SEP 707: Communications Technology and Public Policy

How Can a Person's Digital Identity be Managed and Protected?

An inquiry into the social, ethical and political implications of digital Identity

Submitted by: Peter Topalovic
Submitted to: Vino Vinodrai
Gail Krantzberg

Course: SEP 707
Date: December 14, 2007
Revision: Final Submission

Table of Contents

1. Introduction

The invention of the transistor by Bell Laboratories in 1947 paved the way for the development of the integrated circuit and eventually the microprocessor. This tiny chip of transistor circuits has found its way into many electronic devices that we use on a daily basis, including the personal computer (PC) developed in the late 1970s. By the 1990s, the microprocessor was integrated into many aspects of everyday life. It was during this era that the processing power of the PC began to compete with mainframe systems used in banks, businesses and public institutions. At the same time, the Internet, once the domain of public institutions, became a part of the public domain and gave birth to the digital revolution [1, 2].

In today's digital world, the lines and barriers between real world and digital transactions have blurred. Banking, government, communication and commercial services are networked together over a digital platform that no longer requires physical transactions to take place in order to deliver services. However, the convenience and efficiency of these digital transactions have social, political, financial and ethical consequences. Much of the controversy surrounds the control and ownership of information. When a person submits information about themselves or their finances to an online retailer or a government service, two important questions arise: who owns that information and how is that person's information protected? The same questions arise when a person uses a credit card at a clothing store. What happens if this information is abused and how can the owner of the information be assured that it will not be used without their knowledge? These questions will be examined further as they relate to the central question posed in this inquiry: **How can digital identity be managed and protected?**

This research project will address issues concerning personal information and digital identity. It provides a background on the development of digital identity, the spheres in which it is applied and possible issues concerning its abuse. Various technologies, mechanisms and strategies that currently exist to protect one's identity will be discussed. The concluding section provides a discussion on policies that can be implemented to mitigate the challenges associated with digital identity management and provide a framework for protecting a user's identity.

2. Background

2.1. What is Digital Identity?

2.1.1. A Working Definition

The concept of digital identity is integral to the management and protection of information in digital environments. In essence, it represents the digital version of a person's real world identity. According to Phil Windley [3], "A digital identity contains data that uniquely describes a person or thing (called the subject or entity in the language of digital identity) but also contains information about the subject's relationships to other entities." This second part of the digital

identity definition is what sets it apart from the real world definition. In the physical world, a person's claim to their identity can be confirmed through visual inspection. In digital environments, no physical information exists to identify the entity making an identity claim. Furthermore, the entity making the claim may not be a person at all. Any entity on a digital network can have a digital identifier (ID) including an organization or software residing on a computer [3]. The identity of the entity is used to gain access to resources, such as a simple web page, on-line credit transaction, corporate VPN portal or a web community.

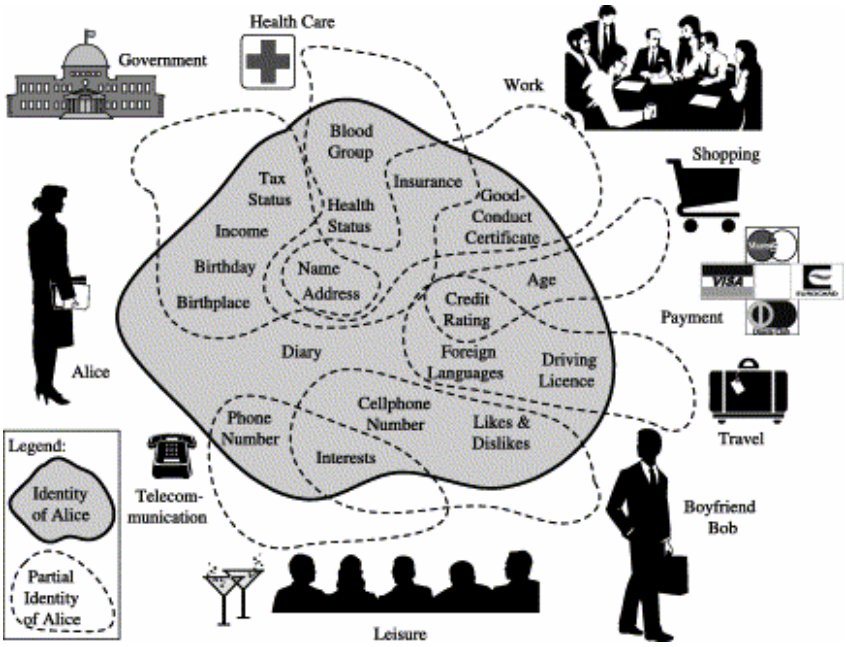


Figure 1 - Digital Identity Management Components

This concept of digital identity can be reformulated in the lexicon of computer networks by defining the two parts of a digital identity as the identifier and the authenticator. The identifier is a unique name used to refer to the entity without having to refer to its component parts, or properties. The properties of a human entity include items such as birth date and hair colour. The second part of an identity is the authenticator which determines the legitimacy of an entity's claim to their identity. An example of this in the physical world would be a photo ID, which visually authenticates the identity of the ID holder [4]. In order to gain access to resources, both the identifier and authenticator are required. For example, accessing a computer network requires a username and password; the identifier and authenticator.

2.1.2. Real World and Electronic Identity

In the physical world, the identity and the authenticator are contained together as part of the entity. Biometric information such as hair color, facial pattern, and other physical traits give proof to a person's identity. When a person performs a transaction in a retail store with a credit card, the name on the card can be cross referenced with the person's name on their driver's license, and matched to their photo. Although this identification method is vulnerable to several

types of fraud, it is much more secure than receiving the credit card number on its own (see appendix A for an evolutionary history of identification cards).

In the digital world the identifier and authenticator are separated or unbundled from each other to allow transfer from the real world to the digital world in the form of binary data. It is impossible for the on-line retailer to match a credit card number with a person's face, as is done in the physical world. In this case, the medium allowing the transaction is rooted in a digital system of ones and zeros, which no longer contains meaningful information about the individual. The challenge is to link the real world attributes of identity with identities residing in the digital world. This trend has begun to consolidate the spheres of physical and non-physical identities and has created a wide range of applications [4, 5].

2.2. Applications of Digital Identity

As the information age matures, the applications of digital identity continue to grow. The increasing number of digital identity applications can be grouped into two main categories. The first category is physical identity technologies which include identification for service provision in the areas of finance, government, commerce and health. The second category of applications deals with on-line transactions which include access to secure networks and portals, e-commerce related activities, targeted and embedded marketing and user preferences.

2.2.1. Physical ID Technologies and their Applications

Physical applications of digital identity encompass all transactions that occur in the physical world which are digitally transformed, such as a credit card transaction. When the card is swiped at the terminal, the customer's credit card account is debited the amount owed to the retailer or service provider. In this situation, the card represents the identity of the customer, and the authenticator is the customer's physical attributes or photo identification card.

Governments are the historical driving force of digital identification and are one of the biggest users of digital identity techniques to provide services and assistance, gather census data, tax citizens, and prevent crime. A major driving force for improved ID technologies is the need to prevent fraud, identity theft and terrorism. In order to meet this need, biometric and microchip technologies are being implemented in e-passports and foreign visitor verification systems to prevent abuse [6].

Many of the security issues that existed with ID technologies in the past still exist today. Authenticators such as photos, signatures and SINs are routinely faked in order to fraudulently obtain services. The use of microchips enclosed in plastic, called smart cards, attempts to solve some of these problems. These cards can hold much more data than magnetic strip cards, including biometrics such as fingerprint information [7]. The greater storage capacities and security features of the smart card allow it to be used for multiple applications. Many countries including Canada and the United States have begun to investigate National ID Strategies

(NIDS), which would combine the social insurance number with health and financial data in a smart card [8]. The implications of the smart card are far reaching and involve possible tradeoffs. In this context, the convenience and efficiency of these technologies is contrasted with the possibility of abuse and privacy issues that exist. For instance, regimes utilizing these technologies could misuse them as a way to oppress and monitor the population [9].

2.2.2. Cyber-ID Technologies and their Applications

This category of identity technologies has many analogues to physical ones. E-commerce, e-government, e-finance, and e-health, are the most common physical-world analogues in the digital world. Web communities, secure networks, context-based marketing, and user experience are amongst the new categories that have developed recently in response to the widespread use of computer networks.

2.2.2.1. Accessing Secure Networks

One frequent task that digital system users are required to perform on a daily basis is login and password entry. These common identifier-authenticator pairs are used to gain access to secure networks, virtual private networks and web portals related to government services, financial institutions, and on-line retailers. A user of computer-mediated communication devices has many digital identifiers which can be attached to different types of information. Depending on the nature of the service being provided the information may be related to general interests, career information, account numbers or credit card information. While the key driver in physical technologies has traditionally been government, the key force behind digital identity management is web 2.0 technologies (see below) and e-commerce [10].

2.2.2.2. Web 2.0, E-Commerce and Web Communities

In the 1990s internet e-commerce was in its infancy. Security, privacy issues and customer uncertainty were some of the barriers preventing e-commerce from entering the mainstream. However, since the turn of the millennium, the internet has earned the partial trust of consumers, encouraging them to shop on-line more frequently. This has changed the way people purchase products and services, creating a need for better ways to manage identity in order to secure the customer's full trust and increase market share [11].

Web 2.0 is a set of philosophies, technologies and strategies that have become a prevalent force in creating a more interactive user environment on the Internet. Web 2.0 sites share common characteristics; they are web-based, funded through advertising dollars, foster collective intelligence (where users add value through sites such as wikipedia) and undergo continuous growth rather than software updates. The centerpiece of this strategy is the web community and its associated commercial applications which depend on digital identity to provide their services [10, 12].

