# "Lose Your Phone, Lose Your Identity": Exploring Users' Perceptions and Expectations of a Digital Identity Service

Michael Lutaaya
*School of Computer Science*
*Carleton University, Canada*
michael@lutaaya.com

Hala Assal
*Systems and Computer Engineering*
*Carleton University, Canada*
assal@sce.carleton.ca

Khadija Baig
*School of Computer Science*
*Carleton University, Canada*
khadijabaig@cmail.carleton.ca

Sana Maqsood
*School of Computer Science*
*Carleton University, Canada*
sana.maqsood@carleton.ca

Sonia Chiasson
*School of Computer Science*
*Carleton University, Canada*
chiasson@scs.carleton.ca

***Abstract*—Digital identities are gaining traction and spurring the interest of governments around the world. In this paper, we explore the concept of digital identity from the user's perspective, using a digital identity prototype as a prop. To this effect, we conducted a user study with 22 participants to understand their perceptions and expectations of digital identity services. We conducted the study in Canada, where digital identities are not yet widely adopted. Our participants identified some benefits of using digital identity, particularly those relating to the convenience of using a digital format rather than a printed one. However, participants did not recognize the privacy-preserving benefits of using a digital service. They also expressed concerns about the associated privacy risks, particularly around how their data would be handled and the risk of privacy and security breaches. Based on our findings, we provide recommendations for designing digital identity services that are both usable and privacy-protective.**

## I. Introduction

While physical proofs of identity have served society well for decades, their status as authoritative documents has diminished as counterfeits have become easier to produce [18], [26]. In addition, an individual's privacy can only be protected to a limited degree with physical documents since there is no guarantee that, during an exchange, the other party will only use the minimal amount of information. For example, car rental agencies must ensure that a driver has a valid driver's license but they do not necessarily need all of the personal information included on a driver's licence card. Many agencies, however, take a photocopy of the card. Some organizations view digital identities as the solution to these problems [37]. The term *digital identity* commonly refers to the digital representation of a set of attributes that describe an individual [22]. While more countries are looking to transition to digital formats for their citizens' identity documents, few works have examined this technology from the user's perspective. To fill this gap, we studied identity services with two research questions: *RQ1: How do users perceive digital identity services? RQ2: What are users' expectations for digital identity services?*

We conducted a study with 22 participants. During the session, participants interacted with a digital identity service prototype and took part in an interview. The prototype was used as a stimulus to explore participants' perceptions and expectations of digital services, and provided context to facilitate the expression of their feedback. Our research was conducted in Canada, a country where physical proofs are still largely relied on for identity verification [14], [17], although recent initiatives could enable a transition to digital formats[1].

While participants were able to identify some advantages of digital identity services, such as speed and efficiency, they did not recognize their privacy-preserving features. In addition, participants were particularly concerned about how using such a service would affect their privacy and security. The contributions of this work include: (1) the characterization of users' perceptions and expectations of digital identity services, and (2) a set of practical guidelines that digital identity services should follow to mitigate against users' main concerns.

## II. Background

Existing literature shows continued advancement in the functionality of digital identity services but few works examine how this technology fares with users. This gap presents an opportunity to analyze digital identity from users' perspective.

### A. Key Terminology

The term *identity* refers to the collection of attributes, preferences, and traits that define who or what an entity is (*e.g.,* a person's name, date of birth, hair color, or preferred email

Workshop on Usable Security and Privacy (USEC) 2021
7 May 2021, Auckland, New Zealand
ISBN 1-891562-73-8
https://dx.doi.org/10.14722/usec.2021.23011
www.ndss-symposium.org

[1] https://bluink.ca/eid-me/individuals

address) [2], [9], [38]. The individual attributes, preferences, and traits that comprise an identity are also known as *identity attributes*. When one or more identity attributes distinguish an individual from a larger population, those attributes are considered *personally identifiable information* (*PII*) [12]. Identity attributes can be represented in a digital format (*digital identity*). Digital identities can be used to represent different entities (*e.g.,* people, devices, applications), but this paper focuses on *eID*: digital identities specifically for people.

Prior to being issued a digital identity, individuals may go through an *identity proofing* process where they provide personal information to a credential service provider (CSP), such as a government agency [3], [7], [22]. If the CSP can validate and verify the information and has enough confidence that the individual is who they claim to be, it will issue a *credential* (*e.g.,* digital certificate) to the individual for use in transactions that require proof of identity [3], [36], [38]. Some implementations of digital identity allow users to present their credential as proof of identity to a relying party without having to share any PII during the transaction.

### B. Canadian Norms

*1) Digital Identity:* The evolution of digital identity services in Canada is rather fragmented. While some provinces have solutions allowing residents to use a single identity across different contexts [20], [21], most Canadians manage their identities with a variety of physical and digital credentials (*e.g.*, multiple identity cards, usernames, and passwords) [10], [14], [17].

*2) Social Insurance Number (SIN):* A Social Insurance Number (SIN) [35] is a nine-digit number issued to citizens, permanent residents, and temporary residents by the Canadian federal government for identification purposes. Individuals must provide their SIN to work in Canada, to receive government benefits, and to file taxes. The SIN is meant to be kept confidential since if it is lost or stolen, it could be used for fraudulent activities, such as redirecting government benefits, redirecting tax refunds, or opening new financial accounts.

### C. Prior Work

Many countries have considered adopting eIDs; however, the switch from paper to electronic is considered a fundamental transition in how citizens and governments interact [1] and can have socio-technical impact across many aspects of daily life. Further, the adoption of eID can have significant privacy and security implications. We provide an overview of the early implementations in which some of these challenges arose and discuss literature that focuses on these implications.

In 1999, Finland made a non-mandatory eID available to its citizens [30] that could be used as a travel document, to access government services, and to sign documents electronically. It never saw widespread adoption because citizens felt that it was unnecessary and there were usability and compatibility issues, particularly with web-based services. Finland's challenges serve as a reminder that, for users, digital identity and its management is not a goal in itself [13]; digital identities should be seamless, secure, and private to allow users to focus on their primary tasks [13]. Besides general usability, this may mean limiting user options in some cases to minimize chances of over-disclosing information. Digital identity services may also introduce confusion around who to contact to resolve issues—is it the organization that issued users their card or the organization requesting their credentials?

