The Economic Impact of Digital Identity in Canada

Understanding the potential for considerable economic benefits and the cost of inaction

Digital identity is critical to the development of the Canadian digital economy. It is a key tool in making digital services safe, secure, efficient and accessible. Without it, many of the issues Canadians encounter will be magnified by the rapid increase in high-connected digital services. Trusted digital identity will enable the right people to access the right services efficiently and securely. This paper explores these issues and solutions needed to establish wide-scale trusted digital identity systems in Canada.

Table of Contents

Executive Summary

Digital identity is critical to the development of the Canadian digital economy. It is a key tool in making digital services safe, secure, efficient and accessible. Without it, many of the issues we encounter will be magnified by the rapid increase in high-connected digital services. For the Canadian digital economy to be able to reach this potential, it is vital that consumers/citizens and businesses are provided with trusted digital identities that allow them to access digital services efficiently and safely.

Governments, businesses, and citizens need to know they can trust digital information about people and organisations.

Right across the economy, identity is key to delivering services for:

- **Citizens:** According to a study conducted by password manager service Dashlane, the average person has 92 accounts registered to one email address and must reset a forgotten password for at least 37 of those accounts each year. It is expected that by 2020, the number of accounts a single person may need to manage will rise to over 200[1]. **The amount of time a citizen/customer wastes having to reset forgotten passwords exceeds 10 hours each year, and if not addressed with a better solution, could easily exceed 25-30 hours.**

  The average citizen/consumer spends approximately 8 hours per year combined either creating new, or using existing, identity sources to prove who they are, confirm certain elements of their identity and that they have the right to access a service. By improving the way in which they can carry out all these tasks, this can result in an aggregate of CAD 213 saved per person, and **CAD 6.1 billion saved** for all individuals over the age of 19[2].

- **SMEs**: For small and medium enterprises, the impact of digital identity could be used to improve processes that are difficult today. This is especially true in situations where businesses need to provide proof of identity to another business.

  Considering SMEs account for approximately 30% of Canada's overall GDP[3] (CAD 450 billion), if we assume that the average SME could be just 1% more efficient with access to trusted digital identity, this results in a potential **CAD 4.5 billion of added value to SMEs**.

- **Financial Services**: In Canada, the DIACC and its participating banks have identified potential net savings per institution at or above **CAD 100 million** per year, through operational efficiencies created by reducing manual processing costs and reducing fraud[4].

- **Digital Commerce**: The Canadian e-commerce market is expected to see sales figures increase from **CAD 21.7 billion** in 2015 to **CAD 28.34 billion** in 2018.[5] Trusted digital identity is key to enabling the continued growth of the sector. From e-commerce to the sharing economy a robust, trusted digital ID establishes trust, provides security, and mitigates fraud. A win for citizens/consumers and businesses.

- **Health**: Currently, billions of dollars per year is wasted in time and effort for healthcare professionals to access patient records, while patients and their care providers experience frustration. **A secure digital identity validation and authentication system could allow Canadians to prove their identity to access health data and consent to record sharing, greatly reducing time and costs associated with referrals,** Release of Information requests (estimated at CAD $200 per fulfillment, with thousands of fulfilments each day), accessing patient records for emergency room and ambulatory visits, and general patient administration.

- **Government**: At both the federal and provincial levels, making information accessible to citizens is a priority for modern digital government. Processes that require identity authentication and validation remain manual, lead to increased costs and slow access to services that directly impact taxpayers. Proving identity is very difficult and often requires an in-person visit of at least 30 minutes, demanding the time of the counter staff and citizen. Assuming the average citizen set up just two accounts each year, at an average wage of CAD 25.88 per hour[6], an estimated **CAD 482 million is lost each year**.

The requirements for verifiable information across industries may vary, but the fundamental need remains the same: reliable data that can be easily provided by the customer at the time it is required, with low friction but appropriate security and trust between parties.

Digital services allow existing manual processes to be simplified and streamlined. They also allow sophisticated new services to be developed that leverage the huge increases in connectivity of people, organisations and devices. These services are often prevented from reaching their full potential due to friction and lack of trust.

Today friction often exists at the point of applying for a service or accessing a service for the first time, but it can occur in many other places as well. Friction is bad for businesses and consumers/citizens alike. It prevents legitimate access to services and impacts conversion rates. The people most likely to suffer are the vulnerable and disadvantaged - including consumers/citizens on low budgets, consumers/citizens with accessibility needs and small businesses. The effects, however, are felt right across the economy.

The digital identity we have in mind is one that is secure, trustworthy and portable using digital technology. It makes responsible use of the highly connected world to bring value to individuals and businesses alike, avoiding the inefficiencies, risks, and friction associated with the systems we have today, many of which were designed pre-internet.

Now is the time for action

There is no better time to ensure consumers, businesses and government entities work together to achieve the common goal of enabling a safe, secure and trusted ecosystem for Canadian digital identity. Not only is there potential to generate more than CAD 15 billion of value to the economy, but there are also innumerable benefits to all corners of Canadian society.

We must all come together, while ensuring a distinctly Canadian approach, to safeguard our collective digital futures, ensure privacy and choice are maintained, and strive to protect the most vulnerable among us. If we do all these things, we will be well on our way to building an innovative, highly-connected, and rewarding environment for the Canadian digital economy to reach its full potential.

Given the evidence from other markets which is corroborated by what we see in Canada, we believe a conservative estimate of the potential value of trusted digital identity to the Canadian economy is at least 1% of GDP, or CAD 15 billion.

1. What role does digital identity play in the digital economy?

Digital identity is critical to the growth and efficiency of the digital economy, but most people do not understand what it is.

The lack of a unified approach to digital identity impacts every one of us. From the average Canadian citizen, to small businesses and entrepreneurs, proving who you are digitally can be time-consuming and cumbersome. Remembering which services you have signed up for and what passwords you need to access the service is difficult, meaning that most of us can't remember and have no record of all of our accounts.

For other Canadians the challenge is more serious - they do not have sufficient means to prove who they are or the task of doing so is just too difficult. This results in people being excluded from convenient digital access to vital services such as healthcare, government, and financial services. Sadly, these are often the most vulnerable people in society with the greatest need for access to such services.