Google, Yahoo, Facebook, Wikipedia and Amazon are examples of web 2.0 sites that rely heavily on knowing and understanding the identity of the user (see appendix B for more information on web 2.0). The concept of the web community ties directly to the concept of identity because digital IDs provide the means for individuals and entities to be networked to each other [2]. Once a user is logged in to a website, they can obtain services that improve their surfing experience and organize their profile data. One example of this is the Google community: when the user logs in, they obtain access to email, documents, customizable user interfaces, shareable calendars and much more [10].

Many of these sites offer their services (such as photo, data and blog space) for free and cover their costs by using embedded advertisements. In the past, the user would have to pay to maintain these services in their own personal website. As network bandwidth increases and storage costs lower, it has become more practical for web community providers to host user content on their websites. This technical and philosophical change has made it easier for users to publish and share content, but it has also enabled service providers to collect more information about a user's identity. In this new paradigm, the focus has shifted from web publishing to web participation, without the need for technical publishing knowledge [10].

Two important questions arise from this discussion: who pays for the data storage and processing required by these communities and how is the user's digital identity important? Google used their AdSense technology to pioneer an automatic way to understand what users (or more specifically, their digital identities) would be interested in purchasing. This automatic and targeted advertising has become a major source of income for the search giant and has caused a change in the way users obtain services [13]. In the past, a user would pay a fee and obtain a service (for example, purchasing the Encarta Encyclopedia CD versus using Wikipedia). The providers of these services now typically generate income through targeted and embedded advertisements.

The user's identity has financial value because it provides clues to their shopping preferences and spending habits. In some cases a person's identity is treated as a commodity to be bought, sold and traded. It is becoming more common for web portals and service providers to ask for extra profile data when making financial transactions, such as the user's address and income level. When combined with data analysis tools, this information is very valuable to a retailer [5, 14].

2.2.2.3. E-Government and E-Health Applications

Governments have been utilizing physical ID technologies for some time; however, until recently they have been slower than financial institutions and business to use the internet for service provision. The Ontario government's strategy focuses on electronic service provision (ESP), which aims to restructure public sector systems such as the judicial, health and education systems, in order to provide an alternative to in-person service [15]. Digital Identity

plays a central role in providing services because on-line government systems must be able to guarantee that the person requesting the service is entitled to it. The government also has a major role in protecting identity through legislation.

Digitization of health information has also lagged behind the web 2.0 revolution for a variety of reasons including: privacy issues, funding, the need for sophisticated data security and cost of large scale implementation. Recently, Canada Health Infoway has investigated the concept of an Electronic Health Record (EHR) which will contain accessible, digital health records for all Canadians. In this scenario, the patient record would be stored centrally and could be accessed by general practitioners, hospital staff and the patient themselves. Digital identity information is vital in the implementation of this system and would be associated with the patient's medical history [16].

2.3. Digital Identity Abuse

Digital identity use has many important applications and enables the citizen, whether on-line or off-line, to be an active participant in their digital experience. However, identity abuse occurs on a daily basis without the knowledge or consent of the user. These abuses include more traditional elements such as fraud and identity theft as well as newer phenomena such as treating identity as a commodity, profiling, surveillance, monitoring and the use of biometrics. Whether these situations should be considered abuse or a typical element of the new digital experience, is an important question.

2.3.1. Traditional Abuses

Digital identity is a major component of the user's on-line experience and possibly the most vulnerable element in the digital world. Despite the use of firewalls and other network protection devices, if a criminal obtains access to a user's digital identity, they can impersonate that individual and obtain sensitive information. Regardless of the technology used, this low tech form of fraud makes networked computer systems vulnerable to attack. In one example, a hacker calls into the IT department of a company, impersonates an employee and requests that their password be reset. Without validating the identity of the person on the phone, the IT department resets the user's password, allowing the hacker to gain access [17].

Another way to gain access to secure databases is through holes in the security system which allows unauthorized access. Programming errors cause personal profile information to be released to the World Wide Web through a glitch in the system's protective hardware and software layers. Many examples since the turn of the millennium have demonstrated that customer information is vulnerable to hacking, even amongst the largest, most secure e-commerce retailers including Amazon and Ebay [14].

Personal identifiers in the real world are also vulnerable to hacking. Smart cards, RFID tags and biometrics are not guaranteed to be fully secure or tamper proof. These instruments use

encryption technologies which can be hacked or identifiers such as fingerprints, which can be faked [18]. In all these cases, the person's real world identity is compromised by technical vulnerabilities. In one example, VeriSign's medical RFID tag was found to be replicable [19]. Cloning of the RFID's frequency allowed the clone to impersonate the digital ID of the user. This could compromise a patient's health information and access to care

The abuse of National ID strategies (NIDS) has been widely discussed [8]. This could result in a loss of privacy for individual citizens because multifunction cards allow the ability to track the card holder's data trail from a central location. There is also some doubt as to whether a NIDS would actually prevent terrorist attacks and provide better security for a nation, which is the primary justification for their use [8].

2.3.2. Modern Abuses

2.3.2.1. Phishing

Phishing is a recent phenomenon that involves stealing a person's digital ID information such as name, password, and credit card number. The most typical situation involves a forged email from a popular web portal, such as Ebay. Customers are asked to click on a link to confirm their profile information or set-up account information. The user is directed to a fake website which collects identity information for criminal or commercial purposes. Identity theft on a large scale through phishing can be very costly for a user, especially when they provide a SIN or credit card number to the fake website [20].

2.3.2.2. Data matching and Profiling

Before the Internet was in widespread use, data was stored in secure, central mainframes that were seldom linked to the outside world. The Internet provided a means for decentralizing data, making it more vulnerable to attack and allowing more linkages between data stores [21]. Software analysis tools can be used to perform data matching and profiling on this linked data. These primary forms of digital surveillance take place on a daily basis using cookies, user profiles, IP addresses, transaction information and click history [14]. Embedded marketing applications depend on these data analysis tools to piece together the partial or full identity of the surfer and their preferences. As an example, Google uses cookies residing on a user's computer to partially identify the user. This identity is linked with search history data, analyzed and used to determine the most relevant advertisements to display [22].

A more effective profiling approach is to have the user log into a website because their preferences, messaging history and interests provide clues to which advertisements would be the most appealing and effective [2, 10]. In one example, when the iLike music application is added to a Facebook profile, it searches the user's profile (their social digital identity) and determines which bands they like. The application then displays these bands, their albums, their upcoming concerts and a link to Ticketmaster for purchasing concert tickets. This type of advertising is very convenient, efficient, targeted and intrusive. Gmail also uses this technology

to analyze a user's email and customizes advertisements to be displayed to them while they read email. This is akin to "the post office opening a user's mail in order to decide what junk mail to send." [14].

Collecting profile and identity data can provide some benefit to the user. Targeted advertisements ensure only relevant ads are displayed, and preferences allow users to customize the sites they regularly visit. Digital profiles allow the user to select content and maximize the benefits that web services provide. They are becoming one of the biggest advantages that dynamic websites have over static sites that do not allow the user to participate in content provision [23].

2.3.2.3. Competing Interests

Market pressures encourage the bundling of as much identity information for each customer as possible, since this maximizes profits for businesses. On the other hand, privacy advocates and ID management schemes necessitate a certain amount of unbundling to ensure the user's privacy is maintained and to ensure that the user has control over the information being disclosed [23]. This argument surrounding identity as a commodity calls into question whether the user has a right to privacy regarding their on-line activity. A third component to this discussion involves law enforcement officials who want access to identity information, in order to ensure that the law is being upheld on the Internet. Legislation, voluntary policies and informed consumer choice will all have roles to play in determining a compromise that benefits all parties involved [23].

A major issue that is representative of this debate is the selling of identity information. Some bankrupt on-line retailers have attempted to sell the identity information of their customers to other interested parties and some governments sell census data for the purpose of commercial data analysis [14]. Privacy advocates have taken issue with larger retailers, such as Amazon.com, who clearly state in their privacy policy that a user's profile information can be sold along with subsidiary companies [24].

2.3.2.4. Surveillance and Identity Creep

Today, the state is only one of the actors able to monitor people's movements, financial transactions and digital activity. It is now possible for commercial entities, organizations and individuals to also conduct surveillance. This can be achieved digitally, without the use of traditional video cameras or tracking beacons [14].

Clickstream data, the series of hypertext clicks that a user undertakes while surfing the Internet, and an entity's data trail enable covert surveillance through software (see appendix C for a typical data trail example). According to Amazon.com they collect the "clickstream to, through, and from [their] web site, including date and time; cookie number; products … viewed or searched …" for every customer who uses their site. They also "may use software tools … to measure and collect session information, including … page interaction information" [24]. Other

companies may use spyware which are programs that can be downloaded to the user's computer in order to obtain this type of data. The data is attached to cookie information and cross referenced with clickstream data to form a user profile and target advertisements. Users can also harness digital surveillance techniques to find old friends, monitor the users of their computer and conduct criminal background checks [14].

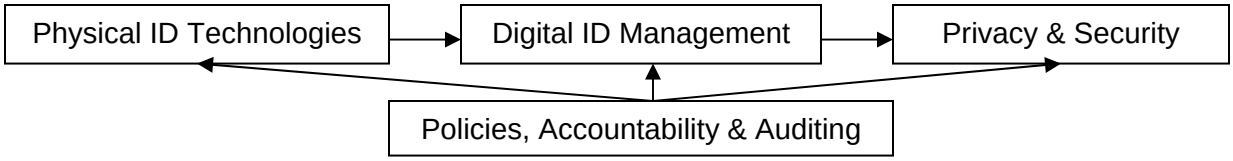
Identity Creep is the abuse of digital identity information associated with the collection and monitoring of personal information and data trails. It occurs when the collected data is used for a function other than its indented purpose and is a factor discouraging users from participating on-line. The lack of anonymity and the digital traces left by users allows for covert activity and falsification of communication data. This could impact e-commerce negatively, especially if companies continue to abuse the collected data [11]. Governments, corporations, law enforcement officials and users must work together to create a system of identity management that satisfies the competing interests that currently exist. This may ensure that digital identity in the physical and digital worlds will not be abused.