In the early 2000s, Austria launched its Citizen Card (CC), an implementation of eID compatible with a range of devices (*e.g.,* smart cards, cell phones, USB tokens) and primarily used to access government services. CC's distinguishing feature is its use of *sector-specific personal identifiers* such that, *e.g.,* one's identity with a hospital (health sector) cannot be linked to their identity used for tax filing (tax sector). Aspects of CC relate to Hansen et al.'s [23] assessment of 'partial identity'—the idea that in most transactions, only a subset of your identity attributes are necessary for the exchange. Managing how these partial identities are used can be unwieldy given that an individual's digital footprint tends to continuously grow. For instance, even after death, one's SIN and associated data might persist to facilitate the payment of benefits to a dependent. The authors further discuss issues relating to partial identity management throughout a user's lifespan, including privacy and security concerns, and suggest mitigation mechanisms, such as packaging privacy policies with user data and logging any misuse automatically.

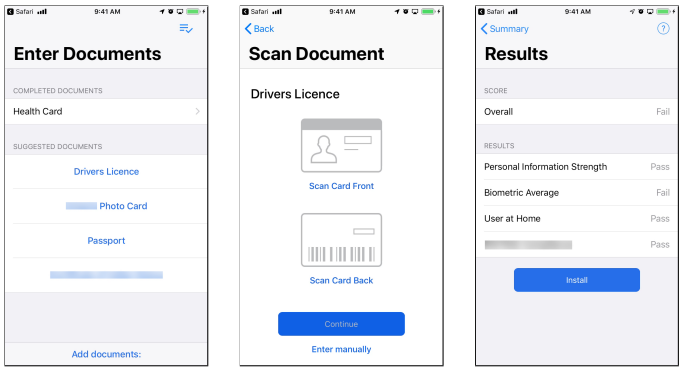
Estonia's mandatory eID smart card allows its citizens to obtain access to services like banking, voting, and health insurance [34]. Its microchip includes users' information and stores a key pair used to sign information shared with a relying party. However, in 2017, a software vulnerability made it possible for attackers to derive the card's private key from the corresponding public key [5], [19]. This highlights a concern held by many users: how safe is their data and to what extent might it be compromised if breaches occur?

Through a systematic literature review, Bazarhanova and Smolander [4] identified the non-technical assumptions made in proposed solutions for digital identity management. They describe a spectrum: at one extreme, users have full control over their digital identity (thus, requiring the provider to assume the user is proficient enough to secure their identity); at the other extreme, intermediaries operate or manage aspects of the solution (thus, requiring them to be trusted by end users). The authors found that in practice, most solutions involved intermediaries, and they called for future research to assess these relationships and the associated incentives.

Nielsen [29] argues that these types of collaborations, particularly those between the public and private sectors, are needed to ensure that a digital identity management solution has "a critical mass of users and volume of use." To support this claim, Nielsen points to both successful and failed solutions as evidence of the correlation between the existence of these partnerships and the success of the solution.

## III. Prototype

We used an eID prototype app to provide context and ground the conversation while exploring participants' perceptions of digital identities. The prototype eID-Me app was developed in collaboration with Bluink Ltd., a local technology company. The final solution is intended for eventual adoption by Canadian provincial governments to allow residents to prove their identity using their smartphone in person or online. An advantage of




(a) (b) (c)

Fig. 1. eID-Me's registration process

digital identity apps, such as eID-Me is that instead of needing to manage usernames and passwords, or fill out lengthy forms, users can identify themselves through the app and digitally transmit their information to the relying party.

### A. Registration

To register, users complete an identity proofing process by providing some PII to the app, including location information from their smartphone, a selfie, and photographs of their government-issued identity documents (Fig. 1a and 1b). The app then sends this PII to the eID-Me Registration Authority (RA) to calculate a Strength of Identity Proofing (SIP) score (Fig. 1c). The RA is a trusted entity which verifies the provided information before issuing a digital identity certificate. In actual deployment, the government would act as the RA for eID-Me and would ultimately be reliant upon partnerships with the private sector to operate the service.

This SIP score reflects the estimated authenticity of the user's PII by considering factors such as how closely the PII matches with government databases and third-party identity verification services, and whether the selfie appears to have been taken by a live person.

If the user's SIP score is high enough, the RA issues a digital identity to the user and assigns them a six-character unique identifier. If the score is too low, users can try to improve their score by submitting additional documents to the app or can complete the process in person by visiting a service centre.

### B. In-Person Authentication

To authenticate in person, users tap the *Use My Identity* button in the app. The app generates and displays a QR code representing a nonce (random number used once) for the user to present to the relying party's scanner (Fig. 3b). Once scanned, the app connects securely to the relying party's point of sale (POS) using Bluetooth without needing an Internet connection. The request for identity information then appears on the user's device (Fig. 3c), which the user can approve, to send the requested information to the POS (Fig. 3d), or decline. This entire process takes approximately ten seconds.

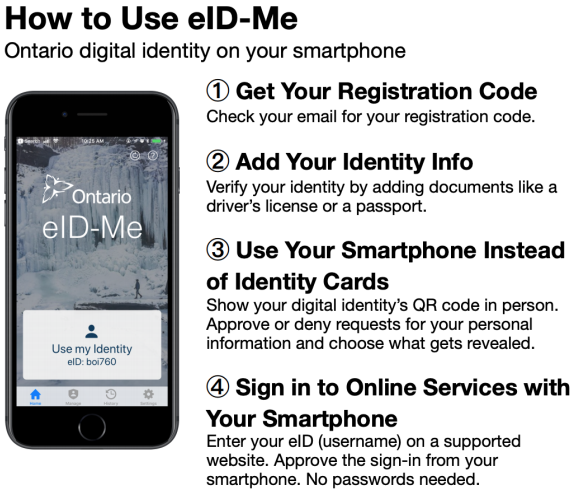



Fig. 2. Pamphlet about eID-Me provided to participants

### C. Online Authentication

eID-Me implements multiple federated identity protocols, such as OpenID Connect [32], allowing authentication on supported websites using digital identities rather than passwords. To authenticate online, the user visits a supported website and clicks on the federated login button for authenticating with eID-Me. The user's browser is redirected to a form asking for their six-character unique identifier. Upon submission, the web page displays a four-digit confirmation code and instructs the user to open eID-Me on their phone. The app lists the information requested by the relying party and requires the user to select the matching four-digit confirmation code (Fig. 3e). Once the user approves the request, the relying party receives the requested information.