> *"All of us increasingly manage our daily lives on mobile devices and online. We want to choose when, where and how we access services and don't care if the service is provided by the public or the private sector. Trusted digital identities are absolutely required to make that possible."*
> *- CJ Ritchie, Associate Deputy Minister and BC Government Chief Information Officer*

Digital services allow existing manual processes to be simplified and streamlined. They also allow sophisticated new services to be developed that leverage the huge increases in connectivity of people, organisations and devices. These services are often prevented from reaching their full potential due to friction and lack of trust. In Canada, there is a great desire by businesses and governments alike to ensure standards for digital identity do not simply follow the lead of other international success stories, but also reflect the values (inclusion, transparency, trust) that Canadians hold dear. If we can do this, while also fostering a safe and secure trusted digital identity infrastructure, we can unlock the full benefits of the digital economy.

This paper explores the current state of digital identity in Canada and how, if we act immediately, we can establish global leadership by fostering a safe, secure and trusted digital economy – for the good of society, the economy and Canada as a leader on the world stage.

So, what is digital identity?

Identity is about relationships and trust.

Every digital organisation needs to "know" its customers before being able to meaningfully interact with them online. But what does that mean? Some businesses are required to follow strict "know your customer" rules to establish the legal identity of customers. Other organisations may not be regulated in this way but still want to know as much as they can about their customers. The problem with this is

these “relationships” are often one-sided with the individual having little visibility or control over their personal data.

Today the average consumer/citizen has a relationship with dozens of digital organisations, each one of them established and managed in isolation. Often consumers/citizens are required to create an account with an online organisation regardless of whether that is what the client wants (i.e. why should a client need to create an account for a one-off purchase?). This is inconvenient, inefficient, and insecure. In effect, every client has numerous “digital identities” represented by the personal data each organisation holds about them and is virtually impossible for an individual to manage.

So, while citizens have many digital relationships, often these are not trusted and/or are difficult to manage.

Identity is about personal data.

Many consumers/citizens do not understand the amount of personal data that they generate when using digital services, nor how that data can be exploited in a variety of ways – good and bad, legal and illegal. Most consumers/citizens do not appreciate the value of their personal data and are implicitly accepting a value exchange (sharing data for access to “free” services) without thinking whether that exchange is fair or not.

The costs and risks to businesses of holding personal data are becoming increasingly evident with each high-profile data breach that occurs. As well as the reputational damage and the risk of litigation, European authorities are introducing punitive fines for data protection failings, which inevitably will influence the direction of data protection legislation in other jurisdictions.
A key concern for policymakers must be the current lack of individual control over personal data.

The digital identity we have in mind is one that is secure, trustworthy and portable using digital technology. It makes responsible use of the highly connected world to bring value to individuals and businesses alike, avoiding the inefficiencies, risks, and friction associated with the systems we have today, many of which were designed pre-internet.

2. Who needs digital identity?

Both governments and businesses need to know that they can trust digital information about people and businesses

The entire economy is impacted.

The requirement for verifiable identity data is necessary for many industries. Right across the economy, identity is key to delivering services and is especially evident in the following areas:

- **Financial Services**: The need for digital identity today is seen most immediately in regulated services, such as financial services. Financial services are required to perform rigorous “know your customer” checks on customers at account opening and periodically. These checks are an important part of helping to prevent money laundering and funding of terrorism, but they are also time-consuming, costly and often duplicative. In Canada, the DIACC and its participating banks have identified potential net savings per institution at or above CAD 100 million per year, through operational efficiencies created by reducing manual processing costs and reducing fraud[7].

- **Digital Commerce**: Trusted digital identity is also needed for a wide variety of digital commerce scenarios where payment is required between two parties. This is especially true when there is no previous relationship between parties, and there needs to be some ability to reduce the risk of fraudsters posing as a "real person" online. This could be between a consumer and a business, from one business to another business, or between two consumers. Payments in a digital environment require a significant amount of trust since you cannot “see” the person on the other end of the transaction and there is often no straightforward way to digitally verify an authentic person or organisation.

- **Health**: Currently, billions of dollars per year is wasted in time and effort for healthcare professionals to access patient records, while patients and their care providers experience frustration. Electronic health records are spread out across multiple proprietary systems that often do not connect with each other. Verifying proper access to data and only sharing necessary information with the intended recipient upon explicit consent from the patient is critical to protecting the sensitive information required during medical treatment. These inefficiencies can lead to duplication of laboratory and diagnostic tests, wasted time waiting for the physical transfer of patient medical records between healthcare providers, and inefficient use of emergency department resources[8]. A secure digital identity validation and authentication system could allow Canadians to prove their identity to access health data and consent to record sharing, greatly reducing time and costs associated with referrals, Release of Information requests (estimated at CAD $200 per fulfillment, with thousands of fulfilments each day), accessing patient records for emergency room and ambulatory visits and general patient administration.

- **Government**: At a federal and provincial level, making information accessible to citizens is a priority for modern digital government. Processes that require identity authentication and validation remain manual, lead to increased costs and slow access to services that directly impact taxpayers. Proving identity is very difficult and often requires an in-person visit of at least 30 minutes, demanding the time of the counter staff and citizen. Assuming the average citizen set up just two accounts each year, at an average wage of CAD 25.88 per hour[9], an estimated CAD 482 million is lost each year. There are also challenges for small businesses

that need to interact with local, provincial and federal government departments. Depending on the industry, there are varying requirements for businesses including business registration, licensing, permitting, and inspections that are all primarily manual processes today.

Beyond these key areas, digital identity is already utilised and will become increasingly important in industries such as retail for address or age verification, employment for background checks or employment verification, education for degree validation, and insurance for fraud prevention.

The requirements for verifiable information across industries may vary, but the fundamental need remains the same: reliable data that can be easily provided by the customer at the time it is required, with low friction but appropriate security and trust between parties.

3. How is digital identity done today?

Today identity is often done badly.

Basic problems

Almost every online service today incorporates some element of personal identity. Often the approaches taken, however, suffer from reliability, security, and usability issues.

At the most the basic level, a cookie placed on a browser allows a website to store a unique reference for the individual along with personal information. This allows the website to detect and track the user across multiple website interactions. Often, the individual is unaware of the data that is being stored and how it is being used.

