digital identity since in-person services were no longer available. While digital identity has an important technical component, it goes much further by also involving legal, social, management, and governance elements.

1.2. WHO IS THIS DOCUMENT FOR?

This document is intended to inform the owners and management team of every organization in Canada about all aspects of the digital identity framework for individuals. It is written in plain and neutral language. It is written in a question-and-answer format for easy reference. It is suggested that you read the sections that really interest you, at least the sections 2.3, 3.1, 3.3, 3.4, 4.1, 4.2, 4.3, 5.2, 5.3, 5.4, 6.1, and 7.

Although the authors have taken great care to provide reliable and up-to-date information as of 12 April 2022 the issues and rules applicable to digital identity are rapidly evolving. This document does not constitute legal advice and should not be used as a substitute for a personalized analysis of the business process being considered by a professional. The reader is invited to remain vigilant since the applicable legal framework, particularly with respect to the protection of personal information, may differ from one jurisdiction to another, and depending on the type of organization.

1.3. WHY TALK ABOUT IT NOW?

Information technology (IT) is omnipresent in organizations of all sizes and business areas. They allow a large quantity of information to be acquired, stored, processed, and transmitted in a very short period. Among the information processed by an organization, there is personal data that identifies the people with whom it deals. This data (see section 2.3) can be sensitive personal information. As a responsible organization, it is imperative to protect it adequately, or risk losing one's reputation and becoming a victim of legal action.

The current context is more than favorable to take an interest in digital identity. On the one hand, several laws that aim to encourage organizations to adopt responsible behaviors in managing sensitive data have recently been passed in Canada. This data includes personal information, such as the digital identities of each citizen. Moreover, digital identity management is at the heart of the digital transformation many governments undertake around the world. This new approach affects all citizens, but also all organizations that do business with governments, their employees, and their partners. It is therefore a whole ecosystem that is being put in place, and to which Canadian organizations are or will be exposed in the very short term.

Finally, it goes without saying that data cybersecurity is front and center in the news and on the minds of citizens and organizations. While cybersecurity goes far beyond protecting data, it is still increasingly targeted for attack and is the basis of a very lucrative business model. While a few years ago data theft was primarily targeted at personal information, a new trend is emerging where the theft of personal information is also accompanied by the theft of coveted business data. Digital identities must therefore be managed securely by Canadian organizations.

2. DIGITAL IDENTITY

2.1. WHAT IS DIGITAL IDENTITY?

Digital identity is the set of identification data of a natural or legal person and consisting of digital identifiers that allow to represent him univocally. This definition is inspired by Article 2 of Law No. 1.483 of December 17, 2019, on the digital identity of the Principality of Monaco (see p. 3870, Journal de Monaco of Dec. 27, 2019). However, there is no consensus, either in research or legally, as to the exact nature of digital identity.

2.2. IS A CONSENSUS ON THE DEFINITION OF DIGITAL IDENTITY POSSIBLE?

The definition of digital identity can vary by discipline and even within the same discipline.

However, Recommendation ITU-T X.1252[1] reflects the need to converge on a relative consensus in the identity management field, at least at the terminological level. By providing nearly 99 definitions for digital identity concepts, the latest version of the Recommendation, dated April 2021, aims to clear up confusion.

Digital identity is presented as the product of attributes, a bit like the real world which relies on the physical or social characteristics of a person to distinguish him. However, we take the opportunity to clarify that digital identity management does not only consist of singling out physical or moral persons, but it also extends to inanimate objects which, in addition to a device, a software application or a service, can turn out to be, in the context of telecommunications, an access point, a subscriber, network elements and many other things. For this reason, the use of digital identity makes it possible to demonstrate that an entity - this is the generic term used - has a "separate and distinct" existence allowing it to be "identified in a [given] context".

Several concepts from ISO/IEC 24760-1: 2019 IT security and privacy - Framework for identity management - Part 1: Terminology and concepts have been adopted in ITU-T Recommendation X.1252. This applies to that of identification, which is intended to be the "process of recognizing an entity in a particular domain, as opposed to other entities". In both cases, it is agreed that it is possible for an entity to have more than one identity, just as it is possible for several entities to share the same identity under certain circumstances[2]. This will always depend on the context[3].

1 The International Telecommunication Union (ITU) is part of the United Nations and contributes to the development of standards (also known as "Recommendations") to ensure the development and proper functioning of information and communication technologies.
2 ISO/IEC 24760-1, art. 3.1.2 s.v. "identity". See notes 1 and 2.
3 ITU-T Recommendation X.1252 uses the term "context" while ISO 24760-1 prefers the term "domain".

2.3. WHAT MAKES THEM UP?

Digital identities are composed of different types of information that can reveal a characteristic of the person concerned. The first category concerns a person's own identity, including his or her profile on the Web, while the second category concerns transactional identity. A third category involves information that can be retrieved or inferred from a basic identity and added to that digital identity.

Basically, digital identities include information that is directly associated with a person. Examples include personal information such as a person's name, address, telephone number, date of birth, unique government-issued identifiers such as a social security number or health insurance number, but also biometric identifiers. Some of this personally identifiable information may be unique to an organization, such as a file number. In the case of a digital identity using a fictitious name used on the Web, for example, the digital identity will then take the form of the pseudonym and the characteristics that would have been provided at the time of registration (such as preferences or interests). This data is relatively stable over time.

Second, digital identities aggregate information about the interactions a subject has had in a digital context. For an organization, for example, the digital identities of customers will include purchase histories, web browsing histories, while the digital identities of employees will include salary data or performance evaluations for example. In a medical field, one will think of medical history, in a bank one will think of banking transactions, in an insurance company one will think of data used to evaluate the eligibility of people, premiums, claims, etc. On social networks, there will be comments, photos, mentions (likes, I'm here, etc.) that make it possible to track a person's activity. So, this data varies greatly from one organization to another, and it is impossible to make a list that would be complete. This data is much more dynamic than the data in the first group and is constantly changing.

Finally, the third type of information that makes up digital identities concerns the data that can be inferred from the analysis of a profile, that is associated with this profile and that is used in subsequent interactions. For example, secondary information that can be retrieved and associated with a digital identity is part of the intel that is added to the digital identity. Another example comes from profile analysis activities (often of a customer) that would allow, for instance, to associate a particular status (classify a customer in a Gold or Platinum category for example) or to assign a propensity rating to react positively to a particular offer. This data is the result of advanced analytics and analytics techniques that are increasingly used in organizations. This secondary use of data often leads to the creation of new information that is added to existing digital identities. This data can be dynamic depending on the frequency of analysis that is performed by organizations and the updating of digital identities.

2.4. WHAT IS THE PURPOSE OF DIGITAL IDENTITY?

Digital identity enables trust to be established between two parties. It is at the heart of identity management, which is based on 4 fundamental steps: identification, authentication, authorization, and logging. This guide focuses on the identification stage.

Identification associates a set of attributes to a person to distinguish him univocally. A unique identifier is an attribute that ensures this distinction. It will be necessary to verify that the attributes are authentic. Authentication consists in asking the subject to provide one or more proofs corroborating the claimed identity. There are four usual proofs: what he knows - such as his date of birth, what he owns - such as a driver's license, what he is - such as a physical feature and where he is - such as an IP address. Authorization provides access corresponding to the subject's level of empowerment, in a discretionary way, based on his role or by a combination of attributes. Finally, logging enables the tracing of subject actions to identify threats to identity and access management. Logging allows to detect, investigate, or prove certain actions based on the subject's identity.

In simple terms, digital identity is at the heart of the process that identifies a person and authenticates them as who they say they are. It allows to authorize a person's access to a computer system within the limits of what they are authorized to do (their access rights) and keeps a record of all their actions that it associates with their identity.

Let's illustrate this with an example. Let's imagine a customer who wants to interact with a financial institution. The bank will first want to make sure that the customer, let's call him Marc Tardif, is who he claims to be. It will therefore ask him to provide information that is associated with his person, in our scenario his login. They will then authenticate him with information known only to him, such as his password. If the information received corresponds to the information known by the bank, they will conclude that it is indeed Marc Tardif who made the request. They will give him access to his account and authorize him to perform certain actions related to his identity, for instance by giving him access only to bank accounts for which he is authorized, accept only the transactions he is entitled to make, and let him consult only the information that concerns him. Finally, the bank will keep track of everything Mark does as a transaction in the computer system and link these actions to his identity.

2.5. HOW CAN I RECOGNIZE DIGITAL IDENTITIES?

Any information held about a physical person that can be used to identify them makes up the digital identity. This information may be confidential. This confidential information may or may not contain personal information. The digital identities of individuals may be held by your organization. If not, a third party organization will hold information about the individual's identity and may share some or all of it with you. Once you have received this information, you become a holding organization. However, the third party organization is only responsible for disclosing this information to you if it has received consent from the individual.

THE PERSONAL INFORMATION THAT MAKES UP A DIGITAL IDENTITY IS PARTICULARLY SENSITIVE. IT INCLUDES

- **First and last names;**
- **Addresses, such as the home address and IP address of a device[4];**
- **Physical attributes, such as weight and height;**
- **Identification codes, such as passwords, client number, social insurance number, passport number and driver's license number;**
- **Beliefs, such as religion;**
- **Dates related to a person, such as date of birth, date of graduation;**
- **Descriptions of property owned by the person, such as a car;**
- **Biometric information, such as the topology of the face or the shapes of a fingerprint;**
- **Physical or mental health information;**
- **Socio-demographic information, such as age, marital status, gender identification and languages spoken;**
- **Location data;**
- **Phone numbers;**
- **Statuses granted to the person, such as an elite level and a line of credit;**
- **Transactions made by an individual, such as purchases, requests, and sales.**

4 Office of the Privacy Commissioner of Canada, *What an IP Address Can Tell About You - Report prepared by the Technology Analysis Branch - May 2013*

< https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/ip_201305/ >: The Office of the Privacy Commissioner of Canada has concluded that the IP address may be personal information particularly when considered in relation to other online activities performed by a user.