3. Central Question and Anticipated Findings

Digital identity is a product of the digital information systems revolution. It is the key identifying construct for every citizen in the real and digital worlds. This information is processed daily by governments, businesses, institutions, financial organizations and users. The potential for fraud is omnipresent and has driven the need for better technologies that protect the privacy of individuals and the information contained in their digital profiles. Central to this issue is the question: "**How can a person's digital identity be managed and protected?"** The question is relevant to many stakeholders whose concerns are different and whose interests may place them at odds with each other in certain debates; however, it is clear that the abuse of identity affects all parties, including those who profit from that abuse. Upon investigating the central question, a number of anticipated findings are revealed which take into account the various stakeholder perspectives and their concerns:

1. **Physical digital identification technologies can better protect information against fraud and identity theft.**
2. **Digital ID management techniques can mitigate the issues associated with the use and abuse of digital identities.**
3. **Policies and legislation are required to ensure the abuse of digital identities is avoided.**

The relationship between the anticipated findings can be summarized as follows:



4. Discussion of Evidence for Anticipated Findings

4.1. Physical digital identification technologies can better protect information against fraud and identity theft.

The question “How can a person’s identity be managed and protected?” can be answered with a discussion of the physical ID technologies that are being researched to replace traditional forms of identity tokens such as driver’s licenses and SIN cards. These new technologies include smart cards, RFID embedded tags, direct biometric scanners, encryption technologies and mobile-GPS tracking. These technologies aim to protect identity, provide greater service and convenience, and ensure that only those entitled to the card-holder’s privileges obtain the associated services. The key drivers in the development of these technologies are increased identity theft, fraud and customization requirements.

4.1.1. Smart Cards, Embedded RFID devices and Biometrics

The smart card has been used in a variety of applications throughout the world and is predicted to replace its predecessor – the magnetic stripe card (see appendix A for a brief history). The term smart card refers to an enclosure that holds information using memory storage devices and carries out simple processing using an integrated circuit and microchip (see appendix F for a detailed description). The advantage of the smart card over the magnetic stripe card is that it can store greater amounts of data which can be encrypted, providing a higher degree of security. Greater storage capacities provide the ability to store biometric information on the card, such as fingerprints, which are important authenticators for identity. These cards can read, write and store information dynamically, while older magnetic stripe cards have limited capcities. In addition, smart cards are more reliable and last longer than the magnetic stripe cards [25].

An RFID contactless smart card uses inductance from a receiving antenna (card reader) to power the transmission of identity data wirelessly. This technology eliminates the problems associated with electrical contact breakdown and provides more convenience for users because they do not have to remove the card from their wallet. An extension of the contactless card is the embedded RFID chip, which can be surgically implanted into human or animal tissue, and is activated when the human or animal comes in close proximity to the chip reader. The VeriChip, developed by VeriSign, uses this technology to identify medical patients who cannot identify themselves. The chip is associated with the patient’s electronic medical record and can be accessed from a variety of sites, ensuring that the patient receives proper medical attention in an emergency [19].

Smart cards have a wide variety of applications in virtually all fields where identification or financial exchanges occur. They are also used as secure network access tokens, electronic cash cards, phone cards and credit cards. Storage capacities, security features and the

read/write properties of the cards make them much more versatile, especially for e-cash and identification purposes [25].

4.1.1.1. Benefits of Encryption and Storage

The smart card's use in digital identity applications is mainly facilitated by its ability to encrypt identity data and store biometric information. Computer network access and service provision in the real world are more secure when a person's identity has been securely identified. In the case of e-commerce and credit cards, a smart card helps solve some of the associated problems. When a customer enters a credit card number, the online retailer has no ability to confirm that the person who is using the card is the same person as the card holder. A smart card with a hardware reader provides two-factor security. In this case, the retailer knows the person is using the physical card and receives an encrypted credit card number. This greatly reduces the chance that the credit card number can be eavesdropped and provides some protection against fraud and identity theft; however it does not guarantee against the use of a stolen card. In the physical world, a smart ID card can provide a tertiary level of security by containing a person's biometric data, which can be used to identify the person when the card is swiped and the biometric is scanned. The card also acts as a person's encrypted identifier which is used to grant services such as building access [26].

The current construct that is widely used for encryption is the public key method. A public key is used to encrypt data that is sent to the user. The user holds a private key that forms a match with the public key, to decode the data. The public key is given to those who wish to encrypt messages; the private key is kept secret and given to only one user. The system works as long as the key holder's identity is certified. A certificate authority confirms the identity of the public key and private key holder in the form of a digital certificate. When the certificate is used to encrypt data, the person decrypting the data can be reasonably sure of its trustworthiness. In theory, this system is sound; however, it is possible to hack the keys, illegally certify keys, and steal keys through brute force methods [27, 28].

The smart card's encryption technology generates and stores the private key on the card so that it cannot be easily stolen or eavesdropped, and certifies the key as authentic. [26]. In addition, brute force methods to gain access to keys on a smart card can be thwarted by the card's circuitry which locks it down if too many incorrect access attempts are made. These security features have made the smart card "the main platform for holding a secure digital identity" [25]. The smart card's storage capacity allows multiple passwords and digital certificates to be stored on one card. The card holder only needs to know the card's PIN number; the passwords are kept secret from the card holder, making them more resilient and secure. This feature allows the smart card to be used for access to multiple services and provides a secure piece of identification.

Smart cards can be used in this manner for Secure Socket Layer (SSL) encryption systems in web browsers and for physical building access. For instance, a smart card can be used to grant entry to a building, and then upon examination of the digital identity profile, certain areas of the building can be made accessible. An example in the digital world would involve swiping the smart card at a computer terminal to gain login access to banking information without typing in a username or PIN. The smart card is a token representing the user's identity and includes the authenticator, in this case an encrypted, strong password [19].

4.1.1.2. Biometrics: The evolution of the Smart Card?

Although biometrics have been used by law enforcement for a century, they have only become popular in identification schemes recently. A direct biometric system, operating in identification mode, circumvents the need for a smart card and relies on directly scanning a person's biometric identifier such as a finger print or facial scan. This scan is matched to a central database of biometric identifiers and identity profiles, which the person has been previously registered in. Once the match is deemed valid, services can be obtained. This helps to prevent identity theft by eliminating the uncertainties involved in smart card encryption, hacking, duplication and brute force stealing. The proper technological improvements can reasonably give a performance benefit over smart cards in terms of reliability [18]. In authentication mode, a smart card is used to store biometric information rather than a central database. When the person attempts to obtain a service, the biometric scan is matched with biometric information on the card, which acts as a distributed data store. This scheme removes the security issues associated with the central storage of ID information [29]. Whether an identification system is based on smart cards, biometrics or a combination of the two, each has its own associated negative aspects which hinder the adoption of the cards for certain applications, especially a national identification scheme [30].

4.1.2. Challenges to Implementation

National identification schemes (NIDS) have been proposed in many countries to help manage and protect identity, facilitate the provision of e-government services, improve citizen authorization, increase national security and improve interactions with business. The identifier, a smart card or biometric, is a key component of this system; however, the limitations of these technologies must be taken into consideration when developing an identification system for both government and business applications, which consolidate multiple functions [26, 30].

4.1.2.1. Technological Issues and Challenges

In any NIDS two primary processes take place. Registration involves presenting documents such as a birth certificate to obtain a digital ID card. The second process of authentication occurs each time the cardholder attempts to obtain services or verify their identity, which involves confirming that the cardholder is the person referred to by the card.

Error rates in data-matching are one of the biggest technical barriers in this process. When biometrics are used, a margin of error exists between the stored image of the biometric and the live scan of it. A biometric system is a pattern recognition and matching system which is not error proof. Imperfect imaging conditions, changes in the physical characteristics of the biometric (cuts, bruises and aging) and loss of the biometric (losing a finger or eye), can provide significant barriers to accurate matches. The system accommodates for this by looking for an approximation of the biometric within a certain threshold. If a biometric comparison is below the allowed threshold, the identity match is rejected. This could cause the system to mistake one person for another (an incorrect match), or reject a person even though they legitimately exist in the database [18].

Biometric and identity theft are another threat to the widespread adoption of digital identification. Smart Cards can be stolen and hacked; biometrics can be faked through 3D fingerprint copying, facial masks, prosthetics and eye contacts; and central databases can be compromised, exposing biometric information. When a password is compromised, it can be changed by the user to avoid future abuse. When a biometric is stolen, it is compromised for life. While it is true that biometrics are difficult to copy compared to passwords, the stealing of biometric information carries with it very high penalties. To combat this, encryption is employed to make the biometric harder to steal. Some authorities also recommend using localized databases rather than central ones, to prevent large scale hacks of data. A high capacity smart card with optical drive can store multiple biometrics and not require the use of databases [31].

A war between technology developers and hackers is occurring on a variety of fronts which could further comprise biometric identification: *Reverse engineering:* involves extracting information from smart cards by reading their memory and copying the contents. *Power analysis:* can determine whether or not a password or PIN was properly processed by a smart card by examining its differing power usage. A redesign of the circuitry can alleviate this threat. *Scanning and tracking:* involves using a reader to examine the signal emitted by a card or passport. This applies to RFIDs which can be scanned or “skimmed” without the cardholder’s knowledge by applying an inductive field within a certain range of the circuit. This can compromise a person’s identity and location for use by pick-pockets. To combat this, the card could be contained in a material that does not allow radio frequencies to pass through to the card. *Eavesdropping*: involves intercepting the data when it is exchanged between the card and the reader. This can be counteracted by encrypting the data being transferred. *Cloning*: involves creating a copy of the card using a fake reader. This could allow RFID keys (such as building access or car keys), to be cloned and used by criminals. Engineers are currently working on non-cloneable RFID tags to address this issue. Although stealing a signal does not necessary imply that it can be used, if the encryption technology is weak, it can be easily hacked [32].