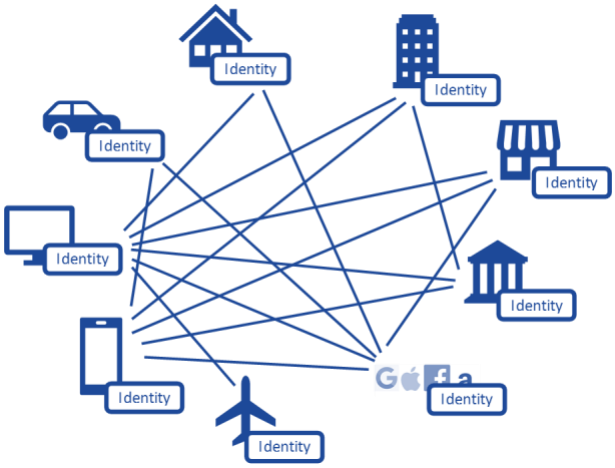


Figure 1: Digital identity today – siloed and fragmented

Many digital services require the creation of an "identity" specific to the service. This results in customers needing to manage multiple accounts, which is time-consuming and costly for businesses too. According to a study conducted by password manager service Dashlane, the average person has 92 accounts registered to one email address and must reset a forgotten password for at least 37 accounts each year. It is expected that by 2020, the number of accounts a single person may need to manage will rise to over 200[10]. The amount of time a citizen/customer wastes having to reset forgotten passwords exceeds 10 hours each year, and if not addressed with a better solution, could easily exceed 25-30 hours.

From a business employee perspective, this problem is even more exaggerated when it comes to internal applications and business tools. Another password manager service called LastPass studied password management in the workplace. They found that on average, an employee must type out credentials to authenticate to their websites and apps **154 times a month**. One thing is clear: Typing passwords is (still) a part of the daily grind. If the average employee is storing **191 logins in their vault**, it seems that not all passwords are used all the time. The data also shows that it takes **an average of 14 seconds to type a password**. That's an **average of about 36 minutes a month wasted** on an activity with no value-add to the business[11].

By extrapolating this data across the entire Canadian workforce, we can see that this simple task alone costs nearly CAD 300 million per month and more than CAD 3.5 billion per year.[12] Beyond the act of typing in passwords, the average administrative cost at call centres to manage and administer lost, forgotten, or stolen passwords is estimated to be CAD 40 per incident[13]. Assuming one incident per year per working Canadian, across 18.65 million working Canadians, CAD 746 million is lost annually to just password management services and lost productive hours. These two examples alone result in potential savings of more than CAD 4 billion per year.

Wasteful duplication

In addition to wasting user time on activities like forgotten passwords, there is a huge duplication of efforts on the part of businesses to verify identity data about consumers/citizens. One obvious example of this is the onboarding and Know Your Customer (KYC) procedures used by financial institutions during account opening. With ongoing maintenance of this information throughout the life of the customer's account. In a study conducted by Thompson Reuters, they found that the costs and complexity of KYC are rising, and while financial firms' average costs to meet their obligations are USD 60 million, some are spending up to USD 500 million on compliance with KYC and Customer Due Diligence (CDD).[14] Since KYC is often comprised of similar processes between institutions, this cost could be streamlined with an appropriate digital solution, and at the same time reduce the risk of identity theft.

CASE STUDY 1 – OPENING A RESTAURANT

Emma is a 42-year-old restaurant owner who has run a small chain of successful restaurants in Fredericton, New Brunswick for the last five years. Her businesses have generated enough excess income that she has decided to open two new locations to expand her operations to other cities.

Without digital identity:
Emma researches what licenses, permits and business registration documents she needs to obtain to open the new locations. The complicated process feels daunting to her, and she puts off getting together all the paperwork she needs to file in order to open the new locations.

With digital identity:
Emma connects to her secure digital government portal with Service New Brunswick (SNB). She already manages her existing business permits and licenses here so has familiarity and comfort with the process. She can easily start the process of registering her new businesses online, being guided through the process to validate information about the proposed locations, relevant permits and licenses for her restaurant type, and any other requirements she must meet. Since SNB can verify that Emma is a real person who is an existing business owner, there are fewer hurdles to trusting her business application is legitimate. After she completes her applications and is waiting for approval, Emma receives an invitation to view a restaurant equipment supplier bidding system where she can specify what kitchen equipment she needs for the new locations. She submits a request for quote and receives responses within a few hours from 10 vendors recognised as legitimate businesses operating in New Brunswick. The next day after reviewing the vendor quotes, she decides on her preferred choice, submits her order, and schedules the deliveries.

Beyond financial services and KYC, the concept of a customer's identity data being duplicated across many digital services is commonly accepted in today's digital economy. When an individual or a business wants to create a new online account or share parts of their data between providers, much of their identity data is often required to establish a new account, despite the fact this same data exists in many other places. Even when data is shared between businesses, this is not often done in a way that respects the customer's privacy. This duplication also poses a problem if any of the customer's

information changes (legal name due to marriage, address change when moving, phone number changes, etc.) and needs to be updated at each of these established online accounts.

The customer is the product

The business model of free internet services relies on establishing a "profile" of the user, which is a form of identity. That profile is compiled from all data that can be collected about the user including data explicitly entered as well as all contextual and usage data that can be aggregated. This is used to target the user with advertisements, which are in turn the source of revenue to those companies.

There are many reasons why this approach is not desirable from an identity standpoint, including concerns about data privacy and control of personal information (geolocation data, personally identifiable information, etc.). This model leaves the customer with little control over their own data once it enters the ecosystem. Beyond privacy, security and control, there is also the concern with the fact that data provided by a user may or may not be completely accurate. Social networks inherently encourage people to share primarily positive information, or even slightly skewed information. This again leads to issues with data quality and the ability to trust the data being validated. Businesses often prefer to trust data that can be verified with a high level of certainty and can be validated by an independent source to reduce the level of risk in conducting any number of transactions.

While people are generally willing to share personal information in exchange for valued services, surveys indicate growing unease in how personal data are being used. A study by the telecommunications operator Orange showed that 78% of consumers/citizens find it hard to trust companies in the way they use such data[15].

4. How do today's processes impact the digital economy?

Shortcomings in digital identity today result in unacceptable risks to individuals and businesses and hamper the growth of the digital economy.