2.6. WHAT IS A DIGITAL CREDENTIAL?

Credentials are used as evidence to establish "some or all of the attributes of an identity" in a specific context. Both ISO 29115:2013 - Information technology - Security techniques - Entity authentication assurance framework and ITU-T Recommendation X.1252 agree on the definition and role of credentials in digital identity.

The credential fulfills two functions that may or may not coexist depending on the objectives put forward by the person who decides to include a digital identity approach in their business model. On the one hand, there is the trust-generating credential whose purpose is to confirm the attributes declared by an entity. On the other hand, there is the credential used to demonstrate the ability to exercise a right, without the obligation that the real identity of the entity be disclosed. Recommendation ITU-T X.1252 gives as an example of this second type of credential the case of a ticket for a sports or musical event. The ticket makes it possible to be present at the venue without the need to attach any other information about the entity. In both scenarios, the idea of digital identification is present.

In developing a digital identity, a thorough analysis of the relationships and dependencies between the entity, identity, and attributes is intended to reconcile the legal principle of minimizing the collection of personal information (where applicable) and the need for caution from a cybersecurity perspective.

3. DIGITAL IDENTITY AND MY ORGANIZATION

3.1. DOES MY ORGANIZATION ABSOLUTELY HAVE TO MANAGE DIGITAL IDENTITIES?

Your organization does not have to manage digital identities itself. It can outsource the management, for example, to a subcontractor based on a service contract. However, your organization is still responsible for protecting the personal information it holds, including the information supporting the digital identity. This should lead it to ensure that its internal practices and those of the service provider, if any, are aligned with good privacy practices (see sections 5.7 and 5.8).

Since no organization is immune to damage under its control, it is important to ensure that your digital identity management practices can reliably identify the individual involved. Moreover, your organization's commitment to these good digital identity management practices should be known to your customers[5].

3.2. WHY SHOULD I CARE IN MY ORGANIZATION?

Digital identities are an important asset for organizations. The personal information that makes it up must be adequately protected. Poor management of digital identities can have various consequences, some of which are legal, some of which are reputational, while they can also hinder your organization's competitiveness. These consequences can last long enough to create irreparable damage that puts your organization at risk.

An informed manager will probably think of scandals related to data theft that have occurred in recent years, such as the data leak reported by Capital One (106 million people in North America, including 6 million in Canada) and Desjardins (8 million people). These events, which received a great deal of media coverage, had a significant effect on raising public awareness. These data leaks or thefts caused strong reactions from those affected. Some customers and partners immediately left these organizations, they flooded it with calls to get answers to their questions, and in the end, they will receive substantial compensation. In all cases, the consequences are significant, costly, and difficult to reverse. Sometimes these data thefts are the result of a cyber attack from an external attacker, and more often they are committed by employees of an organization whether intentionally or not. In the case of employee-committed incidents, they are mostly the result of poor data governance practices that, if implemented and followed rigorously, could often have reduced some of the consequences or even prevented the event from occurring.

5 The Office of the Privacy Commissioner of Canada's Interpretation Bulletin on the Form of Consent (March 2014) is currently being revised: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_07_consent/

That said, despite the visibility given to these data leaks and the significance of the consequences for organizations, a much more common and persistent impact of poor digital identity management is reflected in the day-to-day business practices of organizations. For example, having multiple customer relationship management (CRM) systems can lead to different ways of representing customers, including the unique identifier (see section 2.1). This can lead to problems with customer service quality, business process efficiency, and reduces an organization's value proposition. These effects, which are persistent rather than episodic, diminish the competitiveness of organizations, whether through continued customer attrition, difficulty recruiting quality labor, or increased operating costs. Ultimately, all of this reflects on the financial health of the organization and puts its sustainability at risk.

In short, digital identity management is essential to ensure the competitiveness of organizations.

3.3. WHO IN MY ORGANIZATION SHOULD DO THIS?

A person's digital identity includes personal information, which is information about an identified or identifiable individual. From this point of view, the executive of your organization is responsible for it and can designate a person responsible for the protection of personal information. This person will have the following responsibilities, among others:

- **Development of company policies in this area;**
- **Inform and educate staff on best practices;**
- **Inform external stakeholders of policies and practices;**
- **Ensure legal and regulatory compliance;**
- **Inform your organization, especially when data changes legal jurisdiction;**
- **Notify authorities of any privacy incidents;**
- **Create, implement, monitor and audit the follow-up of policies and procedures;**
- **Ensure the completion of a Privacy Impact Assessment (PIA) where appropriate;**
- **Establish and maintain records relating to the collection, processing, disclosure and destruction of data;**
- **Receive and process complaints from affected individuals;**
- **Be the point of contact for your organization at the individual and authority level.**

The Privacy Officer is not required to have any specific technical skills, other than to:

- **Be familiar with privacy laws, regulations and industry standards;**
- **Pay attention to details;**
- **Be irreproachable in terms of personal information management;**
- **Exercise sound judgment in relation to confidentiality risks;**
- **Provide leadership for change;**
- **Know how to communicate in clear and concise language;**
- **Ability to work in a team, especially with legal or technological experts.**

An important point to note is that this person reports, according to good practice, to the board of directors or administration of the organization. This ensures that the person has the authority and independence to carry out his or her mission. Your chief information officer must work with various stakeholders in your organization to protect digital identity data. First, recognize the role of the person or persons responsible for information technology in ensuring the proper and secure operation of the systems storing business data, including digital identity data, and the overall technology architecture ensuring the interaction between these systems. The systems management function integrates both locally operated and cloud-hosted systems. The role of data stewards will also be recognized as being responsible for the sound management of business data, including digital identity data. The role of the data steward includes managing the quality and security of data, as well as ensuring that all individuals in an organization understand and use sound data management practices. This multi-stakeholder coordination can be formalized through formalized business data governance structures and practices.

3.4. WHERE SHOULD I LOOK FOR SUCH DATA?

Organizations manage a large volume of digital and paper data, including data specific to digital identity, across its operations. This data may reside in different computer or archival systems within an organization, or even appear in multiple copies in several of these systems.

It is unrealistic to expect to produce an exhaustive list of all the technologies or practices that can be used to store digital identity data. However, the MIKE2.0 Information Management Framework[6] provides a framework for researching and identifying potential sources of such data. For example, the MIKE2.0 framework recognizes five categories of systems that can exist in either digital or physical form:

- **Information access, retrieval, and delivery systems, including communication tools such as email, mobile applications or enterprise portals;**
- **Business content management systems, including collaborative suites, disk or cloud storage, enterprise ERP (enterprise resource planning) and CRM (customer relationship management) systems, or web content managers;**
- **Information asset management systems, including access control and monitoring tools or workflow systems;**
- **Enterprise data management systems, including data marts and warehouses or master data management systems;**
- **Business intelligence systems, including performance management systems and tools supporting analysis, analytics, and artificial intelligence.**

When searching for and identifying digital identity data, vigilance is required. Indeed, depending on the practices in effect in an organization, data can end up, by negligence, by mistake or by choice, outside of the official and listed systems. This is the case if data is found in employees' personal emails or on free storage media in the cloud.

Finally, it is important to note that digital identity data can be fragmented and scattered. This creates an increased level of complexity when searching and identifying. Individually, some data may go unnoticed, while combined they may reveal the identity of a natural person.

This means educating and training staff on the appropriate practices and systems for managing this data and ensuring its proper use.

6 http://mike2.openmethodology.org/

3.5. WHEN SHOULD I DO SOMETHING WITH THIS DATA?

Vigilance is required to take full responsibility for your organization. There are six main situations in which to respond: (1) when identity data is acquired or collected unnecessarily, (2) when identity data is collected without the individual's knowledge, (3) when identity data is retained without direction, (4) when identity data is lost or stolen, (5) when identity data is shared with a third party without legal obligation or consent of the individuals involved, (6) when the location of identity data changes.

THESE ARE DESCRIBED IN THE FOLLOWING TABLE:

CASE	EFFECT	POTENTIAL CAUSES	SOLUTION(S)
1	No need	• Poor governance	**Destroy** the collected data **Educate** staff on legal requirements regarding personal information collection and digital identity **Establish** and **implement** internal policies and practices to address legal requirements regarding the collection of personal information
2	Lack of transparency	• Illegal act • Error or omission	**Establish** and **implement** policies and practices consistent with laws and regulations to govern personal information **Make** policies available on the organization's website **Create** a policy regarding the collection and management of personal information and digital identity **Investigate** when there is reasonable doubt
3	No retention schedule	• No data lifecycle management	**Implement** the management (policies, mapping, etc.) of digital identity data with respect to legal and regulatory requirements

CASE	EFFECT	POTENTIAL CAUSES	SOLUTION(S)
4	Privacy incident, including data leakage	• Inadequate data protection (technology and governance)	**INCIDENT MANAGEMENT** **Promptly** notify the organization's Privacy Officer and report the leak to the appropriate authorities **Actively** manage the crisis (media, technology) **Seek** assistance from a specialized cybersecurity firm to manage the active incident **POST-CRISIS CORRECTIVE MEASURES** **Establish** and **implement** a crisis management policy by taking reasonable steps to reduce the risk of harm **Seek** assistance from a specialized cybersecurity firm to conduct an audit of the incident, identify the root cause of the leak, and implement corrective and preventive measures **Improve** your organization's security posture, including staff awareness of legal requirements regarding personal information, digital identity, and information security **Maintain** a confidentiality incident log
5	Illegal sharing	• Poor governance • Lack of legal expertise	**Stop** sharing and require your third party organization to destroy the information received **Consult** a legal firm before sharing data with a third party organization **Prohibit** individuals in your organization from sharing the identity of individuals without the explicit authorization of the Privacy Officer **Ask** for explicit consent before sharing digital identities
6	Storage outside the jurisdiction	• Not managing contracts with IT service providers	**Check** the storage jurisdiction of the targeted provider or a new cloud platform **Check** the privacy policies and terms of use of the intended provider or any new cloud platform **Avoid** "free" platforms **Use** legitimate contractual terms for all contracts, including contract termination clauses that ensure secure and appropriate management of digital identities

It should be noted that the "necessity" test is the one that guides the scope of acquisition or collection of personal information. It implies that an assessment of the context must be made to determine whether the information is needed. What is necessary is assessed more strictly than what is useful or practical, especially when it is possible to rely on the collection of other, generally less sensitive, information that may serve the same purpose of establishing identity.