Digital ID technologies, while vulnerable to threats, are more secure than existing technologies which rely on non-encrypted magnetic strips and username-password pairs. It is more difficult to copy, share and distribute biometrics and it is impossible to misplace or forget them. They are also more difficult to forge and steal. Passwords on the other hand are generally weak, rely on the user's management and can be hacked in massive lots. A variety of combinatory biometric techniques can be used to further thwart criminals, such as requiring more than one biometric to be presented in a predetermined order to grant access [18].

4.1.2.2. Social Issues and Challenges

"The introduction of biometrics is not just a technological issue; it poses challenges to the way our society is organized" [30]. Digital ID technologies present governments, businesses and individuals with a variety of challenges. One major issue surrounds the combination of digital IDs with information technology tools such as central database information storage. When ID processing is combined with profiling and data-matching, those who maintain the database have access to surveillance information that could expose private citizen data. Using centralized databases for identification authentication can become a surveillance tool for law enforcement, especially when NIDS are put into place and aggregate large amounts of information in central locations. This information convergence could include sensitive information such as health records, criminal records, spending habits, location based tracking and financial transaction histories. Once stored, the information can be copied, analyzed and cross-referenced without a person's knowledge or permission [31].

National security interests are frequently used to justify surveillance creep. However, this type of monitoring can lead to social stereotyping, privacy invasion and social sorting. A good example of this is the profiling of Arab passengers after the September 11, 2001 attacks on the World Trade Centre. Smart cards combined with centralized databases, facilitate sorting and classification techniques, which could infringe on civil liberties [33]. Another related type of social segregation occurs for those who may not have the proper biometric or whose metric is not reliable. Some people have fingerprints which can't be scanned, while others may not have the proper fingers, voice patterns, or irises. These people may be unable to access services or unable to authenticate their identity in a variety of spheres including commerce applications and international travel. In a worst case scenario, the lack of biometrics, or information associated with a digital ID may cause employers to reject applications for employment or businesses to deny service to an individual [18].

Unintended functional creep involves the use of biometrics for secondary information extraction rather than identification. Some research indicates that finger scans, retinal scans and DNA scans (which are not yet in widespread use), can provide clues to the health of the individual, their predisposition to diseases and their current emotional state. This type of

information could be obtained by insurance companies or employers and used to screen individuals [18, 30].

Non-scientific assumptions regarding the security of biometrics, smart cards and RFID tags can be a major hindrance to their widespread adoption. Law-makers and citizens who do not recognize the social and technical limitations of these technologies put themselves at greater risk of fraud and identity theft. Furthermore, technologies such as RFID implants, tracking devices and other technologies that combine digital IDs with authentication services can infringe upon a person's civil liberties. Questions as to whether the government could require citizens to be implanted and who owns biometric data stored in central databases arise frequently in discussions regarding automatic identification. GPS technologies can easily be used to track implanted individuals and allow them to be monitored by an abusive state or by their employer. It is important for decision-makers to understand the duality of digital ID technologies. Their ability to manage and protect identity is great; however, their ability to be abused is equally as great, if the proper policies are not put in place to protect individuals [34].

4.2. Digital ID management techniques can mitigate the issues associated with the use and abuse of digital identities.

In the previous section, the evidence presented concerned the physical technologies used to manage and protect identity. The discussion centred on the devices as identity inputs to the digital world and explained their role in authentication and access to information. Digital ID management techniques are software based solutions that exist primarily in cyberspace. The identifier or input could be a username and password, a smart card or a biometric since the management of digital ID is independent of the identifier technology. This section will focus on software-based management solutions which can help answer the question: how can a person's digital identity be managed and protected? It will include a brief technical overview of ID management and a discussion its advantages and associated challenges.

4.2.1. Technical Overview

Identity management is defined as a "set of processes, tools and social contracts surrounding the creation, maintenance and termination of a digital identity for people … systems and services to enable secure access to … systems and applications" [4]. A repository or central data store holds the profile information associated with the identity along with the policies that govern access to information. These authorization and privacy policies determine how the information is used and protect the user from invalid uses. Auditing is generally conducted to ensure policies have been adhered to [4]. A key characteristic of these systems is a single sign-on access point which allows the user to obtain access to multiple services with only one identity authentication process. Although no universal sign-on schemes currently exist

on the internet, examples of small scale systems are Microsoft's .Net Passport and OpenID, an open source ID management system used by AOL and other web portals.

4.2.2. Current Issues

The identity management trend is driven by the convenience of single sign-on, as well as the ability to personalize the web experience. This is important for e-commerce and social networking applications which depend on user profiling to tailor advertisements and meet commerce-related needs efficiently [4]. The Internet's lack of a universal platform for ID management is a major problem which compromises the management of digital IDs and requires additional applications to perform management tasks. Unlike email, the Internet's only built-in personal identifier, different applications do not follow the same standards. The lack of a universal set of communication standards and unbundling of identity information can hinder communication between internet entities and create areas of weakness that can be easily hacked [35].

At the same time, unbundling may protect an individual's privacy by supplying only the portions of an entity's identity that are required for the transaction to take place. For instance, some transactions may only require that the age of the user be over 18, or that they be located in a certain region. In terms of law enforcement, user anonymity makes it very difficult to track on-line activities and curb crime. The business case parallels the law enforcement case on the basis that the more information they are able to collect from users, the better they can target advertisements and product innovations. The compromise between a fully unbundled environment and a totally anonymous Internet may be achieved through ID management [2].

The dominant identity management scheme today is the silo method in which a single organization manages identity for a fixed set of users. When a user wants to obtain services from a silo organization, they must create a profile, login and password. The popularity of these sites for e-commerce, social networking, career building and e-government has caused user inconvenience and confusion with a large array of independent profiles. The current system allows the user to remain semi-anonymous, but requires a great deal of profile management. Information collection is also a major issue, since the user is generally required to provide much more information than is required to obtain services. It has become popular for service providers to collect and link these profiles through cookies to accumulate sensitive information about individuals [4, 35].

4.2.3. Advantages of New Identity Management Platforms

There are three additional types of management platforms that attempt to overcome the silo's proprietary and fixed nature. The walled garden method consists of a closed network of organizations which use a common, centrally operated identity management system. This suits business to business transactions where the members share a common interest or investment.

The federated system concept, a more flexible ID management system, shares the operation of the system with all federation members. Multiple identity providers share a distributed data store of identity information. Operating policies define the roles and rights of all the providers in the network. Regardless of which provider performs the processing, a certain level of service is guaranteed and each provider adheres to the same set of policies. In this scheme, the end user is provided with control over how profile data is used amongst members of the federation. Another related scheme is the Open system which defines a universal protocol for identity management across the entire Internet. It can be viewed as an extension of the federated system, where all entities on the Internet share a common identity management system and a distributed data store. The key to implementing these systems are the use of directory services and a global repository to manage the various entities and their data [4].

The advantage of these last two systems, federated and open, is their distributed nature. No entity holds the entire set of data and therefore the systems are protected from a large scale attack. Previous implementations of these systems using the ISO Open Systems Interconnection (OSI), have proved to be either too complicated or too simple [35]. However, the Open ID consortium has made some headway in creating an open identity management system. Social, service and commerce based networks such as America Online (AOL), have begun to use this service. Anyone with an AOL username and password can sign-in to other sites who also use open ID, without having to re-register. The flexible and adaptable nature of these systems is what sets them apart from their predecessors. [36].

These systems provide the framework for user-centric control of identity information and data access. The European Union has begun creating legislation that aims to achieve this goal. Under this approach, users can chose what personal data to disclose and which credentials to present when entering sites that require authorization. This philosophy is in marked contrast to the current identity management paradigm of centralized systems, which allow the identity administrator to have full profile monitoring abilities. Examples of this include current e-government solutions, Facebook, Amazon and Google. User-centric federated systems operated by the Liberty Alliance, Microsoft's Card Space and Open ID satisfy privacy interests, provide better management schemes and when combined with security cards, biometrics and encryption technologies provide improved security. These systems also give the user control over how they interact with websites, especially those involved in embedding e-commerce. To protect the user's interests, federated alliances require that individual providers maintain the overall privacy policies of the network and remain accountable [37].

The ability of federated and open systems to maintain user privacy and allow the use of multiple personas provides a major advantage in protecting identity. The user is only required to register once with one of the providers in the federation (the identity provider). When logging into another member of the federation (the relaying party), the user's single identity, can also be

used for the other party. The user can request that the identity provider send the relaying party only specified information (a pseudo-identity). This process allows the user to remain semi-anonymous and guarantees that he or she is authenticated under the trust established between the identity provider and the relaying party [36].

The convergence experienced in the commercial sector, under the leadership of corporations such as IBM and Microsoft, indicates that ID management systems may be the solutions required to legitimize e-commerce, marketing and advertising, by allowing the enforcement of privacy policies through user control. At the same time, the lessons learned in this industry may have implications for improving e-government. Open ID management systems address the concerns associated with centralized government databases, citizen anonymity and security. Digital Citizenship combines digital identity with credentials that are processed by an identity management system. This would allow one national ID card to be used for multiple services, but only release the information required to complete the transaction or service being requested. Different levels of government can provide the registration for services, while one or more government entities can act as the identity provider. When combined with biometrics, these access control schemes will be of vital importance to the success of electronic government, banking and commerce [26, 30, 35].