Data breaches

Where personal data is being collected, stored, or processed, security incidents can heavily affect privacy. They also generate significant costs to firms as well as to users. According to data by the Privacy Rights Clearinghouse[16], the number of incidents identified oscillates around 45 incidents per year, while the total number of records stolen is increasingly determined by large-scale data breaches, i.e. data breaches involving more than 10 million records. Since 2005, more than 6,000 companies and organisations have reported breaches. In just 2015, for example, nearly 165 million records containing [US] Social Security numbers were compromised in 338 breaches, according to the Identity Theft Resource Center.[17]

The Home Depot data breach of 2014 (56 million credit and debit cards), cost the company USD 263 million in mitigation expenses, or roughly USD 4.70 per record lost. The 2013 data breach of Target (40 million credit and debit cards and 70 million non-card customer records) cost the company USD 291 million in mitigation expenses, or roughly USD 2.65 per record[18].

These examples, among many others over the last decade, have eroded consumer confidence in the digital economy. This has caused many consumers/citizens to be hesitant about sharing any information online, let alone sensitive identity data they perceive could be lost, stolen or shared in an unauthorised way without their consent.

Account takeover

As a result of these high-profile data breaches, a new set of problems has begun to take shape beyond simply fraudulent credit card purchases. Especially in cases where more personally identifiable information was stolen, cybercriminals have spent more time attempting identity theft and account takeover fraud. Unlike credit card account data which can be easily changed by the issuing bank if stolen, identity data such as one's home address or social insurance number cannot be so easily changed.

While the security industry is focused on preventing breaches, criminals are focused on extracting value from the stolen data. Like a business building a profile of a customer, criminals are trying to create a complete digital dossier on potential victims. For high net-worth individuals, such profiles can fetch a premium, going for more than USD 450 on the dark web[19]. With this data, the cyber-criminal can potentially open new financial accounts or access funds in existing financial accounts by impersonating the customer.

Evolving fraud risks

Fraud is no longer as simple as catching criminals using stolen physical credit cards. Data breaches have caused thousands, if not millions, of stolen financial accounts and personal identity data to be available to criminals on the dark web. As a result, fraud now takes many shapes and forms. Call centre fraud has become a higher profile issue after Apple Pay was released in September 2014. There was an immediate uptick in call centre fraud, as cybercriminals realised they could set up accounts using stolen credit card data.

In 2015, one in every 2,900 calls coming into large banks' call centres was fraudulent, according to Pindrop Security[20]. In 2016, the number was closer to one in every 2,000 calls. Among regional banks, it's more like one in 700. Criminals use account takeover techniques to socially engineer call centre agents to take control of customer accounts, set up new lines of credit, and transfer money.

Another type of fraud being encountered on a regular basis is synthetic identity fraud. This kind of fraud differs from traditional identity theft in that the perpetrator creates new synthetic identities rather than stealing existing ones. The process starts with someone stealing real social security numbers that aren't actively being used — think children and elderly people who use little, if any, credit — and then creating identities by adding fake addresses. Playing a long con that can take years to pay off, these thieves slowly build a credit rating for these new identities, interacting with banks using temporary prepaid phones that are disposed of at some point. They eventually rack up debts of USD 20,000 or more on countless accounts only to disappear without a trace[21].

5. What will the wider benefit to the economy be?

The economic benefits will be huge.

We firmly believe the collective benefits of implementing digital identity standards and identity systems that can provide verified information will have many qualitative and quantitative benefits to the

Canadian economy. While it can be difficult to predict exactly how much value will be generated and savings realised, the following perspectives show the potential economic impact.

Quantifying the potential economic benefit to Canada

The potential economic benefits to the Canadian economy could be realised through a variety of domino effects of properly implemented digital identity solutions, such as introducing efficiencies where identity assurance today is difficult and costly, reducing identity-related fraud, and opening new avenues of value for both individuals and businesses.

To quantify the potential benefit, we consider the cost of identity assurance today for the 36.7 million citizens, 28.8 MM of which are age 19 and over[22], and the 1.17 million employer businesses[23] (not including "self-employed" businesses).

Individuals
For individuals, we know that there are many day-to-day tasks that are simply more difficult than they could be if the proper digital tools were in place. In today's inefficient environment, we can assume the average citizen/consumer spends approximately 8 hours per year combined either creating new, or using existing, identity sources to prove who they are, confirm certain elements of their identity and that they have the right to access a service. By improving the way in which they can carry out all these tasks, this can result in an aggregate of CAD 213 saved per person, and CAD 6.1 billion saved for all individuals over the age of 19[24].

Businesses
For small and medium enterprises, the impact of digital identity could be used to improve processes that are difficult today. This is especially true in situations where businesses need to provide proof of identity to another business, such as in attempting to get access to financial products or services to grow their business, attempting to locate and buy goods from suppliers, conducting transactions remotely from distant geographic locations, and validating beneficial ownership of the enterprise.

Considering SMEs account for approximately 30% of Canada's overall GDP[25] (CAD 450 billion), if we assume that the average SME could be just 1% more efficient with access to trusted digital identity, this results in a potential CAD 4.5 billion of added value to SMEs.

Actual economic benefit realised in Estonia and India

There are some countries across the globe where at least some form of an efficient and effective digital identity is a reality and has shown significant economic benefit. Secure, authenticated identity is the "birthright" of every Estonian: before a newborn even arrives home, the hospital will have issued a digital birth certificate, and health insurance will have been started automatically. All residents of the small Baltic state aged 15 or over have electronic ID cards, which are used in healthcare, electronic banking, online shopping, signing digital contracts, encrypting e-mail, tram tickets, and much more. In all, the Estonian state offers 600 e-services to its citizens and 2,400 to businesses[26]. In addition to making it easier for Estonians to go about their daily lives, Estonia claims its online systems add 2% per year to its GDP[27] and the use of electronic signatures in the country helps save 2% of Estonian GDP per year, the size of the Estonian defence budget[28].

In recent years, India has made remarkable progress with its successful Aadhaar program in registering its people and issuing them with a digital identity, with many of these Indians previously not having official identification documents. Aadhaar is operated by the Unique Identification Authority of India (UIDAI). The program is ongoing; registration is continuing, and efforts are being made to 'seed' Aadhaar numbers into the databases of various social benefit schemes[29], income tax records, public sector HR systems, company registrations, etc. More than 1 billion Indians have been registered[30], a remarkable achievement by any measure.

The World Bank estimates the Aadhaar initiative **to be saving the Indian government about USD 1 billion annually by thwarting corruption**, as well as underlining that digital technologies promote inclusion, efficiency and innovation.