4. DIGITAL IDENTITY PROTECTION IN CANADA

4.1. DOES THE PRESENCE OF DIGITAL IDENTITIES IN MY ORGANIZATION HAVE AN IMPACT ON MY BUSINESS PRACTICES?

If an organization wants to use digital identification solutions, it must clarify its intentions and especially its obligations. It is sometimes undesirable to automatically link certain actions and transactions to a person[7]. To avoid this, it is possible to use anonymity or a non-significant identifier.

The scope of the collection of information that may constitute personal information will vary depending on the need to establish a strong link with an individual. In addition, the association between a unique identifier and an individual may be required. For example, if one wants to avoid granting a privilege twice to the same person, such as an electronic vote.

Your organization may be subject to stricter requirements to deal with identity theft, including money laundering and terrorist financing. For example, Part 3 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* [8] sets out how an individual's identity can be verified. To the extent that federal, provincial, and foreign governments issue little or no digital identity documents, the person required to meet the verification requirements is placed in a position where he or she must bridge the physical and virtual worlds. As a result, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) Guideline on Methods to Verify the Identity of Individuals and Entities[9] provides some alternatives such as:

7 Paul A. Grassi et als, National Institute of Standards and Technology Special Publication 800-63-3A, Enrollment and Identity Proofing (2017), 2, < https://doi.org/10.6028/NIST.SP.800-63a>.
8 SOR/2002-184.
9 Government of Canada, Methods of Verifying the Identity of Individuals and Entities (fintrac-canafe.gc.ca), November 2021.

- **Participate in a live video chat with the individual to compare the name and features of the video images with the name and photo on the government-issued identification document; or**
- **Have the individual take a self-portrait, then using a facial recognition application, compare the features of the self-portrait to the photo on the verified government-issued identification document and compare the name provided with the name on the identification document.**

Therefore, your organization should always ensure that policies and procedures are in place to verify the authenticity of an identity document.

4.2. DOES MY ORGANIZATION HAVE ANY LEGAL OBLIGATIONS TOWARDS THE MANAGEMENT, INCLUDING PROTECTION, OF DIGITAL IDENTITIES?

Collecting, holding, managing, using, or otherwise utilizing information including a natural person's digital identity creates legal obligations for your organization.

The indicative obligations listed below are inspired by the best legal practices, particularly in Canada, for a secure digital identity framework. Observing these best practices allows SMEs to comply with the Canadian legal framework in this area.

Designate a person responsible for protecting or securing the digital identity within your organization (see section 3.3).

Establish an inventory of digital identity data held by your organization to facilitate governance and management (see sections 3.5 and 4.4) and then determine whether each system involved provides the level of privacy and protection that is required.

Implement policies and procedures consistent with legal requirements supporting the governance and management of digital identity data. We can note:

- **Policies establishing principles for the collection, management, disclosure or other use of digital identity data;**
- **Policies for receiving and processing complaints and claims from citizens wishing to exercise their rights;**
- **Data security policies;**
- **Policies for reporting and managing privacy incidents;**

- **Specific policies on the use of biometric systems applied to digital identity, the use of digital identity information for research and artificial intelligence, etc.;**
- **Default protection policies for all systems in your organization;**
- **Privacy Impact Assessment (PIA) policies prior to any project involving digital identity data. Define the criteria that trigger the requirement to conduct a PIA.**

4.3. WHAT PRINCIPLES MUST MY ORGANIZATION FOLLOW TO BE COMPLIANT WITH THE LAW?

Any collection, holding, management, use, etc. of information relating to the digital identity of a natural person must comply with the guiding principles[10] . What can we retain succinctly from the main principles?

4.3.1. IDENTIFICATION OF A PURPOSE

Your organization must determine in advance the purposes for which digital identity data is collected for processing. These purposes must be specific, explicit, legitimate, and lawful. Simply put, each collection of identifying data must have a pre-determined purpose that is specific, explicit, legitimate, and lawful. For example, you collect the address of your customers to be able to deliver the ordered products.

4.3.2. DATA MINIMIZATION

Your organization should only collect digital identity data that is adequate and relevant to the purpose of the transaction. Data is relevant or adequate if it has a direct link to the purpose of the processing. Identifying data collected must be accurate and, if necessary, updated. For example, you avoid asking your customers for their driver's license number even though this could have reduced the incidence of fraud.

4.3.3. SECURITY AND CONFIDENTIALITY

Your organization must take all necessary and appropriate technical, software and organizational measures considering the purpose of each processing and the nature of the digital identity data, to prevent its disclosure, unauthorized access, or loss, to ensure a high level of security. For example, you encrypt customer databases to prevent a cyber attacker from stealing the information they contain.

10 PIPEDA Fair Information Principles, Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/

4.3.4. THE PRINCIPLE OF RESPONSIBILITY

Your organization must be mindful that it is responsible for the protection of the digital identity information it collects or holds and, as a result, must always be able to demonstrate and document that each use complies with the relevant legal framework. In other words, you must comply with all legal obligations you have in collecting, using, managing, or otherwise using digital identity information within your organization. This includes implementing internal mechanisms and procedures to demonstrate compliance. For example, when a customer information system is changed, you ensure that a Privacy Impact Assessment (PIA) is performed and act proactively when the risk is too great.

4.3.5. THE PRINCIPLE OF TRANSPARENCY

Your organization must inform the individual when it collects their digital identity. For example, an individual who has provided his or her payment information must check a consent box for you to retain that information for future payment.

4.4. WHAT HAPPENS IF MY ORGANIZATION DOESN'T DO IT?

Failure to comply with the principles and obligations set out in section 4 may expose organizations to administrative monetary penalties or criminal prosecution, as well as to damages under domestic and international privacy laws.

In Canada, a violation of the legal framework can result in penalties of up to $100,000 or $25,000,000, whichever is greater, or 4% of worldwide sales for the previous fiscal year

At the European Union level, the General Data Protection Regulation (GDPR), which may apply in Canada, provides that violation of the principles may result in an administrative fine of up to €20 million or, in the case of an organization, up to 4% of the total worldwide turnover of the previous financial year, whichever is greater.

In addition to these penalties under specific privacy laws, there is also the risk of non-compliance with constitutional and quasi-constitutional principles of customer privacy, opening the door to the risk of contraventions of laws from other areas of law, including Canadian criminal law, the rules of civil liability, and the fundamental protections provided by the Charter of Human Rights and Freedoms, exposing an organization to the laying of criminal charges or the payment of damages as well as punitive damages.

In protecting digital identity data, an organization must also consider business risks such as damage to its reputation, the costs of mitigating issues arising from non-compliance or theft of that data, and the loss of current or potential customers or employees who would no longer want to be associated with the organization.

4.5. AS THE OWNER OF MY ORGANIZATION, AM I PERSONALLY RESPONSIBLE FOR MEETING THESE LEGAL OBLIGATIONS?

Every person who operates an organization is responsible for protecting the digital identity information of citizens held by that organization, and the person with the highest authority is responsible for ensuring compliance with and implementation of the legal framework for protection. However, he or she may delegate this function in writing, in whole or in part, to a staff member.

However, given the variety of models and the diversity of operations, it is not easy to draw a picture of all the undesirable consequences[11] that can result from poor identity management. Some situations will require a high level of insurance[12] and others less, which is why it is important to conduct a rigorous analysis at regular intervals. An identity management policy[13] remains an essential tool.

Furthermore, the mere fact of being the owner of an organization that collects or processes elements that make up a user's digital identity does not make the owner personally liable for the company's failure to comply with legal obligations. There are, however, certain situations in which the contractor would be liable. For example, the owner may become personally liable when he or she (1) acts as a director or officer or agent of the business and (2) directed or authorized or consented to the performance of the act or omission that constitutes a violation by law. In addition, in the case of a sole proprietorship or sole proprietorship, the owner-entrepreneur retains responsibility for the obligations of the business. He or she is required to comply with the above-mentioned legal obligations. Failure to do so may result in administrative monetary penalties, criminal penalties, or damages. In the case of a co-owner of a partnership, each partner is personally liable for the debts of the partnership when his assets are insufficient to pay his debts arising from administrative or penal sanctions or damages due to the failure to comply with the legal obligations of the partnership.

11 For an overview of examples of harm, see Appendix B of the Guideline on *Defining Authentication Requirements*: Guideline on Defining Authentication Requirements - Canada.ca (tbs-sct.gc.ca)
12 For an overview, see the *Identity Assurance Guideline*: Identity Assurance Guideline - Canada.ca (tbs-sct.gc.ca)
13 See the Government of Canada's Directive on Identity Management last amended July 1, 2019: Directive on Identity Management- Canada.ca (tbs-sct.gc.ca)

5. MANAGING THE DIGITAL IDENTITY ECOSYSTEM

5.1. HOW CAN I BE A RESPONSIBLE ORGANIZATION WHEN IT COMES TO DIGITAL IDENTITY MANAGEMENT?

A responsible organization ensures that it manages the social, environmental, and economic effects of its activities in a manner that is responsible and consistent with public expectations. It ensures that it uses ethical, inclusive, environmentally sustainable, and socially acceptable practices. Ethical practices of interest with respect to digital identity include compliance with legal principles (see section 4.3), security management (see section 5.7) and transparency. Inclusive practices allow for a representation that is consistent with the reality of the individual, both in terms of identity and preferences. Respect for the environment can prohibit the use of energy-consuming technologies. Finally, the acceptability of systems is described in section 5.2.