## IV. Methodology

To address our research questions, we conducted an IRB-cleared lab-based user study with 22 participants[2] . Participants tried out eID-Me, completed pre- and post-test questionnaires, and took part in a semi-structured interview. While we were interested in the usability of the app, we primarily used it to prompt discussion about eID in general. Study sessions were audio recorded and transcribed. All sessions were conducted on our university campus, situated in Ottawa.

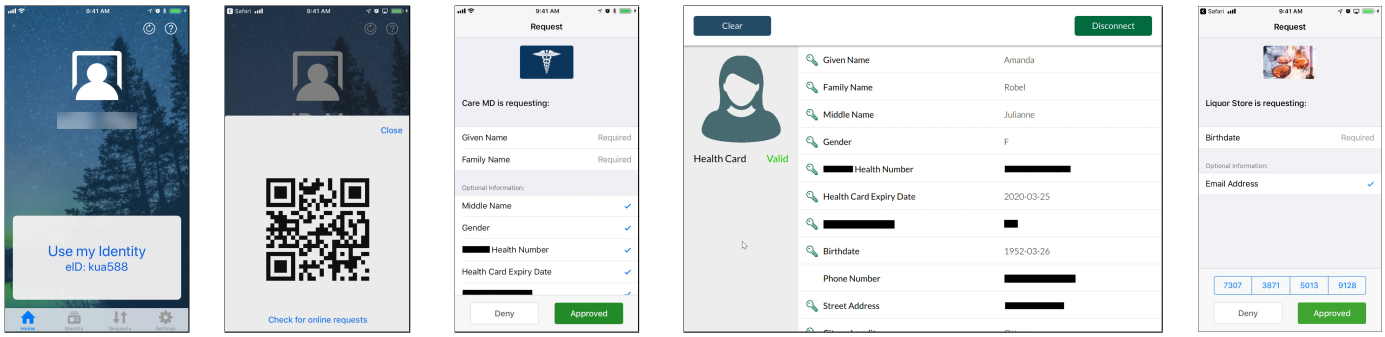
### A. Recruitment

Participants were recruited through posters displayed in public locations and on various online channels (*e.g.,* email lists, Facebook groups). They had to be at least 18 years old, fluent in English, and own an iPhone or Android smartphone.

### B. Procedure

Participants were provided an overview of the study, an explanation of the general concept of digital identity, and a pamphlet (Fig. 2) briefly explaining the app's purpose. In these explanations, we did not specify any particular entity as the

[2]Data collection occurred prior to the COVID-19 pandemic.




(a) (b) (c) (d) (e)

Fig. 3. (a) eID-Me's home screen; (b) QR code generated for the relying party (c) the in-person authentication process (user); (d) the in-person authentication process (relying party); (e) the interface for online authentication

RA; Participants completed a pre-test questionnaire and the following tasks [3]:

1) **Register:** Participants entered a researcher provided email address in the app and received an email with a registration code and link for forwarding the code to the app.
2) **Sort Documents:** Participants were provided with mock physical identity documents to use as their own, which they categorized according to their level of comfort at providing them for identity proofing: *comfortable providing*, *will provide reluctantly*, and *uncomfortable providing*. Participants were asked to explain their choices.
3) **Take Photo:** Participants captured a 'selfie' using the app by photographing the individual on the mock documents instead of themselves to maintain their privacy.
4) **Input Documents:** Participants entered into the app the documents which they classified as *comfortable providing* or *will provide reluctantly* in Task 2. They did this by using the phone's camera or by entering the information manually. After verification, the app issued a digital identity to the participant.
5) **In-Person Use:** To test in-person authentication, participants role-played using it to check-in to an appointment at the hospital. For this, we operated a physical barcode scanner and proof-of-concept medical practice software.
6) **Online Use:** To test the app's online authentication, participants visited a proof-of-concept website of an alcohol retailer and used the app to verify their identity.

Participants completed a post-test questionnaire evaluating their likelihood of using a government-approved smartphone app for digital identity in various contexts.

The second half of the session covered a 25-minute semi-structured interview exploring (1) participants' views of digital identity (2) their willingness to use digital identities in different contexts (3) their willingness to use specific documents as proof of identity (4) perceived advantages and concerns with regards to digital identities (5) and their experience using eID-Me.

### C. Analysis

**Quantitative Data:** We summarize participants' responses to the Likert-scale questions in the questionnaires, and their level of comfort with providing identity documents.

[3]Specific contexts (*i.e.,* a hospital and an alcohol retailer) were used for *Tasks #5* and *#6* but many other contexts are also plausible.

TABLE I. CATEGORIES AND SUBCATEGORIES FROM QUALITATIVE DATA ANALYSIS

| |
|---|
| **Attribution of Responsibility** |
| Government |
| For-profit companies |
| **Perceived Benefits** |
| Speed and efficiency |
| Redundancy |
| Less to carry |
| **Drawbacks and Concerns** |
| Hacking, identity theft, and forgery |
| Tracking and monitoring |
| Secondary use of personal information |
| Reliance on mobile phones and network connectivity |
| Technology misconceptions |
| **User Requirements** |
| Requests for additional security features |
| Requests for additional functionality |
| Technical support |

**Qualitative Data:** We analyzed 361 pages of transcripts for 27 hours of recorded audio, and 11 pages of written notes. We used the qualitative content analysis methodology [15] to analyze this data. We split these documents into two sets with 36% overlap. Each set was coded by one researcher (*i.e.,* two researchers coded the data), using the individual questions posed to the participants as the unit of analysis. We used a common codebook, which was created using both deductive content analysis (*i.e.,* we based the initial codebook on our research questions) and inductive content analysis (*i.e.,* as coding progressed, we revised the codebook to reflect the nuances present in the data). The two researchers met regularly to discuss their analyses and resolve disagreements. The researchers reached 80% agreement on the overlapping documents, thus meeting established guidelines [27] for reliability. For discrepancies, the researchers discussed to meet consensus. Table I lists the most relevant subset of categories and subcategories that resulted from this analysis. We focus on results relating to the concept of digital identities and our research questions.