Potential economic benefit identified in Australia and the UK

In addition to benefits already realised by digital identity systems that are currently in place, numerous countries have conducted studies to determine the potential value that could be introduced to their economies with digital identity solutions. In joint research conducted by Australia Post and Boston Consulting Group, "[T]he potential value of a digital identity solution for Australia [was identified as] **up to AUD 11 billion that could be saved through reduced cost to serve, cost of fraud and improved client experience**[31]." This AUD 11 billion represents approximately 1% of the Australian GDP.

A joint study between the Open Identity Exchange (OIX) and Ctrl-Shift on the size and potential of the UK market for identity assurance also showed significant potential value. The report suggests that over the next decade the total **identity assurance costs for organisations could fall from today's £1.65 billion [CAD 2.86 billion] to less than £150 million [CAD 260 million]** as new digital processes based on the principles of 'make once, use many times' bed down. This will encourage a further shift of transactions online[32]. There is not one single over-arching 'business case' for the provision of, or purchase of, identity assurance services. Each party's

CASE STUDY 2 - ACCESSIBILITY

Thomas is a 23-year-old recent college graduate who has a mobility impairment that prevents him from being able to sign paper documents. He would like to rent his first apartment out of college and has identified his top three choices.

Without digital identity:
Thomas contacts the property managers at each apartment to set up an appointment to view each one. After seeing all three, he decides on his preferred choice and calls a friend to help him fill out the rental contract and background check paperwork the next day. After he sends in the paperwork, he gets a call from the landlord that someone else has already put in the paperwork and signed a contract to rent the apartment. Thomas must settle for his second-choice apartment in a different neighbourhood and because of the delay in finding out the first choice was not available, now he can't move in for another two weeks. He also must mail a cheque to the landlord who does not have an option for electronic transfers or automatic monthly debits.

With digital identity:
Thomas contacts the property managers at each apartment to set up an appointment to view each one. After seeing all three, he decides on his preferred choice and uses his mobile phone to open a link the property manager sent him to fill out the rental contract and background check process online. Thomas can automatically populate all his personal information for the application using his trusted digital identity and apply within hours of seeing the last apartment. He hears back from the property manager the next morning that his application has been approved and he can start moving in within a week. Since he also has his bank account connected through his digital identity, his payment for a security deposit and the first month's rent will be sent to the property manager the day before he moves in, and his monthly rent will be withdrawn from the same account automatically each month

cost structures and incentives are different, creating millions of different ‘mini business cases'. Overall, however, the market for verified attributes and the services they enable will be central and critical to the 21st-century personal information economy.[33]

Making Canada a digital leader

By embracing digital identity and working together across businesses and government, Canada can likewise become a digital leader that can foster an environment for startups, small businesses, and innovation. With more efficient systems for establishing and operating a business, getting better access to financial services, and making verifiable information more easily accessible, Canada can enable businesses to grow in ways that were not possible before.

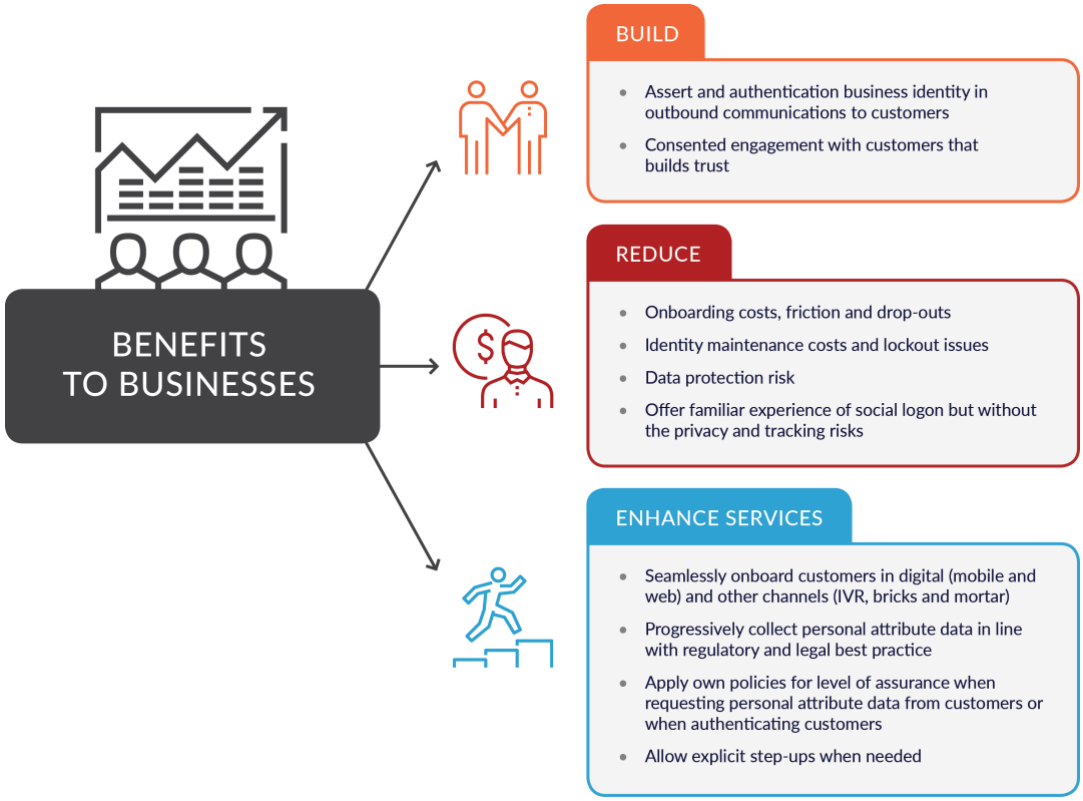
In addition to encouraging business growth within the country, Canada could also take a leading international role similar to what Estonia has done to promote their own digital identity solution. Not only do they have efficient digital processes for those that live in the country, but they have also enabled outside investment in Estonia. This has been accomplished by allowing a fully digital remote business opening process (subject to a background check) and by exporting identity capabilities to similar countries (e.g. Azerbaijan)[34].