Attention must be paid to balancing the interests of an organization with those of its customers and partners. Cost savings should not come at the expense of digital identity security, including relationships with cloud service providers. In addition, mores and data security concerns are rapidly evolving and your organization must stay on top of them. Finally, a proactive approach is often preferable to a reactive one, thus avoiding costly patches.

5.2. HOW DO I CONSIDER THE SOCIAL ACCEPTABILITY OF THE DIGITAL IDENTITY APPROACHES ADVOCATED BY MY COMPANY?

To ensure the success of a digital identity system and, more broadly, of an organization's digital transformation, it is important not to ignore the issue of social acceptability, i.e., the degree of agreement of the parties involved with respect to a project. In fact, a lack of social acceptability can result in a low level of use of the digital identity system, or even in strong opposition from the parties involved, despite significant investments in the implementation and management of the system. Beyond the loss of money, low social acceptability can result in low customer confidence in your organization, culminating in a bad reputation. In addition, a lack of social acceptability could result in additional financial costs for your organization, including project abandonment, in addition to exposing you to social and legal challenges.

It is appropriate to briefly discuss the elements that influence the risk that one of your projects will not be socially acceptable. Among the elements influencing social acceptability, we note the adequacy between the environment and the project, which translates into respect for values (e.g., privacy concerns). Next, it is important to consider the clientele's perception of the presence and extent of benefits/damage, the level of risk, novelty, and uncertainty regarding the project (e.g., perceived risks of privacy intrusions or leaks of personal information). Also, the trust that customers have in an organization and their digital identity management is not to be neglected if we want to ensure good social acceptability. Ultimately, these elements are influenced by the quality of the consultation process with the parties consulted. Often taken for granted, social acceptability should not be neglected given the possible consequences of its absence, especially since it is never acquired and can be lost at any time.

5.3. WHAT TO DO WITH MY SUPPLIERS AND SUBCONTRACTORS?

Vendors and subcontractors who manage digital identities in partnership, or on behalf of an organization, must abide by the same laws, rights, and obligations as the primary organization. Since the final responsibility lies with the organization, it must monitor them closely. This should be planned at the outset of the partnership and clarified in writing between the parties exchanging information, as digital identity information can be made vulnerable through inadequate security management. Measures should be identified and implemented to manage third-party access to the information processing facilities that form the basis of the digital identity.

It is essential to clearly define the respective responsibilities and obligations. It is therefore necessary to ensure that the contractual clauses are exhaustive. Thus, in addition to the standard clauses, it is necessary to ensure that the following are well defined

- **the implementation of appropriate security measures;**
- **compliance with certain policies and procedures of your organization;**
- **the right to be audited or to receive a document certifying compliance, such as a System and Organization Controls 2 type 2 (SOC 2, type 2) report;**
- **mutual obligations of confidentiality, including all matters relating to digital identity and personal information. These obligations limit access to confidential information to what is strictly necessary, prohibit any disclosure to third parties, prohibit any secondary use, force the secure deletion of confidential information at the end of the contract, affirm that any leak will cause harm to the other organization, ensure that a confidentiality undertaking is administered to its personnel who will have access to confidential information, etc.;**
- **the management of confidentiality incidents, in particular the notification period which must be short (less than 48 hours if possible), the necessary collaboration between organizations, the necessary escalation according to the severity of the incident, etc.;**

- **the prescription of penalties;**
- **prior notification of any change in the location of confidential information;**
- **the non-abusive limitation of liability;**
- **the presence of adequate insurance coverage for cyber security, errors and omissions, and civil liability.**

It may be appropriate to validate the vendor's previous experiences to assess their level of organizational maturity in digital identity management.

5.4. WHAT ARE THE IMPLICATIONS IF I WANT TO SHARE MY ORGANIZATION'S IDENTITY DATA?

The implications are notably of a legal and economic nature. Indeed, the communication or any other form of availability of data in general and of personal information forming the digital identity of citizens is a sensitive and sometimes complex issue. The best practices in this field, whatever the form of processing envisaged, prescribe the strict protection of the fundamental rights and freedoms of individuals regarding their personal information.

Simply put, if your organization plans or undertakes to disclose or make available digital identity data, it must rigorously ensure that all data subjects' privacy rights are respected and that it complies with its strict obligations as a privacy officer.

Failure to comply with these privacy requirements creates legal uncertainty within your organization and exposes it to various types of sanctions (see sections 5.4, 5.6 and 5.8); anything that could negatively impact your organization's image and result in a loss of financial gain.

In the context of the single digital market, the intensification of the circulation and economic valuation of information capital are recurrent to the point where we often see cases of mergers, partnerships, or acquisitions of companies with their information capital. The question of the resale of the data held by the company could then arise.

Particularly with respect to resale in such cases, the organization must be aware of the risk that some information may reveal personal information, including digital identity information, so the above best practices should be adopted as a matter of prudence, including the use of anonymization techniques depending on the sensitivity of the data.

5.5. WHAT IS ADEQUATE CONSENT WHEN I PROVIDE DIGITAL IDENTITY INFORMATION?

To the extent that personal information is involved, disclosure without the knowledge or consent of the individual is limited to those exceptions set out in the legislation. An organization wishing to resell such information would be well advised to ensure that individuals are able to consent to the resale using plain language.To get a clearer picture of the scope of consent expectations, it may be wise to review the findings of the Office of the Privacy Commissioner of Canada in the joint investigation into Facebook Inc:

> "71. For consent to be considered meaningful, organizations must inform individuals of their privacy practices in a clear, comprehensive, and understandable manner. Disclosure should be timely, so that users have relevant information and context to make an informed decision before their personal information is collected, used, or disclosed. As of June 2015, PIPEDA also provides that an individual's consent is valid only if it is reasonable to expect the individual to understand the nature, purposes, and consequences of the collection, use, or disclosure of personal information to which the individual has consented."[14]

5.6. IS DATA SECURITY EXPENSIVE?

In the context of data processing, organizations have access to more and more ways to protect themselves and their customers. The logic is simple: without data security, the organization will face backlash from its customers, lawsuits, and a rapid decline in revenue. The question is not if organizations will suffer a privacy incident, but when? Based on recent surveys of Canadian businesses, cyber attacks affect more than one in four companies annually.[15]

Many measures require little or no technology and are cost-effective. Thus, policies related to data confidentiality are the basis of the measures to be put in place. (see section 4.2). It is also important to ensure that the organization's personnel are informed and trained on data confidentiality (causes, risk behaviors, impacts). Finally, when dealing with suppliers, organizations must ensure that contractual obligations are adequate (section 5.3). These measures allow for a rapid increase in organizational maturity with respect to the protection of digital identities.

14 Office of the Privacy Commissioner of Canada, Joint investigation by the *Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia into Facebook, Inc*, Report of Findings No. 2019-002, April 25, 2019.

15 See IT.Rends on https://info.novipro.com/en/it-trends

For example, a web platform has been created by company X and sold to customer Y. The visitor goes to the platform and enters identity data. This data will transit through the platform of company X to be stored in the databases of customer Y. Company X must therefore specify in its privacy policy and in the terms of use of the platform how the data is processed.

Finally, a firm specialized in cybersecurity will judiciously advise executives on the most appropriate measures considering their obligations, organizational structure, information systems and market.

5.7. WHAT ARE THE MINIMUM SECURITY MEASURES MY ORGANIZATION MUST HAVE IN PLACE TO ADEQUATELY ENSURE DIGITAL IDENTITY PROTECTION?

Security safeguards cover several areas, including:

- **Documentation of principles, roles, responsibilities, obligations, penalties and waivers in policies;**
- **Development of procedures to ensure repeatability of sensitive activities;**
- **Access management to systems managing digital identity;**
- **Protection of the organization's devices and networks, including antivirus and firewalls;**
- **Systems monitoring and proactive detection of abnormal situations;**
- **Keeping information assets up to date, especially those containing confidential information.**

These measures must be adapted to the reality of each organization and its environment. They evolve with the rhythm of technologies, best practices, threats, etc. Hence, it is important to follow the governmental recommendations at least[16].

16 Basic Cybersecurity Controls for Small and Medium Organizations, Canadian Centre for Cybersecurity, https://cyber.gc.ca/fr/orientation/controles-de-cybersecurite-de-base-pour-les-petites-et-moyennes-organisations

5.8. DOES MY ORGANIZATION REMAIN ACCOUNTABLE FOR COMPLIANCE WITH DIGITAL IDENTITY PROTECTION OBLIGATIONS WHEN USING CLOUD COMPUTING?

Organizations are always responsible for the protection of their digital identities, whether they are kept inside or outside their walls, whether they are managed by employees, contractors, or external firms. This responsibility is fundamental, especially for the people who do business with or work for the organization. In addition, the organization's leaders remain responsible for the proportionality and adequacy of the safeguards that are put in place.

This means that an organization is required to act in the best interests of its customers, with care and diligence, even when outsourcing the management of its customers' personal information. The organization is also required to act in accordance with best practices. European Union law is even more specific on this point: an outsourcing contract must be concluded between the organization and the service provider to whom the processing of personal information is delegated. Therefore, any person who suffers damage because of unlawful, improper, or unreasonable processing of digital identity information is entitled to obtain compensation from the organization and its subcontractors for the damage suffered. It should be noted that the subcontractor is only liable for the damage caused by the unlawful processing if it has not complied with its specific obligations under the subcontracting agreement or if it has acted outside or contrary to the authorized instructions of the organization.