### D. Participants

Twenty-two participants (11 female, 10 male, 1 unspecified) completed the study. They were between the ages of 19 and 59 years ($M$ = 32, $SD$ = 12). All but one completed post-secondary education or were in the process of earning accreditation from a post-secondary institution. We identify participants as P1–P22.

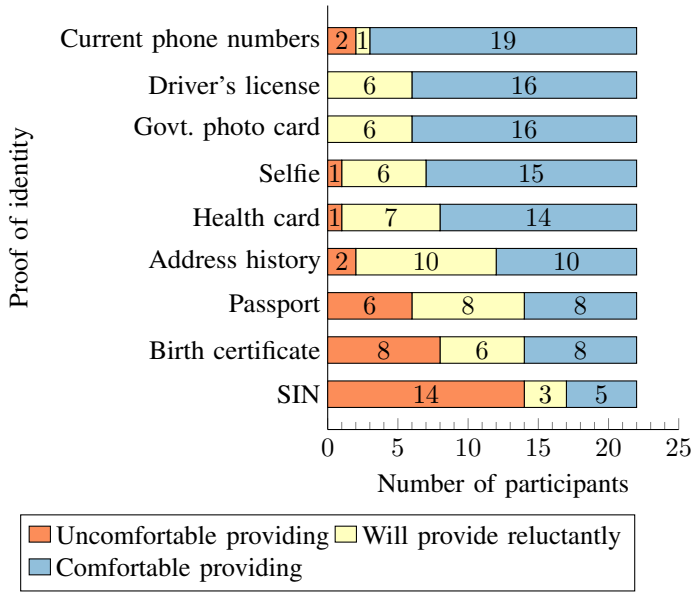



Fig. 4. Willingness to provide specific PII documents and information for digital identity registration purposes ($\boldsymbol{N}$ = 22).

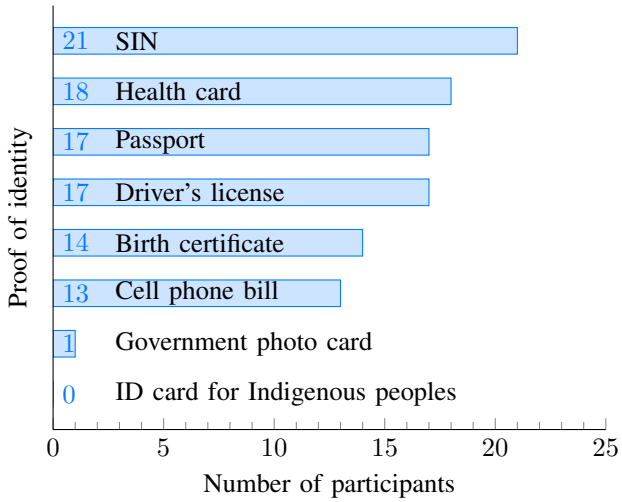



Fig. 5. Proofs of identity owned by participants ($\boldsymbol{N}$ = 22).

Our participants were avid smartphone users: 95% kept their phone within reach and operable for at least 80% of their waking hours. They also used their phones for person-to-person payments ($n$ = 17), saved payment information in apps ($n$ = 11) and on websites ($n$ = 11), and used their phone with contactless card readers ($n$ = 10).

## V. Quantitative Results

### A. Comfort With Providing Documents

Fig. 4 shows the outcomes of the document sorting exercise (Task 2). Specifically, it shows that participants were comfortable providing certain types of documents and information to eID-Me (*e.g.,* phone numbers, driver's license, photo card), but were strongly opposed to sharing others. From participants' explanations, we found that their level of comfort with providing information was generally dependent on their perceived risk of information misuse. For example, many participants were opposed to providing their Social Insurance Number (SIN) because it could be used to commit fraud (*e.g.,* to redirect government benefits or tax refunds).

### B. Document Ownership

From the questionnaires, we found that the most commonly owned identity documents among participants were the SIN, health card, passport, and driver's license (Fig. 5), but none were universally owned. No one owned an Indigenous peoples' identity card and only one owned a government photo card (issued on request, typically to those who do not have a driver's license but want government-issued photo ID). This suggests that identity proofing processes and applications should be designed to request and accept a variety of proofs from users.

### C. Likelihood of Use

We used four 5-point Likert scale questions (1 = Extremely unlikely and 5 = Extremely likely) to evaluate participants' perceived likelihood of using a government-approved app as their proof of identity instead of traditional documents. In general, participants were more comfortable using a digital identity to access healthcare services or as proof-of-age for a business, and but about half were reluctant to use it with law enforcement. Participants responded to this question before and after using our app prototype. We found that participants were initially amenable to using a government-approved app as their proof of identity (pre-test: $M$ = 3.95, $SD$ = 1.17), but these sentiments became slightly more negative in the post-test questionnaire ($M$ = 3.77, $SD$ = 1.31). One explanation could be that by using the app, participants become more aware of possible privacy concerns, which changed their perceived likelihood of using the government-approved digital identity app. A second possibility is that participants focused on specific details of the app in the post-test given that they had just interacted with it, as opposed to considering the broader question. Furthermore, an individual's likelihood of use in practice may be affected by factors not known at the time of the study (*e.g.*, which organizations accept the identity, what alternatives are available).

## VI. Qualitative Results

Table I provides an overview of categories and subcategories most relevant to our research questions; for brevity, we excluded categories and subcategories that, *e.g.,* relate to the usability of the prototype itself.

### A. Attribution of Responsibility

We found that participants generally had expectations for who should be responsible for managing digital identity services, but these were not uniform. In fact, we found strong contrary opinions, which suggests that adoption of a widespread digital identity service would face resistance by some portion of the population regardless of who manages it.

The **government** was the obvious contender for some participants, *e.g.,* because "*the government is screening everything*" (participant P7). Others were skeptical of government-backed digital identity systems, *e.g.,* participant P22 said,

"*How much can we trust the government to do [technical projects] properly?*" These participants preferred relying on **for-profit companies** as these are incentivized to "*guarantee that everything is secured and that the customer is happy*."

### B. Perceived Benefits

In our analysis, it was what participants did *not* mention as a potential benefit that was most noteworthy. There was little or no mention of any possible privacy-preserving features, indicating a need for careful attention to how digital identity services are framed, given that this is one of their key benefits. Participants' views on the benefits of a digital identity service mostly related to the convenience of having their information in a digital format rather than a traditional printed format.