4.2.4. Challenges in Implementing ID Management

Technological and social barriers challenge the widespread adoption of federated and open systems. The concept of identity itself is not universally represented in the same format amongst service providers, which hinders the interconnection of federated systems. For widespread adoption to occur, the concept of identity must be able to encompass all current and future properties in a global, standardized format [35]. The isolated development of new ID management systems does not further the goal of true single sign-on. Although there is a trend towards convergence, there still remains a variety of different ID federations and many hold-outs. Some consortiums do not wish to create standards for identification and profiling because of vested interests in profile data for e-commerce and marketing purposes [38].

Modern identity management systems can be flexible and dynamic, providing a high level of user control over personal information. This feature addresses the lack of control over the processing of profile information and clickstream data, but can become un-manageable for the user when they belong to a variety of websites and utilize a variety of services. Systems such as the Platform for Privacy Preferences (P3P) provide a framework for automating the user's permissions, in order to deal with complex preference sets. However, automated processes can keep the user unaware of the information being processed about them. Therefore, identity management systems should build in privacy and data trail awareness to avoid the potential problems users encounter with privacy invasions such as saved search histories and un-approved targeted ads [39, 40].

Security is an omnipresent issue in the digital identity management debate. Systems need to ensure that an entity's identity properties cannot be fraudulently changed or stolen. Single sign-on systems, while providing convenience and enhanced control over data, can also pose a severe security risk. The large number of applications that get bundled under the single identity increase the risks associated with identity theft and fraud. If a hacker gains access to a user's identity login or smart card, the entire collection of the user's on-line life is vulnerable [37].

Digital ID management providers should also ensure that the communication partners are who they claim to be. Although most systems address this through digital credentials or the use of identity providers, the links are not fully secure. Auditing this information is a major challenge, and is necessary for mitigating the effects or fraud and theft. An auditing system must check credentials, ensure policies are adhered to and protect the user's privacy interests. Currently most websites that collect profile information must be trusted to adhere to their policies. The user has no way to guarantee the site's accountability and current laws are not uniform across all jurisdictions, which allow for many grey areas regarding user privacy [40].

Current centralized management systems utilize digital signatures and credential based public key encryption rather than the modern techniques of policy and anonymity support, provided by federated systems. These systems are currently used in e-government schemes and generally do not address security needs successfully. They allow for the abuse and unintended disclosure of profile information by the service provider without explicit consent. Furthermore, the authentication processes which confirm the claim to identity through the examination of credentials are not flexible. Current systems require fixed information to authenticate a user whose full identity is revealed. New implementations should allow the user to choose which credentials to use and what information to reveal. Since the identity and its associated profile information can be augmented by the user or a third party, access rights to the identity profile should be set on a per interaction basis. For instance, age and birth date may come from a person's birth certificate; however, their credit rating is set by an external party who needs to be granted access to set profile information [35, 41].

Many of the leading Internet companies have acknowledged that present systems can have negative repercussions for e-commerce and e-government. Many retailers are working to define clear roles in identity management to ensure that they do not lose their customer base over privacy issues [41].

4.3. Policies and legislation are required to ensure the abuse of digital identity is avoided

In the past, cities were protected by walls and moats so that citizens and economies were protected from intruders and criminals. Eventually, invasion technologies such as the cannon were able to breach the security of these cities making traditional methods of protection useless. The modern city has no walls or guards for protection, instead new systems of commerce and

methods to establish trust were designed to make commerce and government more easily accessible. Today, a similar development is occurring in corporate, commercial and government computer networks. Security issues, lack of trust and privacy concerns are threatening to bring down the walls that have traditionally protected digital entities. This could be perceived as a threat or as an opportunity to renew the way digital identity is conceptualized, authorized and utilized [3].

The understanding and management of digital identity is represented in the policies that govern its use for data processing, storage, authentication and service provision. An examination of policies and legislation that are currently in place or being proposed can help answer the question "How can a person's digital identity be managed and protected?" In the past, new technologies have been introduced without a true understanding of their impact, creating a policy gap. It is possible that a policy gap exists where digital identity is concerned. An examination of the evidence can help ascertain this claim.

4.3.1. Current Policies and Perceptions

A prominent belief in most Western societies is that a person's identity data should be kept private and protected by the law. In traditional spheres these laws have sufficed; however, in this new age of cookies, data aggregation, data mining and identity theft, the problem and its context have changed [3]. Citizens and legislators throughout history have been apprehensive about new technologies they do not understand. It was thought that the television would replace the radio and that RFID tags will allow the government to track its citizens. Although there is some truth to both assertions, policies that do not allow TVs in automobiles have ensured the dominance of radio in that sphere, and RFID tags for building access cannot easily be used for tracking individuals, other than knowing when they've entered and exited a building. Regardless of the reality, the introduction of new technologies, especially when they impact personal privacy, are treated suspiciously by the public. Further complicating the issue is ill-conceived legislation developed to minimize the impact from isolated or fringe events, while not addressing the root issues associated with protecting identity [3].

Europe's privacy laws are generally thought to be more advanced than those in North America. Numerous laws, such as the European Data Protection Initiative outline privacy protection regarding the collection, storage and use of employee and customer personal information. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000 was created in response to the European legislation in order to facilitate cross border information exchange without disruption. It outlines ten principles for protecting identity, based on those developed by the Canadian Standards Organization (outlined in Appendix D).

PIPEDA attempts to balance the need to protect a person's right to privacy with the needs of organizations who collect, use and disclose personal information as part of their legitimate commercial and information processing activities. The legislation has benefits and drawbacks

for maintaining a citizen's privacy when they interact with the digital world. On the positive side, it is technology independent, has low associated costs of implementation and incorporates an efficient complaint mechanism which was designed with input and support from multiple stakeholders. The accountability requirements of the act aim to ensure that domestic and international third parties who may come in contact with personal information handle it in conformance with PIPEDA. On the whole, the legislation lays the groundwork for a national privacy protection policy based on sound principles which aim to reduce the instances of data mining, surveillance, spamming, phishing and illegal use of biometric identification.

The legislation is a step in the right direction; however, it is not without drawbacks which pose challenges to the act's ability to protect digital identity. In part, this is due to situational factors associated with the constantly changing nature of the digital world. Increase in personal information flow across international borders, illegal data trafficking, spyware, threats to computer system security and government interests in personal information have impacted the relevancy of the legislation to some degree. For example, the web 2.0 revolution and its use of cookies to track user movements in cyberspace are not significantly covered under this legislation, as it applies mainly to commercial transactions [42].

The nature of the legislation itself can also act as a barrier, especially in the oversight and enforcement of the act. The privacy commissioner's office is responsible for investigating infringement claims and making compliance recommendations, but in their capacity as an ombudsman, do not have the ability to enforce the recommendations they make. That power lies in the hands of the federal court; however, court cases have proven to be expensive, time-consuming and under-utilized. According to Christopher Berzins [43], a complaint-based enforcement system may encourage a reactive resolution process that is not well suited to a privacy context. Usually, a dispute involves two stakeholders and the resolution pertains to their single case. This case may be use as a standard to guide new policy development, yet it was not conducted in the context of a transparent, multi-stakeholder approach. This could lead to narrowly focused legislation that treats fringe cases rather than root issues [43].

The legislation's policies may favour organizations over users in some cases involving disclosure. On many occasions, the general public is not made aware of abuse cases or the issued recommendations, making PIPEDA somewhat ineffective, while continuing to compromise the security of the public. Personal security is further comprised by PIPEDA's lack of notification requirements. Currently, organizations who have suffered a security breach do not need to notify their customers of the issue [42].

PIPEDA requires that the user consents to the use of their personal information. While this keeps the user informed of possible abuse situations, the legislation also allows information to be collected without the user's knowledge or consent for national security, government and law

enforcement investigations. Once the data is obtained by the government, it is no longer subject to PIPEDA's regulations and therefore can be used for monitoring purposes [42].

Corporate privacy policies are considered a necessary element of digital interactions in order to maintain the trust of the customer and outline the company's terms of service. In many instances these policies are not clear or are difficult to read. Under PIPEDA, the organization is only required to obtain blanket consent of a policy. In many cases there is no way to ensure that the policies are carried out by the company and therefore the customer has no ability to ensure that the company is not using data for an un-advertised purpose. This is especially true when a user is required to submit information that is not explicitly required for a transaction. Excessive or needless data collection can sour the relationship between the user and the website provider and erode trust [31].

Perceived credibility is very important to user relations. If an organization has had too many database attacks where data was lost, or has a track record for selling customer information, users will not been very keen on using the service the site provides. Ebay, Amazon and Yahoo have been criticized for suspiciously changing their privacy policies. This tends to alarm users to the possibility that loopholes and policies can result in the manipulation of their data [3].

4.3.2. New Methods to Protect Identity: The Laws of Identity

> "The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities are so diminished as to lead to its demise. Enter the 7 Laws of Identity" [44].

Privacy involves the control over one's personal information in terms of its collection, use and its disclosure. An examination of the current digital systems that collect and process identity information has proven that individuals have little control over their information once it is submitted to a digital entity. The solutions mentioned in this paper attempt to technologically manage and protect privacy; however, policies are required to direct the development of these solutions so that privacy considerations are embedded in their design. In creating an identity metasystem, or identity layer of the internet, which will universally identify individuals, policy development, implementation and auditing will prove to be crucial components of the system's success [44].

The Identity Metasystem, as described by Microsoft engineer, Kim Cameron, in his Identity Blog [45], is a platform which enables different identity management systems to communicate with one another. By implementing policies, protocols and various software technologies, federated, open and silo systems could process identity information from various providers. Many experts agree that one internet-wide open ID management system is not a likely prospect, given the large variety of systems that currently exist. Instead, a metasystem that connects every ID management system together could provide the same functionality of an open system;

a platform for establishing a single identity and various pseudo-identities for each user on the Internet [45].