6. BENEFITS FOR MY ORGANIZATION

6.1. WHAT BENEFITS CAN I EXPECT FOR MY ORGANIZATION?

Any action to improve the management of digital identity data is also an opportunity to increase your organization's digital maturity and, when properly executed, can yield positive benefits. This is especially true for organizations transacting online, reducing the time, cost, and errors associated with identifying individuals. In addition, a digital identity system makes it easier to verify the digital identity of your customers by recognizing forgeries and fraudulent uses. For example, your organization could detect individuals using another person's identity to use its services, such as using a subscription to an online digital service or gym.

Implementing recognized practices can also improve your brand image and customer confidence. With growing public awareness, organizations that demonstrate a superior ability to adequately protect and manage digital identity will gain public trust and reduce barriers to the use of their digital services.

Finally, formal digital identity management can protect your organization from online fraud in today's booming digital economy or reduce the risk of incidents and associated economic losses.

6.2. AND FOR MY CLIENTELE

There are three broad categories of benefits that the implementation of a large-scale digital identity system could bring to customers and the public. On the one hand, it could provide a smoother and simpler customer experience than many current digital identities allow. For example, this could mean fewer passwords to remember, as well as the use of the same digital identity for various services, both online and offline. On the other hand, it also has the potential to increase the financial inclusion of the population. This translates into greater ease of obtaining online identification documents for people who do not have traditional identification documents (e.g., driver's license) and therefore, become more integrated into the digital economy and become potential customers. Finally, this digital identity could provide a digital environment in which customers have more confidence.

6.3. WHAT ABOUT MY STAFF?

The implementation of an identity system translates into a more fluid, and more efficient use of the organization's systems. Information will be better managed which will facilitate value creation. A sense of pride, even belonging, should emerge among the personnel. In a context where recruitment of the workforce is increasingly difficult, responsible management of staff digital identities can be an asset in recruiting people who are sensitive to these ethical and legal considerations. A dedicated and responsive workforce can only be an asset to an organization that manages digital identities, fostering the development of the right behaviors by employees, and reducing the risk of privacy incidents.

7. IN SUMMARY

7.1. THAT'S A LOT! IN SUMMARY, ON ONE PAGE, WHAT DO I NEED TO REMEMBER?

Digital identity is made up of all the data that identifies a person. The federal and provincial governments understand the importance and sensitivity of this data and are rapidly enacting new laws and regulations to govern its management. New legislation has brought about obligations to protect this data for all Canadian organizations, regardless of their sector of activity or size.

Digital identities affect all groups in an organization's ecosystem: customers, employees, partners. They concern personal information, their interactions, and the result of secondary analysis of these interactions. They serve to establish trust between parties and must be actively managed.

The management of digital identities is based on various laws and regulations that affect all business activities, but also on general governance principles applied to the responsible management of information technologies. A wise manager must be aware of these principles, integrate them into his daily activities and monitor their respect and compliance over time.

Organizational leaders and boards of directors are responsible for sound governance of digital identity data management. They must oversee the risk and help leverage the benefits.

Failure to protect digital identity data can result in numerous consequences that directly affect an organization's prosperity, including fines, financial loss, temporary inability to continue business operations, and reputational loss. To mitigate this risk, an organization must educate all its employees on how to behave safely and wisely, identify digital identity data, and protect it with practices that are appropriate to their context and comply with current and future laws and regulations.

Digital identity data protection compliance will enable an organization to operate in the Canadian and international business ecosystem in a competitive and sustainable manner. It will contribute to its recognition as a responsible, respectful, and trusted organization. Ultimately, the economic, social, and environmental benefits will be significant for organizations and Canadian society.

7.2. I WANT TO LEARN MORE; DO YOU HAVE ANY RESOURCES TO SHARE WITH ME?

Digital identity data management is developing rapidly in Canada. It can be useful to keep an eye on the different aspects of the field. Here are some resources that may be useful for organizations operating domestically and internationally. A much more detailed list of information sources is presented at the end of this book for organizations wishing to develop a detailed understanding of the field.

DEMYSTIFYING DIGITAL IDENTITY

- Can I see your (digital) ID? [Government of Canada]
- Digital identity of citizens [Deloitte].
- Quebec Digital Identity Service (in development) [Government of Quebec] and [Government of Quebec].

REGULATORY RESOURCES

- European Union General Data Protection Regulation (GDPR) [Government of Canada]
- Bill C-11 [Government of Canada].

DIGITAL IDENTITY DATA MANAGEMENT

- IDLab the digital identity laboratory [idlab.org]
- Digital Identification and Authentication Council of Canada [diacc.ca]
- Emerging Economy Series: Digital Identity as the New Policy Frontier [Government of Canada]

BIBLIOGRAPHY

SOCIAL ACCEPTABILITY OF DIGITAL IDENTITY

[1] Dhamija, Rachna and Lisa Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges," IEEE Security Privacy, vol. 6, no. 2, 2008, 24-29, accessed 11/27/2021, DOI 10.1109/MSP.2008.49

[2] Adjei, Joseph and Henning Olesen, "Keeping Identity Private," IEEE Vehicular Technology Magazine, vol. 6, no. 3, 2011, 70-79, DOI 10.1109/MVT.2011.941894

[3] Gehman, Joel, Lianne M. Lefsrud and Stewart Fast, "Social license to operate: Legitimacy by another name?", Canadian Public Administration, vol. 60, no. 2, 2017, 293-317, DOI 10.1111/capa.12218

[4] Cespiva, R. B. (2018). Factors Influencing the Decision to Adopt a Digital Identity: A Correlational Study [D.I.T., Capella University]. In ProQuest Dissertations and Theses. https://www.proquest.com/docview/2124445405?pq-origsite=gscholar&fromopenview=true

[5] Digital Identity-Will the New Oil Create Fuel or Fire in Today's Economy? (n.d.). ISACA. Retrieved July 14, 2021, from https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/digital-identitywill-the-new-oil-create-fuel-or-fire-in-todays-economy

[6] Ishmaev, G., & Stokkink, Q. (2020). Identity Management Systems: Singular Identities and Multiple Moral Issues. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00015

[7] Kalvet, T., Tiits, M., & Laas-Mikko, K. (2018). Public Acceptance of Advanced Identity Documents. Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, 429432. https://doi.org/10.1145/3209415.3209456

[8] Kim, A.-Y., & Kim, T.-S. (2016). FACTORS INFLUENCING THE INTENTION TO ADOPT IDENTITY THEFT PROTECTION SERVICES: SEVERITY VS VULNERABILITY. PACIS 2016 Proceedings. https://aisel.aisnet.org/pacis2016/68

[9] Klaus, T., Wingreen, S., & Blanton, J. E. (2007). Examining user resistance and management strategies in enterprise system implementations. Proceedings of the 2007 ACM SIGMIS CPR conference on Computer personnel research: The global information technology workforce, 5562. https://doi.org/10.1145/1235000.1235013

[10] Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. Information Systems Research, 2(3), 173191. https://doi.org/10.1287/isre.2.3.173

[11] Rocha, M. (2016). Data Privacy and Social Acceptance of Smart Meters. In Smart Grid Handbook (p. 19). American Cancer Society. https://doi.org/10.1002/9781118755471.sgd026

[12] Rome, J. D. (n.d.). Understanding Adoption Barriers of Superior Technologies to Authenticate and Protect Users from Ongoing Cyber Threats [Ph.D., Ashford University]. Retrieved July 14, 2021, from https://www.proquest.com/docview/2481091755/abstract/6531302EDF7A4386PQ/1

[13] Sindi, A. F. (n.d.). Adoption Factors of a Blockchain Digital Identity Management System in Higher Education: Diffusing a Disruptive Innovation [Ed.D., California State University, Los Angeles]. Retrieved June 16, 2021, from https://www.proquest.com/docview/2359384031/abstract/7AA1753726E44F8EPQ/1

[14] The factors that influence small and medium enterprises' intention to adopt the government credit program | Emerald Insight. (n.d.). Retrieved June 16, 2021, from https://www.emerald.com/insight/content/doi/10.1108/JRME-01-2020-0013/full/html#loginreload

[15] Tiits, M., Kalvet, T., & Mikko, K.-L. (2014). Social acceptance of epassports. 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), 16.

CONSENT

[16] J. Pandit, H., Jesus, V., Ammai, S., Lizar, M., & D'Agostino, S. (2021). Role of Identity, Identification, and Receipts for Consent. Gesellschaft für Informatik e.V. http://dl.gi.de/handle/20.500.12116/36495

RISK MANAGEMENT

[17] Appendix_1_e1_maturity_model_for_identity_management_intrahealth_international_digital_square_notice_e1.pdf. (n.d.). Retrieved June 17, 2021, from https://applications.digitalsquare.io/sites/default/files/notice-e1/1592580188/appendix_1_e1_maturity_model_for_identity_management_intrahealth_international_digital_square_notice_e1.pdf

[18] Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA) | Elsevier Enhanced Reader. (n.d.). https://doi.org/10.1016/j.cose.2010.03.002

[19] Bhardwaj, A., & Kumar, V. (2011). Cloud security assessment and identity management. 14th International Conference on Computer and Information Technology (ICCIT 2011), 387392. https://doi.org/10.1109/ICCITechn.2011.6164819

[20] Campbell-Verduyn, M., & Hütten, M. (2021). The Formal, Financial and Fraught Route to Global Digital Identity Governance. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.627641

[21] In the News - Canada's Strong Digital Identity System | In the News - Canada's Strong Digital Identity System. (n.d.). Retrieved June 21, 2021, from https://cba.ca/cba-in-the-news-canada-needs-a-robust-digital-id-system?l=fr

[22] Farah, B. (2011). A Maturity Model for the Management of Information Technology Risk. The International Journal of Technology, Knowledge, and Society, 7(1), 1326. https://doi.org/10.18848/1832-3669/CGP/v07i01/56174

[23] PalsonKennedy, R., & Gopal, T. V. (2010). Assessing the risks and opportunities of Cloud Computing-Defining identity management systems and maturity models. Trendz in Information Sciences Computing(TISC2010), 138142. https://doi.org/10.1109/TISC.2010.5714625