***Speed and efficiency.*** Several participants felt that using a digital identity could be faster than traditional identity documents, such as participant P21 who said it would be quicker than "*searching [her] bag and bringing out the ID*" and participant P7 who said users could "*just scan once and go*" instead of filling out lengthy forms at hospitals, for example. Others pointed to the reduction in manual work as a key benefit, by automatically transferring the information to the relying party.

***Redundancy.*** Multiple participants thought of a digital identity as a backup of their physical identity documents. Participant P3 explained that if he had forgotten his wallet, it would be advantageous to "*have [a driver's license] in [his] phone*" since people "*carry [their] phone all the time.*"

***Less to carry.*** Several participants explained that digital identities would eliminate their concerns with needing to carry physical identity documents. Participant P15 explained that a digital identity could alleviate her "*[paranoia] as to whether [she] had a certain form of ID*" since mobile phones are "*the one thing [people] don't leave the house without.*"

### C. Drawbacks and Concerns

In clear contrast with perceived benefits, participants' concerns and views on the downsides of digital identity services were primarily rooted in how their data would be handled, risks associated with providing personal information to an app, and technology misconceptions. Participants had several security and privacy concerns.

***Hacking, identity theft, and forgery.*** Some participants feared identity theft, believing that determined attackers would be able to surmount any protective measures. For example, Participant P16 felt that digital identities would be just as susceptible as any other system: "*Somebody's going to become me . . . One way or another, [the information] can get stolen. My credit card information is another database that can get stolen and hacked. Anything can get hacked at the end of the day.*"

Despite mechanisms for verifying users' identity claims, some participants were concerned that it would be possible for digital identities to contain fraudulent information. Participant P4 imagined a scenario where a young teenager could pretend to have reached the legal drinking age because identity claims are "*not verified by anyone.*" On the other hand, participant P15 expressed confusion over what confirming the legitimacy of a digital identity entails; he wondered whether the absence of physical security features (such as holograms on ID cards) might make it "*more difficult for bartenders and such to determine if [the ID is] real.*"

Although digital identities can provide additional protection against identity theft compared to traditional methods, participants were unaware of these protections and many instead perceived greater risk.

***Tracking and monitoring.*** Participants had significant privacy and surveillance concerns. They were concerned about whether their use of these services and any personal information they provide would be tracked by the government or private companies. For instance, participant P19 expressed weariness over private-sector companies operating a digital identity service and wondered if her use of the service could be used against her: "*. . . I guess media has conditioned me to think, 'Oh, what are [private-sector companies] doing with this information? What are they going to do with it later? Could this become Big Brother? Could this be used to discriminate for jobs?'*" In another example, participant P16 asked if using his digital identity at a liquor store would mean that "*the government [would know] how often [he goes] to the liquor store.*" Several participants wondered what kind of statistics this would enable the government to keep.

Similarly, participant P22 expressed skepticism over the trustworthiness of permission requests after "*recent issues with Facebook*," such as the Cambridge Analytica data scandal [8]: "*I don't know if the camera's on right now but if it is on in the background and it's seeing my face, that could potentially be a little unsettling.*"

Some participants were unable to establish a clear understanding of who would be able to access their PII and information associated with their use of a digital identity service. Participant P4 believed that Apple (the manufacturer of our test device) could obtain access to a digital identity and its contents though iCloud Backup saying, "*as soon as the information's on the cloud, [Apple has] access at all times.*" In discussing their avoidance of OS updates, Participant P15 said, "*Every single time that you do an update, more of your personal information just gets accessible to—not everybody but, like, law enforcement and such [...]*"

***Secondary use of personal information.*** Participants worried about what else might happen to their data. Participant P16 felt that companies were not incentivized to put users first: "*. . . companies are accountable to shareholders, board [sic] of directors, and other people who are more in it for profits than they are for providing a national service to the people.*"

Participant P8 worried that if a police officer took her phone away to verify her digital identity, the officer could go through other information on the phone, such as her medications. In her words, an app makes "*too much information available to anybody. . . . it's too open.*" Participants with these types of concerns were uncomfortable with hosting their proof of identity on the same device that has access to so many other facets of their life. To alleviate this concern, the digital identity app should be able to provide the requested identity information while keeping the rest of the phone locked.

***Reliance on mobile phone and network connectivity.*** Participants discussed pain points that deter the replacement of their traditional documents with digital identities. These points were specific to the device, such as losing power or connectivity. Participant P15 said that the unreliability of his "*older model*" phone would encourage him to "*always make sure [he] has [his] paper documents . . . in case the app didn't work. . . .*" In addition, participant P11 felt that using a digital identity was too risky, saying, "*Lose your phone, lose your identity, lose everything.*" Others worried about infrastructure issues such as natural disasters disrupting service, or travelling to jurisdictions without this service. Participants noted that while cumbersome, the 'low-tech' identity cards were less susceptible to technological problems.

***Technology misconceptions.*** We found that general technology misconceptions, such as those about QR codes, also hindered participants' ability to accurately understand digital identity. For example, participant P11 misinterpreted the purpose of the app's QR code; she thought the QR codes existed only to "*[give] you. . . detailed information on objects,*" such as when looking up information about a product while in a retail store. This highlights the need for very explicit (yet brief and simple) instructions within the app relating to key interactions, even when the interaction itself is simple (*e.g.,* scanning a QR code).

These general technology misconceptions can also lead to misconceptions about privacy, thereby impacting users willingness to adopt digital identity services. For example, at least four participants incorrectly believed that their identity information was embedded in the QR code when in reality, the QR code was random, contained no personally identifiable information, and was only used to connect the smartphone to the POS terminal. Participant P4 speculated that relying parties would "*only [scan] the information that they need and not any additional information even though all the information is in your barcode*". In reality, the relying party only has access to the data that was authorized by the user (and none is in the QR code). This misconception could lead users to believe that the trustworthiness of relying parties (to not access more than they should) is paramount, whereas in practice the system protects against this threat and control over information sharing remains with the user.

### *D. User Requirements*

Participants also described what they expect a digital identity service to offer. These remarks help to identify requirements for future implementations of digital identity services.

***Requests for additional security features.*** Some participants expressed interest in mechanisms for disabling their digital identity. Participant P20 wanted to "*[be] able to lock [his digital identity] out completely*" upon losing his phone and be able to reactivate his identity on a replacement device.