The policy that governs the design of this system is summarized in the laws of identity. They were developed by Kim Cameron through open dialog with users, industry leaders and many experts in the digital identity field; they were also adopted by the Privacy Commissioner of Ontario and a long list of stakeholders across various industries. Increasing the privacy and security of digital identities on the Internet, and in other sectors such as government, commercial and financial is a crucial step that the metasystem could provide. The laws complement worldwide fair information practices such as PIPEDA, but go beyond their limitations. While PIPEDA must be enforced through a complaint system, the laws are embedded in the design of the system and are audited to ensure compliance [3, 44].

The laws of identity, found in Appendix E, outline the policy component of the metasystem, which incorporates policy in the design of a universal identity scheme. They help to ensure that users have direct control over their personal information and authorize the use of their data for only the purposes agreed upon in the transaction. This is in line with legislation developed in a variety of countries since the 1970s which aim to limit the collection, use and disclosure of personal information. In addition, the laws ensure that only the minimum required amount of user data is used in a transaction, helping to prevent identity theft. The concept of directed identity enables the user to chose which identity profile will be used to communicate with the relaying party. This profile can be a subset of the entire profile, allowing the user to remain semi-anonymous during the transaction [44].

Interoperability is another key concept in maintaining privacy. It provides a platform for different ID technologies to communicate with each other, creating a common login interface and account creation, and at the same time gives the user choice in which ID provider to use. This can help diminish the chances for a user to be tracked or profiled, as would be the case if a central system were used. Finally, the laws can protect users from fraudulent emails and websites, making them less susceptible to phishing [45].

4.3.3. Interoperability and Convergence

Policies, legislation and standards are required for sustainable ID management systems. Without them, customers and citizens will avoid establishing trust relationships with service providers. Customers may also avoid services that are not interoperable with other systems. This has motivated service providers to adopt interoperable systems in order to gain market share and improve the user experience. E-government applications will need to do the same, by designing systems at all levels of government that are interoperable with each other. One important application of this is the biometric smart device. The value of the device increases as the applications it can be used for grow. For instance, a government ID that can be used as a social security number and a bankcard has a high level of convenience and applicability. In

other cases, interoperability may be necessary for correct operation, such as in the case of a biometric passport which needs to be readable at the departure and arrival port of two different international airports [30].

In the case of biometric systems, interoperability may not be desirable. Interoperable systems can pose a threat to personal data and its abuse, especially where biometrics are concerned. Silo-based systems hinder the interoperability of systems, limit the transfer of personal data and lessen the possibility of data abuse. A biometric smart card system which stores all the data used to compare live biometric readings to images on the card may be more secure than a system that requires live readings to be compared to a central database of metrics. However, many digital systems are moving towards interoperability and require the development of new security technologies to prevent fraud and theft [30].

Interoperability has also given rise to the use of digital IDs in a variety of applications, including mobile phone and global positioning system (GPS) technologies. The convergence between Internet, telephone and electronics has provided the medium for mobile services. It has allowed mobile numbers to act as individual identifiers which communicate with the service operator as long as the device remains powered [46]. One important application of this is the provision of location based services (LBS) which provide a great deal of convenience for the customer and can invade privacy in a multitude of ways. When this is coupled with a national ID scheme, the government and other authorities can easily monitor an individual with extreme accuracy [47].

Examples of LBS include using mobile phone signals to provide real time traffic data, and delivering targeted ads to mobile devices using geographical information. The proliferation of mobile technologies has provided a way for advertisers to remain digitally connected to customers all day, in an extremely personal way. In another example, GPS mapping technologies can provide destination directions and suggest places to dine while traveling. In this scenario, a free service is provided and an advertisement is delivered. The convergence in this mobile world mimics that occurring Internet-wide and requires the same identity management mechanisms to protect citizens and privacy [48].

One major difference between mobile and fixed technologies is that mobile devices can be used to explicitly locate and track individuals, which can have negative implications for privacy and civil liberties. Furthermore, data protection and fair information practices legislation such as PIPEDA protect against the processing of personal information, but do not address the issues of mobile services and tracking in an explicit manner [46]. Unlike Internet-based applications, mobile tracking services are based on control. They can be used by law-enforcement to track criminals, by parents to track their children in order to lessen the risk of harm, by care-givers to ensure infirm patients remain safe and by commercial organizations to control what type of advertisements are sent to potential customers. The implications of these control situations, whether altruistic or criminal, pose a threat to a person's civil liberties and privacy [21].

Policies which regulate the use of interoperable and convergent technologies need to balance the threat these technologies pose to privacy with the threats to security they help alleviate. Control, trust, privacy and security are the main factors involved in this policy analysis. For instance, increased control can diminish an individual's trust. In the case of an advertiser's increased intrusiveness, too much control will deter the consumer from trusting or buying products from the advertising company [48].

The need for security and privacy usually develop into competing interests. Risks to privacy include continuous surveillance of citizens, susceptibility of data storage technologies to hacks, and function creep where data is used for unintended purposes without the citizen's knowledge. Where security is concerned, the risks are opposite to those associated with privacy. Security risks occur when authorities have limited knowledge of a person's activities and vulnerabilities in their control provide a motive to commit crimes [48]. The possible solution to these competing interests is to develop policy which seeks to balance privacy protection with commercial and law enforcement interests.

5. Policy Recommendations and Discussion

5.1. Central Question Revisited

Smart cards, biometrics, RFIDs, location based services, computer technologies, data management solutions, and digital ID management systems all have a role to play in defining the current notions of security and privacy. The designers and regulators of these technologies must ensure that the mistakes of the past are not repeated. The root of the issue concerns the decision-maker's understanding of the technology. Many times, the implications of the technologies being considered are poorly understood. This has been evident throughout history and its repercussions have been far reaching. According to Ellul, "… once man has given technique its entry into society, there can be no curbing of its gathering influence, no possible way of forcing it to relinquish its power. Man can only witness and serve as the ironic beneficiary-victim of its power" [49]. It is therefore vitally important that ID technologies be fully understood in terms of their social, ethical and financial impact before being implemented on a global scale.

The central question posed in this inquiry asks "**How can a person's digital identity be managed and protected?"** Three anticipated findings were investigated. Physical identification technologies, digital ID management software, policies and legislation were explored as methods which could be utilized to manage and protect identity. In all three cases there were both positive and negative aspects to the implementation of these technologies as identity managers and protectors. The evidence indicates that less consideration has been given to the social implications of identity technologies than to their technical, commercial, financial and political applications, creating a policy gap [48].

Most of the laws developed between 1970 and 2000 are based on an outdated technology context that did not foresee some of the technological advances that have come about since. Although attempts to address this have resulted in technology neutral legislation, such as

PIPEDA, new forms of data and the conversion of once anonymous transactions into identifiable ones, are not covered. Examples of this include the use of mobile devices for delivering targeted advertisements and new surveillance techniques that nearly eliminate the anonymity that the internet once provided. These new technological contexts have the potential to turn the majority of law abiding citizens into potential suspects under continuous observation and monitoring. Adding to the complication of this policy gap is the introduction of legislation that facilitates the invasion of privacy and the removal of civil liberties in the name of counter-terrorism [46].

A great deal of evidence indicates that this policy gap allows for an array of privacy invasive scenarios. Data-matching analyses a person's behaviour patterns and compares them against templates which can be used by governments to track citizens and by businesses to influence purchasing decisions. Tracking data can be used as circumstantial evidence by law enforcement to discourage criminal behaviour, but can also lead to an increase in wrongful convictions due to questionable digital evidence [46]. Furthermore, the lack of regulation could lead to an Orwellian scenario in which governments limit the freedoms of individuals, especially in non-democratic countries, or corporations use technologies to silence regulators, activists and whistleblowers. Ultimately, the question of whether a citizen should have the right to be anonymous accompanies the analysis of the central question. In this new digital milieu, national security, customer convenience and corporate efficiency are used to justify the suspension of a citizen's anonymity.

5.2. Policy Recommendations

Much of the research on identity technologies leads to negative and gloomy conclusions about the future of identity management; however, a growing body of evidence indicates that the positive benefits of identity technologies can be realized in the right policy context. Progress needs to be made in a variety of areas to extract the potential benefits, including transparency and accountability, privacy-security balance, and the business case for privacy enhancing technologies (PETs).

5.2.1. Transparency and Accountability

Citizens and consumers have a right to know how their information is being used and when it is subjected to a security breach. PIPEDA legislation includes effective and proactive compliance tools to educate citizens, audit those suspected of privacy breeches and publicize information on those who do not comply with the legislation; however, these tools are seldom utilized. When a significant threat to personal data occurs, PIPEDA should mandate, rather than recommend, that customers be notified. This will provide incentive for organizations to better manage the protection of their data [43].

Blanket consent is another area in which the legislation needs to be improved. Unclear legal terms in corporate privacy policies and the granting of consent only once, at the creation of a profile, does not transparently convey to the customer how their data will be used. Furthermore, the government should also be subject to PIPEDA legislation, just as the private sector is. The exception that the government and law enforcement agencies can use citizen data without consent makes the legislation less effective [42].

Education programs and advertising campaigns are required to create awareness for privacy and security issues amongst the public. A large percentage of the population is unaware of the potential privacy invasiveness of some technologies. The designers and developers of these technologies need to understand the privacy and security implications that exist. Law enforcement agents should be aware of the implications of their work and in some cases, the identity information collected without the user's knowledge should be inadmissible in court, if that data has been subjected to function creep [46].

5.2.2. Privacy-Security Balance

Network based, automated services have changed the commercial, government, health and financial services industries, creating a shift from a product oriented society to a service oriented one. For instance, music records and CD products are being replaced by digital files. This has radically altered the music industry, called into question the digital rights to creative art and changed the way retailers sell music. The changes occurring in service provision have a common thread in that they no longer require a human to establish trust and initiate the transaction. Automated processes have become the key mediators of transactions between parties, continuously taking over a role that humans once had. Establishing and enforcing trust in these transactions is the key to successfully mitigating the technical issues encountered with digital relationships [3].