[24] physical, T. authoritative resource for, & Security, C. (n.d.). Identity management best practice planning-Access & Identity Management Handbook 2011-Hi-Tech Security Solutions. Retrieved June 21, 2021, from http://www.securitysa.com/regular.aspx?pklregularid=4702

[25] Report-transformation-numerique-en.pdf. (n.d.). Retrieved June 21, 2021, from https://lautorite.qc.ca/fileadmin/lautorite/grand_public/publications/professionnels/rapport-transformation-numerique-fr.pdf

[26] Rasouli, H., Valmohammadi, C., Azad, N., & Esfeden, G. A. (n.d.). Proposing a digital identity management framework: A mixed-method approach. Concurrency and Computation: Practice and Experience, n/a(n/a), e6271. https://doi.org/10.1002/cpe.6271

[27] WEF_Digital_Identity_Strategic_Imperative.pdf. (n.d.). Retrieved June 23, 2021, from http://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf

DIGITAL IDENTITY GOVERNANCE

[28] 6_Rannenberg_framework_for_identity_management.pdf. (n.d.). Retrieved June 23, 2021, from https://fg-secmgt.gi.de/fileadmin/FG/SECMGT/2012/6_Rannenberg_framework_for_identity_management.pdf

[29] Bernabe, J. B., David, M., Moreno, R. T., Cordero, J. P., Bahloul, S., & Skarmeta, A. (2020). ARIES: Evaluation of a reliable and privacy-preserving European identity management framework. Future Generation Computer Systems, 102, 409425. https://doi.org/10.1016/j.future.2019.08.017

[30] Bucík, B. D. F. (2021). Optimization of user digital identity gathering process. 100.

[31] Huang, J., Wu, M., & Huang, Y. (2020). Research and Application of eID Digital Identity. Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacture, 266270. https://doi.org/10.1145/3421766.3421830

[32] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers. https://doi.org/10.1007/s10796-020-10044-1

[33] Kabwe, F., & Phiri, J. (2019). A Framework For Digital Identity Management.

[34] Maldonado-Ruiz, D., Torres, J., El Madhoun, N., & Badra, M. (2021). An Innovative and Decentralized Identity Framework Based on Blockchain Technology. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 18. https://doi.org/10.1109/NTMS49979.2021.9432656

[35] NIST Special Publication 800-63-3. (n.d.). Retrieved July 8, 2021, from https://pages.nist.gov/sp800-63-3.html

[36] Rasouli, H., Valmohammadi, C., Azad, N., & Esfeden, G. A. (n.d.). Proposing a digital identity management framework: A mixed-method approach. Concurrency and Computation: Practice and Experience, n/a(n/a), e6271. https://doi.org/10.1002/cpe.6271

[37] Sarmiento, D. L. (2014, February 28). A conceptual framework for an interoperable online identity management system [Info:eu-repo/semantics/masterThesis]. University of Twente. https://essay.utwente.nl/64801/

[38] Staite, C. (2012). Identity management architecture and implementation: Evaluation and improvement [D_ph, University of Birmingham]. https://etheses.bham.ac.uk/id/eprint/3388/

[39] The-Sequoia-Project-Framework-for-Patient-Identity-Management.pdf.(n.d.). Retrieved June 21, 2021, from https://sequoiaproject.org/wp-content/uploads/2015/11/The-Sequoia-Project-Framework-for-Patient-Identity-Management.pdf

DIGITAL IDENTITY MANAGEMENT

[40] D6.1.2-economic_valuation_of_identity_management_enablers-public.pdf. (n.d.). Retrieved July 8, 2021, from http://primelife.ercim.eu/images/stories/deliverables/d6.1.2-economic_valuation_of_identity_management_enablers-public.pdf

[41] Preibusch, S., Kübler, D., & Beresford, A. R. (2013). Price versus privacy: An experiment into the competitive advantage of collecting less personal information. Electronic Commerce Research, 13(4), 423455. https://doi.org/10.1007/s10660-013-9130-3

[42] Private Sector Economic Impacts from Identification Systems. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems

[43] Understanding Cost Drivers of Identification Systems. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/702641544730830097/Understanding-Cost-Drivers-of-Identification-Systems

[44] Jackson, P. M., Ligertwood, J., O'Donnell, J., & Shelly, M. (n.d.). Small Business: Issues of Identity Management, Privacy and Security. 15.

SELF-SOVEREIGN DIGITAL IDENTITY

[45] 200820-Digital-Wallet-Interview-findings-report.pdf. (n.d.). Retrieved July 8, 2021, from https://www.swinburne.edu.au/media/swinburneeduau/research-institutes/smart-cities/200820-Digital-Wallet-Interview-findings-report.pdf

[46] Alsobhi, H., Mirdad, A., Alotaibi, S., Almadani, M., Alanazi, I., Alalyan, M., Alharbi, W., Alhazmi, R., & Hussain, F. K. (2021). Innovative Blockchain-Based Applications-State of the Art and Future Directions. In L. Barolli, I. Woungang, & T. Enokido (Eds.), Advanced Information Networking and Applications (pp. 323335). Springer International Publishing. https://doi.org/10.1007/978-3-030-75078-7_33

[47] Banihashemi, S., Homayounvala, E., Talebpour, A., & Abhari, A. (2016). Identifying and Prioritizing Evaluation Criteria for User-Centric Digital Identity Management Systems. International Journal of Advanced Computer Science and Applications, 7(7). https://doi.org/10.14569/IJACSA.2016.070707

[48] Campbell-Verduyn, M., & Hütten, M. (2021). The Formal, Financial and Fraught Route to Global Digital Identity Governance. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.627641

[49] Coutor, S., Hennebert, C., & Faher, M. (n.d.). BLOCKCHAIN AND DIGITAL IDENTIFICATION. 102.

[50] De Filippi, P. (2016). The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies (SSRN Scholarly Paper ID 2852689). Social Science Research Network. https://papers.ssrn.com/abstract=2852689

[51] Digital Identity. (n.d.). Retrieved June 23, 2021, from https://learning.oreilly.com/library/view/digital-identity/0596008783/

[52] Gilani, K., Bertin, E., Hatin, J., & Crespi, N. (2020). A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data. 2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS), 97101. https://doi.org/10.1109/BRAINS49436.2020.9223312

[53] Ishmaev, G., & Stokkink, Q. (2020). Identity Management Systems: Singular Identities and Multiple Moral Issues. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00015

[54] Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). A Systematic Review of Blockchain for Consent Management. Healthcare, 9(2), 137. https://doi.org/10.3390/healthcare9020137

[55] Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (p. 6262). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01142020

[56] Mahula, S., Tan, E., & Crompvoets, J. (2021). With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. DG.O2021: The 22nd Annual International Conference on Digital Government Research, 495504. https://doi.org/10.1145/3463677.3463705

[57] Maldonado-Ruiz, D., Torres, J., El Madhoun, N., & Badra, M. (2021). An Innovative and Decentralized Identity Framework Based on Blockchain Technology. 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 18. https://doi.org/10.1109/NTMS49979.2021.9432656

[58] Meghana, A. R., & Krishna, C. V. R. (2020). Identity management using blockchain technology. 3(10), 6.

[59] Nchinda, N., Cameron, A., Retzepi, K., & Lippman, A. (2019). MedRec: A Network for Personal Information Distribution. 2019 International Conference on Computing, Networking and Communications (ICNC), 637641. https://doi.org/10.1109/ICCNC.2019.8685631

[60] Pannifer, S. (2021, June 17). Digital Identity Wallets are coming. Consult Hyperion. https://chyp.com/2021/06/17/digital-identity-wallets-are-coming/

[61] Rahman, S. M. T. (n.d.). BUSINESS MODEL OF BLOCKCHAIN ENABLED SMART CITY SERVICES. 134.

[62] Rathee, T., & Singh, P. (in press). A systematic literature mapping on secure identity management using blockchain technology. Journal of King Saud University- Computer and Information Sciences.

[63] Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., & Cunningham, R. (2019). SoK: Blockchain Technology and Its Potential Use Cases. arXiv:1909.12454 [cs]. http://arxiv.org/abs/1909.12454

[64] Sahmim, S., Gharsellaoui, H., & Bouamama, S. (2019). Edge Computing: Smart Identity Wallet Based Architecture and User Centric. Procedia Computer Science, 159, 12461257. https://doi.org/10.1016/j.procs.2019.09.294

[65] Schanzenbach, M. (n.d.). Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management. 183.

[66] Schanzenbach, M., Grothoff, C., Wenger, H., & Kaul, M. (2021). Decentralized Identities for Self-sovereign End-users (DISSENS). Schanzenbach, Martin; Grothoff, Christian; Wenger, Hansjürg; Kaul, Maximilian (2021). Decentralized Identities for Self-Sovereign End-Users (DISSENS) In: Open Identity Summit. Gesellschaft Für Informatik. Open Identity Summit, Lyngby, Denmark. https://oid2021.compute.dtu.dk/

[67] Sin, E. S., & Naing, T. T. (2021). Digital identity management system using blockchain technology. In D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, & A. Jaiswal (Eds.), International Conference on Innovative Computing and Communications (pp. 895906). Springer. https://doi.org/10.1007/978-981-15-5148-2_78

[68] Sindi, A. F. (n.d.). Adoption Factors of a Blockchain Digital Identity Management System in Higher Education: Diffusing a Disruptive Innovation [Ed.D., California State University, Los Angeles]. Retrieved June 16, 2021, from https://www.proquest.com/docview/2359384031/abstract/7AA1753726E44F8EPQ/1

[69] Stasis, A., Triantafyllou, N., Georgakopoulos, P., Armitt, R. L., & Kavassalis, P. (n.d.). Designing an academic electronic identity management system for student mobility using eIDAS eID and Self-Sovereign Identity technologies. 12.