Participant P8 wanted some degree of ephemerality when sharing information with relying parties: "*Once they've printed off my hospital bracelet, I [should be able to] press on my phone 'Disconnect' so that they can no longer see my information. They have it already recorded, they don't need to stare at it anymore.*"

***Requests for additional functionality.*** Participants envisioned a wide range of uses for a digital identity. For example, participant P8 wanted to add documents for people in her care: "*. . . As a mom, if I'm going to do my health card, I'd like to do my children's so it's all together, right? And maybe, perhaps if I'm responsible for other people.*" Others wanted to be able to use the app for storing other types of information, such as car insurance information and student IDs. In addition, participant P4 believed that storing his credit card information in such apps is more "*secure than just in the Apple Wallet.*"

***Technical support.*** Participants expressed a need for clear support channels in digital identity apps. Participant P17 suggested that the app should include contact information for the people responsible for the app so users can ask questions: "*You know when you buy something from IKEA and they tell you, 'Well, don't break it. If you don't know how to do it, call us.' Something like that.*" Participant P8 echoed this suggestion saying that a toll-free number should be provided to make your identity "*inoperable*" or to "*put a pause on the app*." On the other hand, participant P5 highlighted the importance of including resources to help identity theft victims. She believed that such resources would "*[show] the friendliness of the app*" and reinforce that someone is "*looking out for [the user] in a sense.*"

## VII. Limitations and Mitigations

To protect participants' privacy, we provided participants with a mobile device, a laptop, and sample identity documents, rather than using their own devices or documents during the study. This may have influenced participants' opinions (*e.g.,* when reporting their level of comfort with providing specific types of information in the sorting exercise). However, we asked participants to treat these devices and documents as if they were their own and contained their personal information. We note that participants did have a range of responses when deciding whether to share particular information (Fig. 5). This sorting exercise asked about willingness to share for the purposes of digital identity registration. It is, therefore, difficult to determine if participants' reluctance to share is a function of distrust of eID-Me or a general privacy concern. To try and minimize this effect, we placed the sorting exercise early in the session (Task 2), before participants interacted much with the app.

All study sessions were conducted in a lab setting, which did not allow for a realistic time lapse between participants' completion of the registration phase and the actual use of the app (*e.g.,* in-person authentication). To increase realism, we did include realistic physical identity documents and POS hardware to scan the QR code.

We provided participants with basic instructions on how to use eID-Me (Fig. 2). These were minimal and did not contain any information about the functionality and implementation of digital identity services. Thus, we believe that they did not unduly influence participants' responses to the questions in our questionnaires and interview.

Our participants were highly educated and regular smartphone users; therefore they were comfortable with technology and, although this describes many people (*e.g.,* in 2017, 89.5% of Canadian households owned mobile phones [11]), this is not necessarily representative of the general population.

## VIII. Discussion

In this section, we address our research questions and provide recommendations for how these findings can be applied generally to the design of digital identity services.

*RQ1: How do users perceive digital identity services?*

Participants mainly understood digital identity services to be convenient alternatives to physical documents but their interest depended on the circumstances of use (*e.g.,* being hesitant to use it with law enforcement *vs.* being comfortable using it with health institutions that already have their data). Participants also viewed digital identity services as a potentially risky technology, raising questions about data breaches, identity theft, the implications of drained mobile phone batteries, surveillance, and more.

Our participants' understanding of digital identity services was frequently misaligned with how these services actually work. In some cases, these misunderstandings led to concern over risks and threats that did not actually apply to the current technology. Like many security tools, conveying a suitable mental model that adequately represents the involved risks may be challenging. Some of the security or privacy benefits of digital identity services are particularly difficult to convey because there are no analogous tools with which users are familiar.

We saw marginally positive responses from participants with respect to using digital identity services. It is likely that many of these users would eventually adopt this type of technology once it became "mainstream". It may also be that, even if fully informed of the risks and benefits, some users will avoid transitioning to a digital identity because they prefer their physical documents.

*RQ2: What are users' expectations for digital identity services?*

Participants' main expectations included clarity around the service's data-handling practices, safeguarding users' security and privacy through principled decision-making (*e.g.,* how the service is operated and who operates it), and processes for dealing with a lost or stolen smartphone. These findings align with previous research on trustworthiness in electronic transactions [6], [31], suggesting that there is a correlation between perceived trust and an individual's willingness to use a system. Ultimately, our results affirm that implementing security mechanisms is often insufficient on its own to foster users' trust; how users *perceive* a system's security and privacy mechanisms significantly influences their adoption of this system.

It is also important to consider that participants' expectations may have been shaped by their knowledge of other technologies and by public discourse on privacy. For example, some participants wondered whether digital identity services would collect and share user data with advertisers—a practice engaged in by some existing technology companies. Others were skeptical of such services due to news reports such as Facebook's data-sharing agreements with Cambridge Analytica [8]. In addition, participants recalled other data breaches seen in the news and speculated about the possibility of their identity information being stolen.

### A. Security and Privacy of Digital Identity Services

To avoid priming, we intentionally avoided educating participants about the benefits and features of digital identity services, because in real deployment many users would not devote attention to such details even if they were made available. And although the prototype was not the focus of this paper, we believe that it is worth discussing some of its security and privacy features because many of the users' concerns would actually be alleviated. We note that these features are not unique to eID-Me, but rather we recommend that they be included in any digital identity service.

In practice, users would retain more control over their privacy than with current physical identity documents because some of eID-Me's features can help minimize how much information users need to share with recipients:

- Instead of having access to more information than necessary, as is often the case with traditional proofs of identity, relying parties only receive the identity attributes specified in their request (*e.g.,* confirmation that someone is eligible for a service, rather than seeing or collecting all of the actual PII on a health card). Additionally, relying parties can designate any of the requested attributes as optional, thus allowing users to provide only a subset of the attributes.
- Via public key cryptography, relying parties can be assured of the integrity of the information they receive from users and that it has been verified by the Registration Authority (RA). This trust also makes it possible to give less information to relying parties (*e.g.*, rather than obtaining a user's birth date, a relying party can simply be assured that a user is over 18).