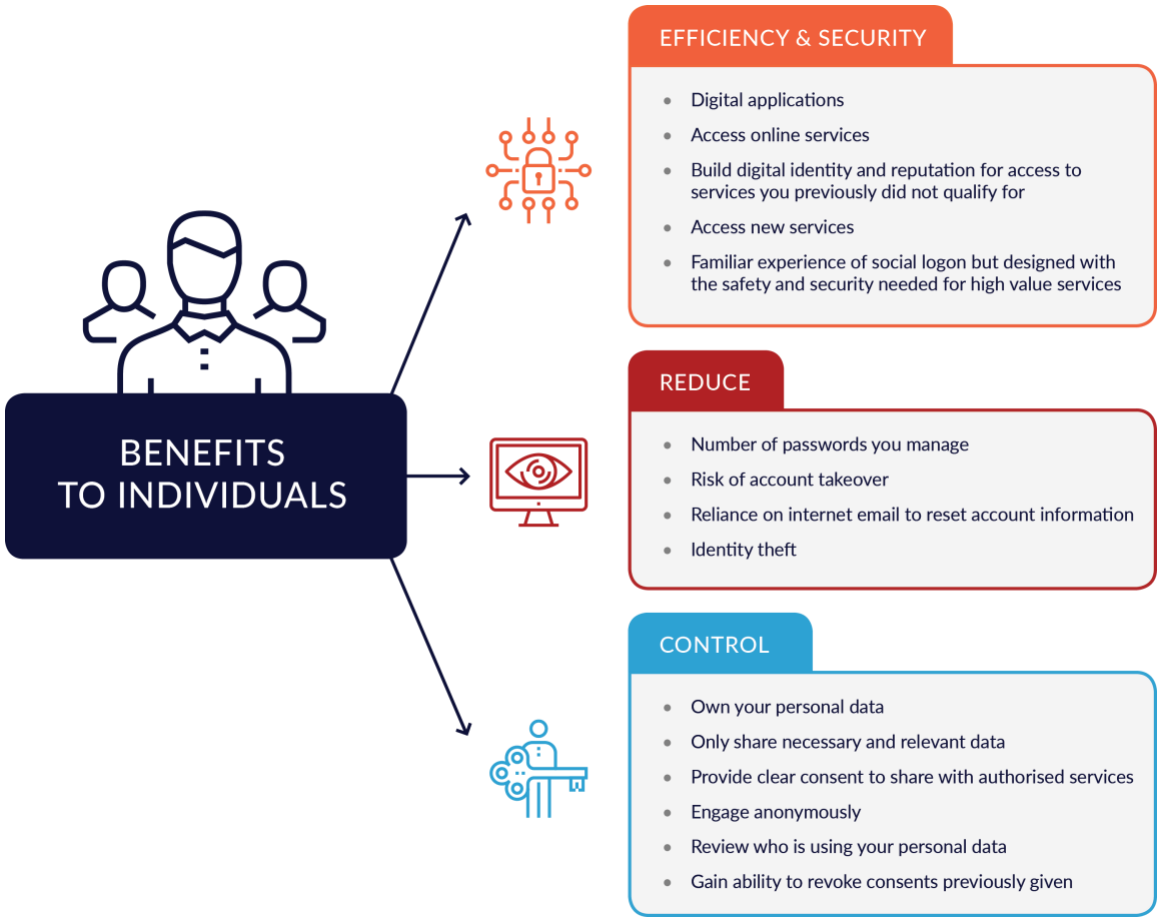
Given the evidence from other markets which is corroborated by what we see in Canada, we believe a conservative estimate of the potential value of trusted digital identity to the Canadian economy is at least 1% of GDP, or CAD 15 billion.

6. How will this benefit individuals and businesses?

The benefits to individuals and businesses are real.

Both individuals and businesses stand to benefit from trusted digital identity. We have discussed the failings of identity today, the risks if we continue down a path of disjointed identity processes, and the potential quantitative benefits to the economy. Below we outline some specific and tangible benefits envisioned to improve day to day life for all Canadians.





7. What is the role of the citizen/consumer?

Fixing the shortcomings of today's digital identity requires the citizen/consumer to be put at the centre

Ownership of data
It is no longer good enough for organisations to think of customer data as "their data". This mindset has led to organisations storing massive amounts of data that, as we've seen with the large data breaches and account takeover attempts, does not often end well for customers. By placing consumers/citizens, and their identity, at the centre of the ecosystem, this can free up organisations to focus on their core business, rather than spending time building their own identity infrastructure or gathering data about the consumer/citizen that already exists elsewhere.

This common problem in today's digital environment can be mitigated using something like a verifiable claim, where instead of the actual identity data being passed among multiple parties, the consumer/citizen can be provided with a tool that allows them to independently verify the data requested (via a known and trusted third party). For example, if a citizen's age is required to

determine their eligibility to access a service, the citizen can use a digital identity service to prove via an existing third-party relationship whether the age requirement is met.

Connecting the dots

In the massively connected digital world, it is the citizen/consumer who is best placed to join together the various parts of their life, including the various parts of their digital life. By providing citizens/consumers with the tools to manage their data and relationships, they can become the control point leading to an approach that is not only more efficient but also provides much better privacy. If we think about this in comparison to the way we use identity in the physical world today (i.e. showing a driver's license or passport to gain access to a service), the identity data provided is not retained, it is simply used for the purpose needed at that moment. This same principle can be applied to digital solutions as well and is increasingly seen as a way to minimize the amount of personal data that gets proliferated across disparate organisations' systems.