Technological standards that are created using a multi-stakeholder approach can establish a balance between privacy and accountability through trust. Standards should encompass the needs of technology developers, users, government legislators, law enforcement and commercial interests. Agreed upon standards should be developed before the privacy-invasive technologies are produced so that all stakeholder concerns will be represented in the final design. This type of consultative and transparent process will alleviate customer concerns that technology policy represents the narrow needs of national security and commerce at the expense of citizen freedoms [21].

Standards build upon transparent dialogue and design lead to privacy embedded platforms, such as the metasystem concept. Many consumer convenience technologies can be designed with privacy embedded, but are not, due to the strong lobby from commercial and law enforcement interests. For this to change, designers of the technology must be aware of

privacy issues. The concept of pseudo-anonymity can be useful to solving the privacy-security dichotomy and meeting the needs of all stakeholders [48].

Many personal information protection laws seek to obtain consent from a user before information is used, but do not include for the creation of multiple personas which protect the user from all surveillance, including that by the government. While legislation assumes the benevolence of government, privacy-embedded technologies and networks give the user true control of their identity information and protect them from all forms of surveillance, when it is required. However, at times, users will have to relinquish some of their anonymity to obtain services, such as e-government services, banking services or while on-line shopping. Organizations would also be able to reveal a person's identity in certain circumstances when fraud or criminal intent is evident. Legal protections will be required to ensure the effectiveness of pseudo-anonymity and to regulate its use and possible abuse by law enforcement. [44].

The privacy-security dichotomy can also be mitigated by the recognition that identity technologies are not perfect. The security of these systems can be compromised and identity information exposed which can destroy an organization's reputation. Furthermore, interoperability and convergence can have severe implications for data matching and data theft. Policy makers and corporations must be made aware that technology-only solutions cannot protect identity or commercial interests without social considerations and regulation [18]. An awareness campaign highlighting the potential for detrimental social change and the loss of on-line business due to privacy infringement could be developed by the privacy commissioner's office.

Similar to the case of corporate sustainable development, where corporate compliance with the law is concerned, over-compliance can have major benefits to the corporation and the general public. Privacy governance can increase positive customer relations, avoid regulatory non-compliance issues, reduce lawsuits, prevent bad publicity, and avoid government investigations [50]. On the downside, when corporate over-compliance is used as a public relations tactic which tries to highlight the benefits of technologies while ignoring their privacy implications, it can be harmful to all stakeholders. For example, technological developments such as emergency locators in mobile devices which have obvious tracking and commercial applications are promoted solely for their safety features. Furthermore its convergence with the mobile Internet is progressing in a manner that is largely unregulated [46].

5.2.3. Developing a Market for Privacy Enhancing Technologies (PETs)

Recently, companies have been developing technologies that are designed to protect a user's privacy by providing a platform for performing anonymous, untraceable transactions. As the public becomes more aware of the dangers associated with privacy invasive technologies, the market for PETs will grow stronger creating a business case for privacy protection and encouraging corporate interest in large scale development. These technologies can also be

used for maintaining true pseudo-anonymity in transactions, which could aid in the search for a balance between privacy and security. Corporations and governments need to facilitate the development of these technologies to meet the market demand and protect citizens [46].

According to Beslay and Clements [21], “privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century”. The solutions required to solve the problems with managing and protecting identity centre on balance, trust and accountability. These elements contribute to the privacy-security dichotomy which must be addressed, along with the need to defend basic citizen rights while legitimizing commercial activities. More effective government regulatory mechanisms will be required along with more transparent and accountable self-regulatory governance policies in industry.

In essence, the key stakeholders in the digital identity debate need to find a balanced way to protect democratic rights and security without infringing upon those rights. Furthermore, a universal definition of digital identity is required to ensure legislative and regulatory measures are harmonized world wide. This should be accompanied by the granting of a universal right to anonymity and pseudo-anonymity for all citizens of the planet. In order to develop these elements, legislation, monitoring methods and systems of accountability must be implemented in the design of technologies and policies. These designs can encourage the trust and confidence of citizens in identity management systems which are required to ensure that the digital economy realizes its full potential [21].

6. Appendix A: A History of Identification Cards

Throughout recorded history schemes and technologies have been used to identify and categorize people. At times this categorization was justified and useful, such as the registration of citizens for census purposes by the Romans. In many more instances, identification techniques such as tattooing and branding were used to oppress certain segments of the population. It is important for the architects of modern identification schemes to understand the possibilities of abuse that exist, in order to ensure the protection of a person's privacy and freedom. ID schemes created without full understanding of their social implications has been the cause of much abuse in the past [9].

The industrial revolution gathered large groups of people together in urban environments allowing them to be close to their employers and families. As these urban centres developed, it was necessary to automate the identification process. Advanced data collection technologies such as the punch card introduced automated processing of citizen information with unparalleled speed and accuracy. Birth certificates and social insurance number cards are examples of documents invented to provide proof of identity and prevent fraud. They allow governments to engage in more large scale data collection and analysis, and help distribute social services to citizens according to their need. The increase and centralization of government services and the need for protection of citizen identity from identity thieves drove technological improvements over the years [9].

These manual identification systems laid the foundation for the creation and study of Information Systems. As the microprocessor found its way into many different applications, it became the technology that best fit the information processing requirements of centralized record keeping. Soon after, magnetic storage drives and sophisticated data management and matching software were developed to handle the processing needs of the industry. Digital processing allowed for better handling and cross checking of fraudulent claims. It also allowed other groups such as corporations, banks and retailers to begin processing information. By the 1980s data processing, storage, cross checking and linking between government agencies, banks and businesses gave birth to the concept of automatic identification. Computers became the primary authenticators of claims to identity by electronically matching names and social security numbers with other official, centralized documents [9].

The next evolutionary step involved eliminating the manual entry of data into the computer. Barcodes, magnetic strips and later, smart cards, became an efficient, error reducing strategy to supplying identifiers to the processing computer systems. The ID process became fully automatic and rapidly led to the adoption of ID systems in almost every industry including the bank card, ATM card and credit card. In some of these cases, an authenticator is required in the form of a PIN (personal identification number). The applications of these new technologies are numerous and have far reaching implications. In the modern digital age, new issues are emerging which include improving the security of ID technology and consolidating ID cards, in order to simplify interactions with government and retailers.

7. Appendix B: What is Web 2.0?

Web 2.0 is a set of philosophies, technologies and strategies that have become a prevalent force in creating a more interactive user environment on the Internet. Web 2.0 sites share common characteristics in that they are web-based, funded through advertising dollars, foster collective intelligence (where users add value through collective sites such as wikipedia) and undergo continuous growth rather than software updates. The centerpiece of this strategy is the web community and its associated commercial applications which depend on digital identity to provide their services [10, 12].

Core Competencies of Web 2.0 Companies

According to Tim O'Reilly [12], Web 2.0 solutions share these common characteristics which set them apart from other sites on the Internet.

- Service-orientated, not packaged software, with cost-effective scalability
- Provide control over data sources that get richer as more people use them
- Trust users as co-developers
- Harness collective intelligence
- Focus on customer self-service
- Software above the level of a single device
- Lightweight user interfaces, development models, and business models

Examples of Web 1.0 versus Web 2.0 [12]

Web 1.0	**Web 2.0**
DoubleClick	Google AdSense
Ofoto	Flickr
Akamai	BitTorrent
Mp3.com	Napster
Britannica Online	Wikipedia
Personal websites	Blogging
Evite.com	upcoming.org
Pblishing	Participation
Content management systems	Wikis
Directories (taxonomy)	Tagging ("folksonomy")

8. Appendix C: Data Trail and Monitoring

The following is taken from the Office of the Privacy Commissioner of Canada's Website [51]:

Fact Sheet: A Day in the Life ...or how to help build your Superfile.

Nothing to hide? It's just as well...from the time we get up in the morning until we climb into bed at night we leave a trail of data behind us for others to collect, merge, analyze, massage and even sell, often without our knowledge or consent.

8:30 Exit apartment parking lot — cameras, and possibly a card, record departure.

8:35 Pull onto toll highway — device records your entry and exit points to send bill at the end of the month.

8:42 Caught in traffic jam, call work to delay meeting — cellular phone calls can be easily intercepted; new personal telephones signal your whereabouts to satellites to deliver calls.

9:17 Enter office parking lot — card records entry and time, cameras monitor garage.

9:20 Enter main office/plant door — "Swipe" cards record comings and goings; active badges allow others to locate you anywhere in the building.

9:25 Log on to computer — system records time in.

9:29 Send personal e-mail to friend, business message to colleague — both can be read by the employer; simple deletion does not erase them from the computer's hard drive.

10:45 Call your mother — supervisors may monitor phone calls.

11:00 Make a delivery using company vehicle — many company vehicles have geo-positioning devices to plot vehicle location; some have "black boxes".

12:05 Stop at bank machine — system records details of transactions, cameras overhead or in machine record your behaviour.

12:10 Buy birthday gift for friend — credit card records details of purchase, retailer's loyalty card profiles purchase for points and directed discounts; banks may use spending patterns to help assemble complete customer profile.

12:35 Doctor's appointment — health cards will soon contain small computer chips to record your complete medical history on the card, blood samples contain DNA which could be tested for wide variety of conditions, doctor's diagnosis may need to be disclosed to insurance company if you buy life or disability insurance and details sent to centralized registry run by insurance companies.

1:15 Pick up prescription — some provinces have on-line drug networks which share your drug history with pharmacies across the province and may be disclosed to police tracking drug abuse.

1:30 Return to work — card records your return.

2:45 Provide urine sample for employer's new drug testing program — reveals use of targeted drugs but not impairment; sample may also reveal use of legal drugs such as birth control pills, insulin and anti-depressants.