[70] The Path to Self-Sovereign Identity. (n.d.). Retrieved June 23, 2021, from http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[71] Van Wingerde, M. (2017). BLOCKCHAIN-ENABLED SELF-SOVEREIGN IDENTITY An exploratory study into the concept Self-Sovereign Identity and how blockchain technology can serve the fundamental basis. https://doi.org/10.13140/RG.2.2.17693.82406

THREATS

[72] BRANKER, J., EVELEIGH, T., HOLZER, T. H., & SARKANI, S. (2016). Access control, identity management and the insider threat. Journal of Airport Management, 10(2), 180 199.

[73] EBSCOhost | 93980989 | Online Identity Theft: A Longitudinal Study Of Individual Threat-Response And Coping Behaviors. (n.d.). Retrieved June 16, 2021, from https://eds.b.ebscohost.com/abstract?site=eds&scope=site&jrnl=15512002&asa=Y&AN=93980989&h=pDeGe%2bCBIhpfaKiMJ0LHzWrJpo7EMh44ZKaEfoVIJBzTsoJkdxwJzLY7bEQue8XQl3YXurmqzdkkicBPoeqcQ%3d%3d&crl=c&resultLocal=ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d15512002%26asa%3dY%26AN%3d93980989

[74] Fritsch, L. (2020). Identity Management as a target in cyberwar. Gesellschaft für Informatik e.V. https://doi.org/10.18420/ois2020_05

[75] Zaiss, J., Zaeem, R. N., & Barber, K. S. (2019). Identity threat assessment and prediction. Journal of Consumer Affairs, 53(1), 5870. https://doi.org/10.1111/joca.12191

TRUST MODELS

[76] Castro, P., & Bettencourt, L. (2017). Exploring the predictors and the role of trust and concern in the context of data disclosure to governmental institutions. Behaviour & Information Technology, 36(3), 321331. https://doi.org/10.1080/0144929X.2016.1234645

[77] Koshy, L. (2018). Identity and trust management in distributed systems - a novel approach. https://uobrep.openrepository.com/handle/10547/624021

[78] Palage, M. (n.d.). Digital Identity and Trust Frameworks. 11.

[79] Seltsikas, P., & O'keefe, R. M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value. European Journal of Information Systems, 19(1), 93103 . ABI/INFORM Collection. https://doi.org/10.1057/ejis.2009.51

[80] Smedinghoff, T. J. (n.d.). The Duty to Verify Identity: A Critical Component of Privacy and Security Compliance. 22.

[81] Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging Citizen Adoption of e-Government by Building Trust. Electronic Markets, 12(3), 157162. https://doi.org/10.1080/101967802320245929

[82] Yanushkevich, S. N., Howells, W. G., Crockett, K. A., O'Shea, J., Oliveira, H. C. R., Guest, R. M., & Shmerko, V. P. (2019). Cognitive Identity Management: Risks, Trust and Decisions using Heterogeneous Sources. 2019 IEEE First International Conference on Cognitive Machine Intelligence (CogMI), 3342. https://doi.org/10.1109/CogMI48466.2019.00014

[83] Yanushkevich, S., Stoica, A., Shmerko, P., Howells, W., Crockett, K., & Guest, R. (2020). Cognitive Identity Management: Synthetic Data, Risk and Trust. 2020 International Joint Conference on Neural Networks (IJCNN), 18. https://doi.org/10.1109/IJCNN48605.2020.9207385

INTERNATIONAL INNOVATIVE PRACTICES

[84] Abolarin, K. (2021). DATA GOVERNANCE AND DATA QUALITY GUIDELINES FOR NATIONAL IDENTITY MANAGEMENT COMMISION (NIMC).

[85] Argentina ID Case Study. (2020). World Bank. https://doi.org/10.1596/33403

[86] Argentina ID Case Study: The Evolution of Identification. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/318351582559995027/Argentina-ID-Case-Study-The-Evolution-of-Identification

[87] Boysen, A. (2021). Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.624258

[88] Gruszka, B. (n.d.). Identity Management in Developing Countries: A SWOT-Analysis. . INTRODUCTION, 8.

[89] Guidelines-for-ID4D-Diagnostics.pdf. (n.d.). Retrieved June 3, 2021, from https://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf

[90] ID4D Practitioner's Guide. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/ID4D-Practitioner-s-Guide

[91] ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe.pdf. (n.d.). Retrieved July 8, 2021, from https://documents1.worldbank.org/curated/en/539361582557916734/pdf/ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe.pdf

[92] Identification for Development (ID4D) 2018 Annual Report. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/967301587472879585/Identification-for-Development-ID4D-2018-Annual-Report

[93] Jefferson, K. A. (2015). What's in a Name: A Comparative Analysis of the United States Real ID Act and the United Kingdom's National Identity Scheme. NAVAL POSTGRADUATE SCHOOL MONTEREY CA. https://apps.dtic.mil/sti/citations/ADA632277

[94] Makarim, E. (2021). Privacy and Personal Data Protection in Indonesia: The Hybrid Paradigm of the Subjective and Objective Approach. In E. Kiesow Cortez (Ed.), Data Protection Around the World: Privacy Laws in Action (pp. 127164). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-407-5_6

[95] Micky, L., & Peichi, C. (2021). Media Technologies for Work and Play in East Asia: Critical Perspectives on Japan and the Two Koreas. Policy Press.

[96] Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. Government Information Quarterly, 37(2), 101442. https://doi.org/10.1016/j.giq.2019.101442

[97] Moldova Mobile ID Case Study. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/279851545919735993/Moldova-Mobile-ID-Case-Study

[98] Mutung'u, G., & Rutenberg, I. (2020). Digital ID and Risk of Statelessness Critique and Commentary. Statelessness & Citizenship Review, 2(2), 348354 .

[99] Noack, T., & Kubicek, H. (2010). The introduction of online authentication as part of the new electronic national identity card in Germany. Identity in the Information Society, 3(1), 87110. https://doi.org/10.1007/s12394-010-0051-1

[100] Relying Party Guidance. (n.d.-a). 91.

[101] Relying Party Guidance. (n.d.-b). 91.

[102] Schwabe, D., Laufer, C., & Casanovas, P. (2020). Knowledge Graphs: Trust, Privacy, and Transparency from a Legal Governance Approach. Law in Context. A Socio-legal Journal, 37, 2441. https://doi.org/10.26826/law-in-context.v37i1.126

[103] South Africa ID Case Study. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/315081558706143827/South-Africa-ID-Case-Study

[104] Teslya, N., Mikhailov, S., & Ryabchikov, I. (2019). Forming of Smart City Resident Digital Identity Based On the City Sources Analysis. IEEE International Black Sea Conference on Communications and Networking. BlackSeaCom.

[105] The State of identification systems in Africa - a synthesis of country assessments. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/156111493234231522/The-State-of-identification-systems-in-Africa-a-synthesis-of-country-assessments

[106] The state of identification systems in Africa: Country briefs. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/298651503551191964/The-state-of-identification-systems-in-Africa-country-briefs

[107] Tupay, P. K. (2020). Estonia, the Digital Nation: Reflections on a Digital Citizen's Rights in the European Union Reports: Estonia. European Data Protection Law Review (EDPL), 6(2), 294300 .

BASIC PRINCIPLES

[108] Axioms for the Practice of Security Architecture. (n.d.). Retrieved September 21, 2021, from https://publications.opengroup.org/downloadable/download/link/id/MC42MTc5MjcwMCAxNjMyMjM2NzE5MTA5NDQzMjExMTk4MTgxMDY2/

[109] Bazarhanova, A., & Smolander, K. (n.d.). The Review of Non-Technical Assumptions in Digital Identity Architectures. 10.

[110] Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 2053951719855091. https://doi.org/10.1177/2053951719855091

[111] Bhandari, V., Trikanad, S., & Sinha, A. (2020). Governing ID: Principles of Evaluation (SSRN Scholarly Paper ID 3774917). Social Science Research Network. https://papers.ssrn.com/abstract=3774917

[112] Dhamija, R., & Dusseault, L. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security Privacy, 6(2), 2429. https://doi.org/10.1109/MSP.2008.49

[113] Digital identity: Towards shared principles for public and private sector cooperation. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

[114] Dubois, E., & Martin-Bariteau, F. (2020). Next Steps for a Connected Canada (SSRN Scholarly Paper ID 3620182). Social Science Research Network. https://papers.ssrn.com/abstract=3620182

[115] Ferdous, Md. S., Norman, G., & Poet, R. (2014). Mathematical Modelling of Identity, Identity Management and Other Related Topics. Proceedings of the 7th International Conference on Security of Information and Networks, 916. https://doi.org/10.1145/2659651.2659729

[116] Hühnlein, D., Roßnagel, H., & Zibuschka, J. (2010). Diffusion of federated identity management. Gesellschaft für Informatik e.V. http://dl.gi.de/handle/20.500.12116/19795

[117] Jericho Forum Identity Commandments. (n.d.). Retrieved September 21, 2021, from https://publications.opengroup.org/downloadable/download/link/id/MC40MjM1OTQwMCAxNjMyMjM2OTcwMTA5NDQ1MzExMTk4MzkzMTk%2C/

[118] Khatchatourov, A., & Chardel, P.-A. (n. d.). The ethical challenges of digital identity. The Conversation. Retrieved July 8, 2021, from http://theconversation.com/the-ethical-challenges-of-digital-identity-126564

[119] Khatchatourov, A., & Chardel, P.-A. (2019). The ethical challenges of digital identity. The Conversation France. https://hal.archives-ouvertes.fr/hal-03126022

[120] Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age (SSRN Scholarly Paper ID 2899131). Social Science Research Network. https://papers.ssrn.com/abstract=2899131

[121] Sullivan, C. (n.d.). Digital Identity. 182.

[122] Wessels, B. (2012). Identification and the practices of identity and privacy in everyday digital communication. New Media & Society, 14(8), 12511268. https://doi.org/10.1177/1461444812450679

CANADIAN LEGAL OBLIGATIONS

[123] Charter of Human Rights and Freedoms, RLRQ c. C-12.