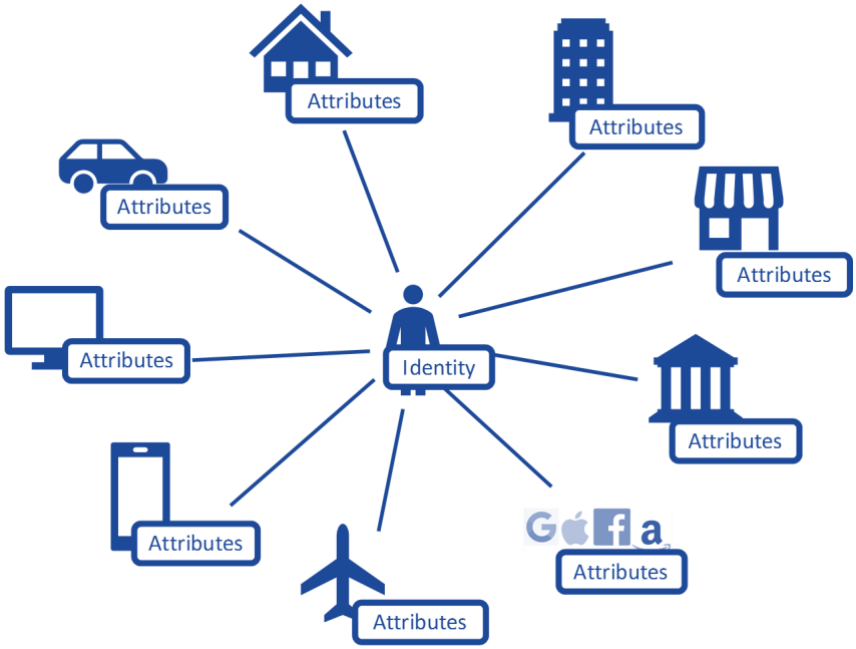


Figure 2: Trusted digital identity – putting the customer at the centre

Empowerment builds trust

Empowering the citizen/ consumer will engender higher levels of trust in online services. When citizens/ consumers have transparency and control over their digital lives, they will be more willing to share identity data to enable digital services. By using techniques to minimise the amount of data, ensure data is only collected with a clear purpose, and with the consent of the user, digital businesses and government organisations can show through their actions that there is specific intent to keep customer data safe, secure and private.

8. What is the role of government and business?

Fixing the shortcomings of today's digital identity also requires governments, businesses, and industry to work together.

Collaboration is fundamental to success.

No one organisation can solve this – all parts of the digital economy rely on digital identity resulting in many potential stakeholders and differing needs. At the same time, the urgent need to put customers in control of their digital identities means that it is no longer good enough for each stakeholder to go in their own direction. Organisations of all types from both the public and private sector need to collaborate in the establishment of standards and in the creation of ecosystems.

The identity of both individuals and businesses is needed in just about every industry in some form. This pervasiveness means that any solutions inevitably will have a major impact across the entire economy.

CASE STUDY 3 – FINANCIAL SERVICES

James is a 45-year-old sales director and father of two teenagers. Suddenly, his refrigerator has stopped working and even once he has a repair technician look at it, determines it needs to be replaced. James is about to leave for a business trip, so he is short on time and needs to get a replacement quickly while he is gone.

Without digital identity:
On the way to the airport, James calls his local appliance dealer to see if he can get the exact same model refrigerator. The associate he's speaking to isn't sure if they have one in stock, so promises to call James back soon. Meanwhile, James must board his flight and while in the air, the associate leaves a voicemail saying they don't have the same one, but there are other models just like it that should be the same dimensions. James decides it's too much hassle and waits until he gets back home to go into the appliance dealer himself and look at the options.

With digital identity:
On the way to the airport, James logs in to his local appliance dealer's website to see if he can get the exact same model refrigerator. The dealer has his previous purchase information available and determines they no longer make the same model refrigerator. Instead, James is presented with three options that are the same dimensions, and he can review the details of each one including photos. After confirming the option he likes best, the dealer asks for his consent to review if there are options to finance his purchase. He agrees, and a seamless process occurs to find the best available deal based on his financial history (which is kept private from the dealer but is used to find a potential match with a financial institution). James picks the best pricing option to spread out his payments, the dealer gets paid instantly, and the refrigerator is delivered to his house before he returns from his business trip.

Why digital identity initiatives have failed in the past

Digital identity initiatives in the past have often struggled to gain scale and critical mass. Often the value of identity (and personal data) is not fully appreciated by consumers/citizens. Businesses tend to focus on the competitive advantage of "owning" the customer identity, failing to see the larger economic benefit of collaborating. There are often questions of liability which prevent potential providers of digital identity from taking the plunge. In combination, these issues make it difficult to produce a proposition that is compelling to both the provider and user of digital identity.

But these issues are not insurmountable. The BankID initiatives in the Nordic countries show that digital identity can be made to work. In those countries, banks collaborated to provide digital identity systems for the banks which have since been leveraged by the government, as a means to provide access to numerous online banking and digital government services. Customers can use their BankID to present their identity information digitally or securely sign digital documents to lease a car, rent an apartment, enrol for college, apply for a student loan, get a driver license or check health records. All these things can now be done more simply and without the need for manual processes that often took many days or weeks in the past.

Role of the DIACC

The DIACC is a neutral industry-led consortium of public and private sector leaders committed to developing a Canadian digital identification and authentication framework to enable Canada's full and secure participation in the global digital economy. DIACC members include representatives from both the federal and provincial levels of government as well as private sector leaders.

The DIACC's objective is to unlock societal and economic opportunities for Canadians by providing the framework to develop a robust, secure, scalable and privacy-enhancing digital identification and authentication ecosystem that will decrease costs for governments, consumers/citizens, and business while improving service delivery and driving GDP growth. By cultivating user-centric identity solutions, and ensuring the adoption of these tools by leading organisations, we will enhance user security and privacy; incorporate digital identity proofing and authentication processes established by DIACC and the National Institute of Standards and Technology (NIST);[35] lower costs and risks for Canadian businesses and governments to operate digitally, and supercharge Canadian innovation, creating thousands of jobs.

9. What is the cost of inaction?

Canada cannot afford not to do this.

If we do not focus on making digital identity a priority for Canada, there will be many missed opportunities including the loss of potential growth in the digital economy, the risk of falling behind other developed nations treating this as a higher priority, and the risk of internet giants such as Google, Facebook, and Amazon taking on even larger roles in citizen/consumer's lives.

Other countries that already have identity solutions in place have begun looking for ways to expand beyond their borders by taking a leading role in promoting digital identity and using their own experiences as a role model for new initiatives. In some cases, this could generate revenue by letting other countries leverage existing solutions, platforms or infrastructure.

While the largest internet companies are already well positioned to take a leading role in digital identity across the world, these services are still not as reliable from a risk perspective (due to the low

assurance of the data). At the same time, we have likely not yet seen the scope of what they can achieve and if, given the opportunity, they will continue to try to consolidate control over their customers to both strengthen and deepen their relationship with consumers/citizens.

Benefits of growing Canada's digital economy

Beyond the quantifiable benefits, there are other qualitative benefits to the growth of the Canadian digital economy because of better digital identity. Better and easier access to verifiable identity services can potentially open new opportunities for those that are currently excluded, such as the unemployed, immigrants, elderly and vulnerable. These groups of people all tend to have a more challenging time either validating their identity or participating in the economy in the same way that others might. By opening new avenues for more efficient, streamlined and secure identity validation, this creates an opportunity to bring them into the economy, allow easier access to employment, government services, benefits, and many other services.