Compared to analog proofs of identity, the app has security mechanisms that give greater control to users and stronger assurances to relying parties:

- Users must unlock the app with their biometrics (if enabled on their device) or a passcode prior to using their digital identity. Even then, information is only shared after the user sees and approves a notice detailing what information the relying party will receive.
- Users can configure the app to require re-authentication before certain attributes are shared.
- For in-person transactions, relying parties can request further authentication from users to confirm their identity. For example, if a cashier suspects that the user may be fraudulently using someone else's identity by having stolen an unlocked phone, the cashier can trigger a request through the POS for the user to provide additional authentication, such as their biometric, through the app before they can use their digital identity again).

Assuming that the RA is trustworthy and the infrastructure is technically secure, two main points of vulnerability remain that involve the user interface.

*Registration:* First, enabling remote registration may create opportunities for imposters to fraudulently obtain a digital identity. When identity proofing for eID-Me is not conducted in person, imposters may find it easier to circumvent the verification process when registering. This would require an

imposter to gain access to multiple physical identity documents from the victim, and pass other secondary verifications by the RA, such as being physically present at the victim's home address during the registration process. To mitigate against this threat, the system could implement mandatory in-person verification at a service centre during the one-time registration process (in essence trading usability and convenience for security).

*Authentication:* In some cases, imposters may be able to authenticate with a victim's legitimate digital identity issued by eID-Me. An imposter may succeed in authenticating with the victim's smartphone because the victim is not following best practices for securing their smartphone (*e.g.*, no biometric lock), or through coercion (*e.g.*, forcing a victim to provide their biometric in the case of online authentication).

We contend that it is difficult to convey these details to users through the user interface or even through education campaigns because the underlying mechanisms are fairly complex and in some cases un-intuitive unless someone has a technical background. Users' perceptions and mental models may remain a barrier to adoption for some users. For this reason, our following recommendations focus on communication.

### B. Recommendations

The results of this study characterize the challenges associated with possible adoption of digital identity services from the users' perspective. We believe that as digital identity services begin to incorporate more sophisticated technologies (e.g., distributed ledger technologies such as Blockchain [39], zero-knowledge proofs [16]), having strategies for mitigating these challenges is even more important to ensure that users can make informed decisions about whether they align with their privacy goals. Our recommendations align with advice from existing literature in other contexts, but we highlight their applicability because they seemed particularly relevant.

*1) Communicate information flows:* Digital identity services should emphasize their data practices. Otherwise, users could fail to discover privacy-related features and dismiss the app altogether. We found that most user concerns related to what would happen to their data in various circumstances. As mentioned by Bazarhanova and Smolander [4], the relationships between the involved parties and their respective roles was also of concern to our participants. Digital identity services should clearly indicate what is happening with personal information so that users understand what information is being collected, who can access it, and where it is being stored. While these types of statements are typically reserved for privacy policies, our participants wanted more upfront information.

*2) Set expectations up front: User onboarding* [25], [28] is a mechanism for guiding first-time users of an app through setup processes and providing them with relevant information, such as instructions on how to perform key tasks. Apps with complex workflows can rely on user onboarding to help set users' expectations. For instance, digital identity apps should explain early on what registration entails (*i.e.,* gathering all of their identity documents and then scanning them while at home or at a service centre).

In addition, user onboarding can help with introducing users to technology they are not accustomed to or informing them of the types of interactions they can anticipate. As an example, explaining the relationship between a user's digital identity and the app's QR code, or clarifying how users can review information requested by the relying party could have helped mitigate some of the issues that our study uncovered.

Ultimately, providing key information early can help users be successful in their use of the service and prevent negative outcomes that could occur from errors, such as inadvertent sharing of more personal information than intended.

Users also wanted clear communication paths when things went wrong or they had questions. We thus also highlight the importance of the surrounding support systems.

*3) Offer privacy assurances and controls:* Participants were vocal against their personal information being misused, whether through the sale of information or through government monitoring. As such, we believe it is crucial for digital identity services to be privacy-preserving, to provide control to the user over data sharing, and to actively emphasize any protections that are in place.

Many apps communicate their practices through privacy policies, but research has shown this to be ineffective as users frequently struggle to comprehend them [24]. Instead, these policies should be supplemented with *privacy notices*. Privacy notices are user-centric documents that contain "timely, relevant, actionable, and understandable information" and can support users in making informed decisions about their use of a particular service or functionality [33]. For example, prior to asking for a selfie, a digital identity app should explain how the facial data will be used.

## IX. Conclusion

In the years ahead, digital identity is expected to play an important part in society as more countries adopt it for their citizens' identity documents. Despite the impact this will have on people's day-to-day lives, little research has explored digital identity from users' perspective. Accordingly, we conducted a usability evaluation to understand users' perceptions and expectations of digital identities in Canada. After conducting our usability evaluation, we learned that designing a digital identity service to be both usable and privacy-protective requires non-trivial consideration for users' prior experiences, the context in which the identity will be used, and users' expectations for the service. Based on our findings, we highlight the need to communicate information flows to users (within the user interface or through external documentation), tell them in advance what to expect when using the app, and offer reasonable privacy controls, to help users form reasonable mental models of the system.

## Acknowledgements

We acknowledge research support for this project from Bluink Ltd, and the Canada Research Chairs and NSERC Discovery Grant programs.

## References

[1] G. Aichholzer and S. Strauß, "Electronic identity management in e-government 2.0: Exploring a system innovation exemplified by Austria," *Information Polity*, vol. 15, no. 1, 2, pp. 139–152, 2010.

[2] G. Alpár, J.-H. Hoepman, and J. Siljee, "The identity crisis. security, privacy and usability issues in identity management," *arXiv preprint arXiv:1101.0427*, 2011.

[3] Attorney-General's Department, "National identity proofing guidelines," Commonwealth of Australia, Tech. Rep., 2016, https://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf. [Accessed: 2021-04-10].

[4] A. Bazarhanova and K. Smolander, "The review of non-technical assumptions in digital identity architectures," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020, pp. 6408–6417, https://hdl.handle.net/10125/64527. [Accessed: 2021-04-10].

[5] BBC News, "Security flaw forces Estonia ID 'lockdown'," *BBC News*, 2017, http://www.bbc.com/news/technology-41858583. [Accessed: 2021-04-10].

[6] F. Belanger, J. S. Hiller, and W. J. Smith, "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 245–70, 2002.

[7] Cabinet Office, "How to prove and verify someone's identity," 2021, https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity. [Accessed: 2021-04-10].