[124] Civil Code of Quebec

[125] Act respecting the protection of personal information in the private sector, RLRQ c. P-39.1.

[126] An Act to modernize legislative provisions respecting the protection of personal information, S.Q. 2021, c. 25.

[127] An Act to establish a legal framework for information technology, RLRQ c. C-1.1.

[128] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

[129] An Act to enact the Department of Cybersecurity and Digital Act and to amend other provisions, S.Q. 2021, c. 33.

[130] Regulation (EU) 2016/79 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons, with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[131] Criminal Code, R.S.C. (1985, c. C-46.

[132] Law No. 1,483 of Dec. 17, 2019, on the digital identity of the Principality of Monaco, Journal de Monaco of Dec. 27, 2019.

SYSTEMATIC REVIEWS

[133] Ante, L., Fischer, C., & Strehle, E. (n.d.). A bibliometric review of research on digital identity. 33.

[134] Bazarhanova, A., & Smolander, K. (2020, January 7). The Review of Non-Technical Assumptions in Digital Identity Architectures. https://doi.org/10.24251/HICSS.2020.785

[135] Cao, Y., & Yang, L. (2010). A survey of identity management technology. Proceedings 2010 IEEE International Conference on Information Theory and Information Security, 287293.

[136] ID Enrollment Strategies: Practical Lessons From Around The Globe. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/539361582557916734/ID-Enrollment-Strategies-Practical-Lessons-From-Around-The-Globe

[137] Mburu, Z. G., Nderu, D. L., & Tobias, D. M. (2019). REVIEW OF DIGITAL IDENTITY MANAGEMENT SYSTEM MODELS. International Journal of Technology and Systems, 4(1), 2133.

[138] Pöhn, D., & Hommel, W. (2020). An overview of limitations and approaches in identity management. Proceedings of the 15th International Conference on Availability, Reliability and Security, 110. https://doi.org/10.1145/3407023.3407026

[139] Torres, J., Macedo, R., Nogueira, M., & Pujolle, G. (2012). Identity Management Requirements in Future Internet.

[140] Wessels, B. (2012). Identification and the practices of identity and privacy in everyday digital communication. New Media & Society, 14(8), 12511268. https://doi.org/10.1177/1461444812450679

UNIQUENESS

[141] Duncan, J. D. (n.d.). Birth of identity: Understanding the value and policy considerations of using birth certificates for identity resolution [Ph.D., The University of Utah]. Retrieved July 8, 2021, from https://www.proquest.com/docview/1765692866/abstract/E6AD1EE7E15A4051PQ/1

[142] Edwards, M. J. (n.d.). Data Quality Measures for Identity Resolution [Ph.D., Lancaster University (United Kingdom)]. Retrieved July 8, 2021, from https://www.proquest.com/docview/2083742845/abstract/B84F15BBC077469FPQ/1

[143] Helland, P. (2019). Identity by any other name. Communications of the ACM, 62(4), 8080. https://doi.org/10.1145/3303870

[144] Janssen, J. (n.d.). Identity management within an organization. 96.

[145] Kumaraguru, P. (n.d.). Submitted By Rishabh Kaushal PhD15008. 50.

[146] Lin, T., & Misra, S. (2021). The Identity Fragmentation Bias. arXiv:2008.12849 [econ, stat]. http://arxiv.org/abs/2008.12849

[147] Staite, C., & Bahsoon, R. (2012). Evaluating identity management architectures. Proceedings of the 3rd international ACM SIGSOFT symposium on Architecting Critical Systems. ISARCS, New York.

[148] Wang, G. A., Atabakhsh, H., & Chen, H. (2011). A hierarchical Naïve Bayes model for approximate identity matching. Decision Support Systems, 51(3), 413. ABI/INFORM Collection.

PRIVACY POLICY

[149] A Novel Methodology for Security and Privacy Protection Issues of Data in Cloud Computing-Indian Journals. (n.d.). Retrieved June 16, 2021, from https://www.indianjournals.com/ijor.aspx?target=ijor:ijemr&volume=6&issue=1&article=026

[150] Abdu, N. J., & Lechner, U. (2016). A Threat Analysis Model for Identity and Access Management. Proceedings of the 2nd International Conference on Information Systems Security and Privacy, 498502.

[151] Agre, P. E. (1999). THE ARCHITECTURE OF IDENTITY: Embedding privacy in market institutions. Information, Communication & Society, 2(1), 125. https://doi.org/10.1080/136911899359736

[152] Alnsour, Y., & Jumah, A. (2021). Exploring the Effects of Information Security & Privacy on Blockchain Mobile Applications Rating: Text Analytics Approach. AMCIS 2021 Proceedings. https://aisel.aisnet.org/amcis2021/sig_acctinfosystem_asys/sig_acctinfosystem_asys/3

[153] Aloui, A., Msahli, M., Abdessalem, T., Bressan, S., & Mesnager, S. (2017). Protocol for preserving privacy in distributed system (PPDS). 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 18851890. https://doi.org/10.1109/IWCMC.2017.7986571

[154] Andreou, A., Goga, O., & Loiseau, P. (2017). Identity vs. Attribute Disclosure Risks for Users with Multiple Social Profiles. Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017, 163170. https://doi.org/10.1145/3110025.3110046

[155] Ben Ayed, G., & Ghernaouti-Hélie, S. (2011). Privacy Requirements Specification for Digital Identity Management Systems Implementation Towards a digital society of privacy. 6th International Conference on Internet Technology and Secured Transactions. ICITST, Abu Dhabi, United Arab Emirates.

[156] Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2), 483. https://doi.org/10.3390/s20020483

[157] Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, 1, 647651. https://doi.org/10.1109/ICCSEE.2012.193

[158] Clauß, S., & Kesdogan, D. (n.d.). Privacy Enhancing Identity Management: Protection Against Re-identification and Profiling. 10.

[159] Clauß, S., Kesdogan, D., & Kölsch, T. (2005). Privacy enhancing identity management: Protection against re-identification and profiling. Proceedings of the 2005 workshop on Digital identity management, 8493. https://doi.org/10.1145/1102486.1102501

[160] de Andrade, N. N. G. (2011). Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), Privacy and Identity Management for Life (Vol. 352, pp. 90107). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20769-3_8

[161] Dienlin, T., Masur, P. K., & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. New Media & Society, 14614448211016316. https://doi.org/10.1177/14614448211016316

[162] Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22(3), 295316. ABI/INFORM Collection. https://doi.org/10.1057/ejis.2012.23

[163] Fragoso Rodriguez, U. (2009). Privacy model in a federated identity architecture [These for PhD, Evry, National Institute of Telecommunications]. https://www.theses.fr/2009TELE0026

[164] Hahn, H. (2021). Digital identification systems and the right to privacy in the asylum context. https://pub-data.leuphana.de/frontdoor/index/index/year/2021/docId/1124

[165] Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., & Waidner, M. (2004). Privacy-Enhancing Identity Management. Information Security Technical Report, 9, 3544. https://doi.org/10.1016/S1363-4127(04)00014-7

[166] Hörbe, R., & Hötzendorfer, W. (2015). Privacy by Design in Federated Identity Management. 2015 IEEE Security and Privacy Workshops, 167174. https://doi.org/10.1109/SPW.2015.24

[167] Jackson, P. M., Ligertwood, J., O'Donnell, J., & Shelly, M. (n.d.). Small Business: Issues of Identity Management, Privacy and Security. 15.

[168] KAUR, J., & Dhillon, S. (2021). Privacy calculus and intension to share confidential information. AMCIS 2021 Proceedings. https://aisel.aisnet.org/amcis2021/info_security/info_security/11

[169] Kaur, P. C., Ghorpade, T., & Mane, V. (2016). Analysis of data security by using anonymization techniques. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 287293. https://doi.org/10.1109/CONFLUENCE.2016.7508130

[170] Nergiz, M. E., Clifton, C., & Nergiz, A. E. (2009). Multirelational k-Anonymity. IEEE Transactions on Knowledge and Data Engineering, 21(8), 11041117. https://doi.org/10.1109/TKDE.2008.210

[171] Prasser, F., Eicher, J., Spengler, H., Bild, R., & Kuhn, K. A. (2020). Flexible data anonymization using ARX-Current status and challenges ahead. Software: Practice and Experience, 50(7), 12771304. https://doi.org/10.1002/spe.2812

[172] Priesnitz Filho, W., Ribeiro, C., & Zefferer, T. (2019). Privacy-preserving attribute aggregation in eID federations. Future Generation Computer Systems, 92, 116. https://doi.org/10.1016/j.future.2018.09.025

[173] Privacy by Design: Current Practices in Estonia, India, and Austria. (n.d.). [Text/HTML]. World Bank. Retrieved June 3, 2021, from https://documents.banquemondiale.org/fr/publication/documents-reports/documentdetail/546691543847931842/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria

[174] Rajendran, K., Jayabalan, M., & Rana, M. E. (2017). A Study on k-anonymity, l-diversity, and t-closeness Techniques focusing Medical Data. 17.

[175] Rocha, M. (2016). Data Privacy and Social Acceptance of Smart Meters. In Smart Grid Handbook (p. 19). American Cancer Society. https://doi.org/10.1002/9781118755471.sgd026

[176] Rodriguez, U. F. (2009). Privacy model for federated identity architectures [Phdthesis, National Institute of Telecommunications; Instituto tecnológico autónomo (México)]. https://tel.archives-ouvertes.fr/tel-00541850

[177] Schwartz, A. (2011). Privacy and Security: Identity Management and Privacy: A Rare Opportunity To Get It Right. Association for Computing Machinery. Communications of the ACM, 54(6), 22. ABI/INFORM Collection.

[178] Wood, S. (2020). Adhering to privacy by design with identity-as-a-service. Network Security, 2020(7), 1417. https://doi.org/10.1016/S1353-4858(20)30081-7