In addition to better access for the underserved, there is also the potential for widespread gains in productivity for broad segments of both individuals and businesses. According to a report from OECD, "the recent digital transformation of economic activities has unleashed four main innovative trends: 1) improved real-time measurement of business activities; 2) faster and cheaper business experimentation; 3) more widespread and easier sharing of ideas; and 4) the ability to replicate innovations with greater speed and fidelity (scaling-up).[36]"

There are also societal benefits to safety and law enforcement that should be considered. Even if it is not conducted "online", face to face identity verification can also be carried out digitally. If an identity solution is designed in a way to prevent undesirable surveillance, this can provide an opportunity to offer something that provides a public service by being more accurate, producing fewer instances of mistaken identity or wrongful accusations, and potentially providing public safety officials with tools to conduct their business more efficiently.

10. Where should we start?

DIACC and the Pan-Canadian Trust Framework

DIACC has engaged in a collaborative approach to developing a Pan-Canadian Trust Framework[37] that will establish guidelines for both private and public sector digital identity service providers. Canada's full participation in the digital transformation and global digital economy depends on developing reliable, secure, scalable, privacy-enhancing, and convenient solutions for digital identity. Made-for-Canada solutions reflect and incorporate Canadian principles, business interests, technical models and, demonstrate compliance with Canadian regulations. The PCTF supports the establishment of an innovative, secure, and privacy-respecting Canadian digital identity ecosystem.

While there has been great progress made, this initiative needs to be accelerated to provide Canadian businesses and consumers/citizens with a baseline expectation of how digital identity initiatives can be successful in Canada.

Prioritising digital identity

Digital identity needs to be high on the agenda of policymakers, politicians and business leaders alike. For the benefits to be realised and the impact to the economy to take full effect, digital identity policy at the government level, as well as the development of digital identity solutions by businesses, needs to be a high priority for everyone involved.

Now is the time for action

There is no better time than now to ensure consumers, businesses and government entities will work together to achieve the common goal of enabling a safe, secure and trusted ecosystem for Canadian digital identity.

Not only is there the potential to generate more than CAD 15 billion of value to the economy, but there are also innumerable benefits to all corners of Canadian society. From a fishing boat captain in British Columbia, to a restaurant worker in Toronto, to a teacher in New Brunswick, everyone stands to benefit from getting this right for Canada.

We must all come together, while ensuring a distinctly Canadian approach, to safeguard our collective digital futures, ensure privacy and choice are maintained, and strive to protect the most vulnerable among us. If we do all these things, we will be well on our way to building an innovative, highly-connected, and rewarding environment for the Canadian digital economy to reach its full potential.

References

[1] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
[2] 8 hours per year x CAD $26.68 average hourly wage = CAD $266.80 per person per year x 28.8M working Canadians = CAD $6.1B, (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/dsbbcan-eng.htm, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-eng.htm)
[3] https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03018.html#toc-09
[4] CAD 225 per user (https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/
18M workers- Statscan: http://www.statcan.gc.ca/pub/91-550-x/2008001/part-partie1-eng.htm
600 Hours - ID Alerts: http://www.idalerts.ca/identity-theft-statistics/
5.68M - Canadian Underwriter: http://www.canadianunderwriter.ca/insurance/canada-second-expensive-country-data-breaches-ibm-ponemon-institute-study-1004115487/
[5] https://www.statista.com/statistics/289741/canada-retail-e-commerce-sales/
[6] Statistics Canada : (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-eng.htm)
[7] CAD 225 per user (https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/
18M workers- Statscan: http://www.statcan.gc.ca/pub/91-550-x/2008001/part-partie1-eng.htm
600 Hours - ID Alerts: http://www.idalerts.ca/identity-theft-statistics/
5.68M - Canadian Underwriter: http://www.canadianunderwriter.ca/insurance/canada-second-expensive-country-data-breaches-ibm-ponemon-institute-study-1004115487/
[8] Canada Health Infoway, Connected Health Information in Canada: A Benefits Evaluation Study, https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/benefits-evaluation/3510-connected-health-information-in-canada-a-benefits-evaluation-study
[9] Statistics Canada : (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-eng.htm)
[10] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
[11] https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html/
[12] 36 minutes per month x 18.65 million working Canadians x CAD 26.68 average hourly wage, (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/dsbbcan-eng.htm, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-eng.htm)
[13] https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/
[14] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html
[15] http://reports.weforum.org/rethinking-personal-data/
[16] http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en
[17] https://www.pcworld.com/article/3075539/security/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html
[18] http://www.digitaltransactions.net/news/story/Expenses-From-the-Home-Depot-and-Target-Data-Breaches-Surpass-_500-Million
[19] https://www.pcworld.com/article/3075539/security/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html
[20] https://www.pindrop.com/resources/download/report/2017-call-center-fraud-report
[21] https://www.forbes.com/sites/alanmcintyre/2018/02/07/the-battle-against-synthetic-identity-fraud-is-just-beginning/#5b0238664ca0
[22] Statistics Canada CANSIM Table 051-0001
[23] https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03018.html
[24] 8 hours per year x CAD 26.68 average hourly wage = CAD 266.80 per person per year x 28.8M working Canadians = CAD 6.1B, (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/dsbbcan-eng.htm, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-eng.htm)
[25] https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03018.html#toc-09
[26] https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge
[27] http://fortune.com/2017/04/27/estonia-digital-life-tech-startups/
[28] https://www.gemalto.com/govt/customer-cases/estonia-eid
[29] http://economictimes.indiatimes.com/news/economy/policy/indias-first-national-social-security-platform-to-be-developed-by-deity/articleshow/52301300.cms?from=mdr
[30] http://www.business-standard.com/article/current-affairs/aadhaar-crosses-1-billion-mark-says-prasad-116040401147_1.html
[31] https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf
[32] https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/ (p. 4)
[33] https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/ (p. 5)

[34] https://cyber.ee/en/referentsid-ja-kogemused/referents/national-electronic-id-solution-for-the-government-of-the-republic-of-azerbaijan/
[35] https://pages.nist.gov/800-63-3/sp800-63-3.html
[36] OECD (2017) – Going Digital: Making the Transformation Work for Growth and Well-Being https://www.oecd.org/mcm/documents/C-MIN-2017-4%20EN.pdf
[37] https://diacc.ca/2016/08/11/pctf-overview/