[8] C. Cadwalladr and E. Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian*, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. [Accessed: 2021-04-10].

[9] L. J. Camp, "Digital identity," *IEEE Technology and Society Magazine*, vol. 23, no. 3, pp. 34–41, 2004.

[10] Canadian Bankers Association, "Canada's digital ID future - a federated approach," Canadian Bankers Association, Tech. Rep., 2018, https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/paper-2018-embracing-digital-id-in-canada-en.pdf. [Accessed: 2021-04-10].

[11] The Canadian Radio-television and Telecommunications Commission, "Communications Marketing Report 2019," The Canadian Radio-television and Telecommunications Commission, Tech. Rep., 2019, https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/cmr1.htm#a2.2. [Accessed: 2021-04-10].

[12] Department of Justice Canada, "Personal Information Protection and Electronic Documents Act," 2000, https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html. [Accessed: 2021-04-10].

[13] R. Dhamija and L. Dusseault, "The seven flaws of identity management: Usability and security challenges," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 24–29, 2008.

[14] Digital ID & Authentication Council of Canada, "DIACC industry insights: Digital ID in government services," Digital ID & Authentication Council of Canada, Tech. Rep., 2019, https://diacc.ca/wp-content/uploads/2019/11/Industry-Insights-Digital-ID-in-Government-Services_Nov-2019.pdf [Accessed: 2021-04-10].

[15] S. Elo and H. Kyngäs, "The qualitative content analysis process," *Journal of Advanced Nursing*, vol. 62, no. 1, pp. 107–115, 2008.

[16] U. Fiege, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, ser. STOC '87. Association for Computing Machinery, 1987, pp. 210–217.

[17] Financial Transactions and Reports Analysis Centre of Canada, "Methods to verify the identity of an individual and confirm the existence of a corporation or an entity other than a corporation," 2019, https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng. [Accessed: 2021-04-10].

[18] A. Gilbert, "Novelty fake IDs fly under forgery radar," *CBC News*, 2012, https://www.cbc.ca/news/canada/hamilton/news/novelty-fake-ids-fly-under-forgery-radar-1.1217994. [Accessed: 2021-04-10].

[19] D. Goodin, "Millions of high-security crypto keys crippled by newly discovered flaw," *Ars Technica*, 2017, https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/. [Accessed: 2021-04-10].

[20] Government of Alberta, "MyAlberta Digital ID," n.d., https://account.alberta.ca/about-us. [Accessed: 2021-04-10].

[21] Government of British Columbia, "BC Services Card," 2012, revised in 2019. https://www2.gov.bc.ca/gov/content/governments/government-id/bc-services-card. [Accessed: 2021-04-10].

[22] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines," National Institute of Standards and Technology, NIST Special Publication 800-63-3, 2017, https://doi.org/10.6028/NIST.SP.800-63-3. [Accessed: 2021-04-10].

[23] M. Hansen, A. Pfitzmann, and S. Steinbrecher, "Identity management throughout one's whole life," *Information security technical report*, vol. 13, no. 2, pp. 83–94, 2008.

[24] C. Jensen and C. Potts, "Privacy policies as decision-making tools: An evaluation of online privacy notices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '04, 2004, pp. 471–478.

[25] L. Mathis, *Designed for Use: Create Usable Interfaces for Applications and the Web*, 2nd ed. Pragmatic Bookshelf, 2016.

[26] J. McAuliff, "Overseas forgers' fake IDs can fool even the experts," *USA Today*, 2012, https://web.archive.org/web/20190712041410/http://usatoday30.usatoday.com/news/nation/story/2012-06-08/overseas-fake-ids-fool-experts/55479636/1. [Accessed: 2021-04-10].

[27] M. L. McHugh, "Interrater reliability: the kappa statistic," *Biochemia Medica*, vol. 2, no. 3, pp. 276–282, 2012.

[28] T. Neil, *Mobile Design Pattern Gallery: UI Patterns for Smartphone Apps*, 2nd ed. O'Reilly Media, 2014.

[29] M. M. Nielsen, "Tackling identity management, service delivery, and social security challenges: Technology trends and partnership models," in *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, ser. ICEGOV2019. Association for Computing Machinery, 2019, p. 1–5, https://doi.org/10.1145/3326365.3326366. [Accessed: 2021-04-10]. [Online]. Available: https://doi.org/10.1145/3326365.3326366

[30] T. Rissanen, "Electronic identity in finland: ID cards vs. bank IDs," *Identity in the Information Society*, vol. 3, no. 1, pp. 175–194, 2010.

[31] J. C. Roca, J. J. García, and J. J. de la Vega, "The importance of perceived trust, security and privacy in online trading systems," *Information Management & Computer Security*, vol. 17, no. 2, pp. 96–113, 2009.

[32] N. Sakimura, J. Bradley, M. B. Jones, B. de Medeiros, and C. Mortimore, "Final: OpenID Connect Core 1.0 incorporating errata set 1," The OpenID Foundation, Tech. Rep., 2014, https://openid.net/specs/openid-connect-core-1_0.html. [Accessed: 2021-04-10].

[33] F. Schaub, R. Balebako, and L. F. Cranor, "Designing effective privacy notices and controls," *IEEE Internet Computing*, vol. 21, no. 3, pp. 70–77, 2017.

[34] M. Scott, "Estonians embrace life in a digital world," *The New York Times*, 2014, https://www.nytimes.com/2014/10/09/business/international/estonians-embrace-life-in-a-digital-world.html. [Accessed: 2021-04-10].

[35] Service Canada, "The Social Insurance Number code of practice," Service Canada, Tech. Rep., 2013, https://www.canada.ca/en/employment-social-development/services/sin/reports/code-of-practice.html. [Accessed: 2021-04-10].

[36] C. Sullivan, *Digital Identity: An Emergent Legal Concept*. The University of Adelaide Press, 2011.

[37] The World Bank, "Principles on identification for sustainable development: toward the digital age," World Bank Group and Center for Global Development, Working paper, 2017, http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf. [Accessed: 2021-04-10].

[38] P. J. Windley, *Digital Identity*. O'Reilly Media Inc., 2005.

[39] A. J. Zwitter, O. J. Gstrein, and E. Yap, "Digital identity and the blockchain: Universal identity management and the concept of the "self-sovereign" individual," *Frontiers in Blockchain*, vol. 3, p. 26, 2020.