3:30 Meeting in secure area — pass through security which scans retina to confirm identity.

5:30 Complete first draft of report — computer records content, can also store keyboard speed, error rate, length of pauses and absences.

6:15 Leave office — exit recorded by computer, entry system and parking lot.

6:30 Buy groceries — debit card purchase recorded, loyalty card tracks selections for marketing and targeted discounts.

6:45 Pick up video — computer records viewing preferences, Social Insurance Number; store may sell your viewing preferences to other companies.

7:20 Listen to phone messages — your phone has recorded callers' phone numbers, displays your number when you call others, unless you enter code to block the display.

8:20 Order clothing from catalogue — company records personal details and credit card number and may sell the information to database-list-marketers.

8:30 Subscribe to new magazine — many magazines routinely sell their subscribers' list to mass mailers.

8:35 Survey company calls — company gathers political views, social attitudes and personal views. Some surveys are actually marketing calls to collect personal data for future sales. Legitimate surveys destroy personal identifiers once data processed.

8:45 Political canvasser at the door — political contributions of more than $100, amounts and the party, are listed in public records.

9:10 Log onto Internet — your choice of chat groups and your messages can be monitored and a profile assembled by anyone, including police; some Web sites monitor your visits.

9. Appendix D: CSA Privacy Code

The following are the 10 principles comprising the CSA Model Code for the Protection of Personal Information (CAN/CSA-Q830-96):

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

10. Appendix E: Privacy Embedded Laws of Identity

LAW #1: PERSONAL CONTROL AND CONSENT

Technical identity systems must only reveal information identifying a user with the user's consent. Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both.

Consent must be invoked in the collection, use and disclosure of one's personal information. Consent must be informed and uncoerced, and may be revoked at a later date.

LAW #2: MINIMAL DISCLOSURE FOR LIMITED USE: DATA MINIMIZATION

The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution. It is also the most privacy protective solution.

LAW #3: JUSTIFIABLE PARTIES: "NEED TO KNOW" ACCESS

Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. This is consistent with placing limitations on the disclosure of personal information, and only allowing access on a "need-to-know" basis. Only those parties authorized to access the data, because they are justifiably required to do so, are granted access.

LAW #4: DIRECTED IDENTITY: PROTECTION AND ACCOUNTABILITY

A universal identity metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy. Unidirectional identifiers are used by the user exclusively for the other party, and support an individual's right to minimize data linkage across different sites. This is consistent with privacy principles that place limitations on the use and disclosure of one's personal information. At the same time, users must also be able make use of omnidirectional identifiers provided by public entities in order to confirm who they are dealing with online and, thereby ensure that that their personal information is being disclosed appropriately. To further promote openness and accountability in business practices, other types of identifiers may be necessary to allow for appropriate oversight through the creation of audit trails.

LAW #5: PLURALISM OF OPERATORS AND TECHNOLOGIES: MINIMIZING SURVEILLANCE

The interoperability of different identity technologies and their providers must be enabled by a universal identity metasystem. Both the interoperability and segregation of identity technologies may offer users more choices and control over the means of identification across different contexts. In turn, this may minimize unwanted tracking and profiling of personal information obtained through surveillance of visits across various sites.

LAW #6: THE HUMAN FACE: UNDERSTANDING IS KEY

Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks. This will advance user control, but only if users truly understand. Thus, plain language in all communications used to interface with individuals is key to understanding. Trust is predicated on such understanding.

LAW #7: CONSISTENT EXPERIENCE ACROSS CONTEXTS:

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. We return full circle to the concept of individual empowerment and informed consent. Clear interfaces, controls and options that enhance an individual's ability to exercise control across multiple contexts in a reliable, consistent manner will serve to enhance the principle of informed consent.
[44]

11. Appendix F: Smart Card Types

Smart cards come in many different forms. A contact card for commerce applications usually comes packaged in plastic with a gold contact on one side of the card to interact with the card reader. However, the circuit housing and card reader can be found in many different combinations. For instance, the circuit can be housed in a universal serial bus device (USB key) for use in a computer and in cell phones as a SIM card. In another implementation of the smart card, Radio Frequency Identification (RFID) technology is used as the communication medium rather than electrical contacts [25].

Above are the images of a contact smart card, a contactless RFID embedded tag and examples of stick-on RFID circuit tags [52].

12. Appendix G: The Digital Identity Web

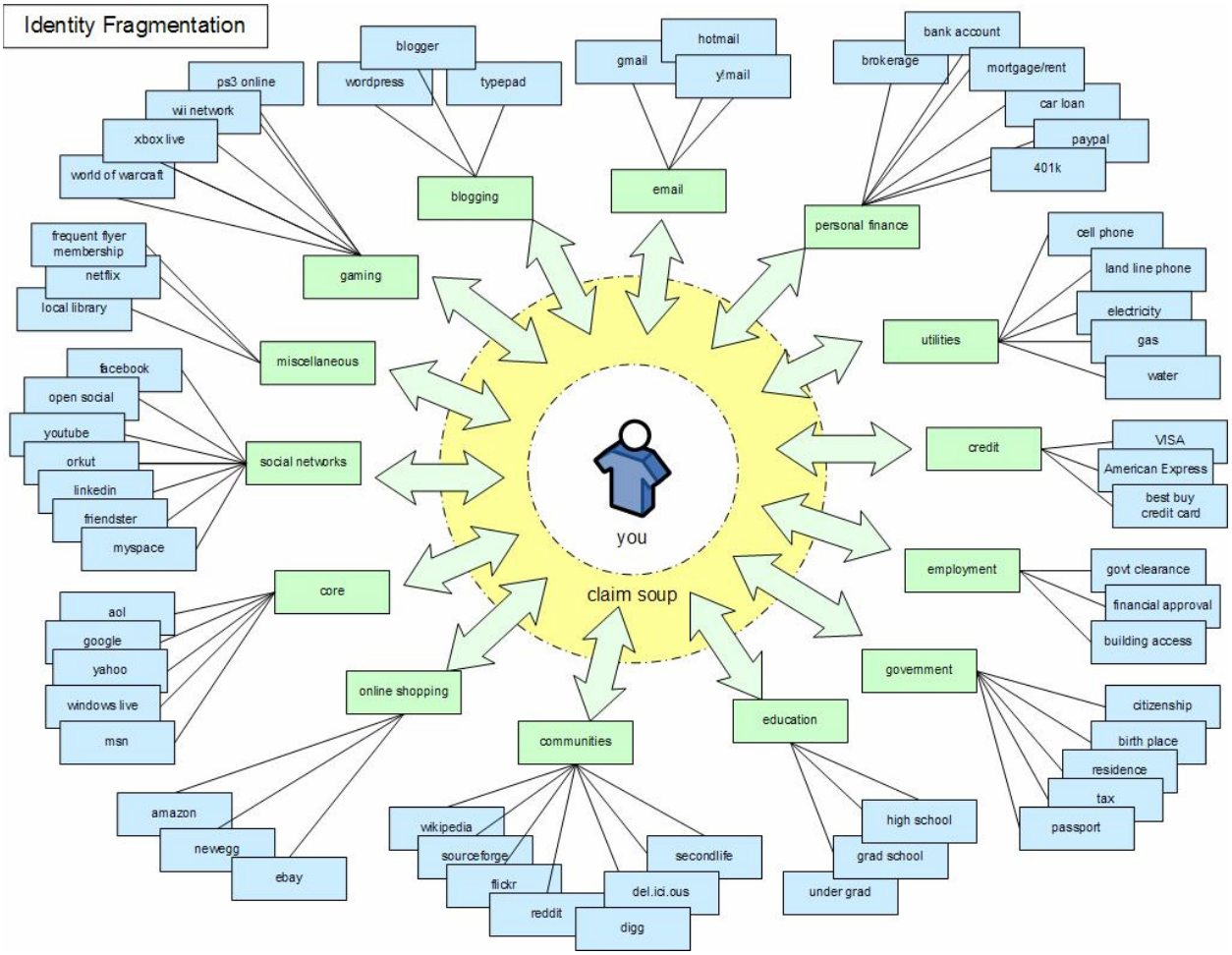


Figure 2: Fragmented Identity [53]

13. References

[1] T. M. Lenard and D. B. Britton, *The Digital Economy Fact Book: Eight Ediiton.* Washington, DC: The Progress and Freedom Foundation, 2006,

[2] K. Mills, "Cybernations: Identity, Self-determination, Democracy and the" Internet Effect" in the Emerging Information Order," *Global Society,* vol. 16, pp. 69, 2002.

[3] P. J. Windley, *Digital Identity: Unmasking Identity Management Architecture.* Sebastopol, CA: O'Reilly, 2004,

[4] J. Pato, "Identity management: Setting context," Hewlett-Packard, Cambridge, MA, 2003.

[5] P. Covell, S. Gordon, A. Hochberger, J. Kovacs, R. Krikorian and M. Schneck. (1998, Digital identity in cyberspace. Masatuchettes Insititute of Technology, Cambridge, MA.

[6] U.S. Homeland Security. (2007, Aug. 14, 2007). DHS US-VISIT: How it works. *2007(10/26/2007),* Available: http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm

[7] S. Petri. (1999), An introduction to smart cards -- part 1 of a two-part series. *Messaging Magazine (September/October),* Available: http://www.opengroup.org/comm/the_message/magazine/mmv5n5/SmartCards.htm

[8] A. Clement, R. Guera, J. Johnson and F. Stalder, "National identification schemes (NIDS): A remedy against terrorist attack?" in *Proceedings of the Sixth Conference on Human Choice and Computers HCC6,* 2002,

[9] K. Michael and M. Michael, "Historical Lessons on ID Technology and the Consequences of an Unchecked Trajectory," *Prometheus,* vol. 24, pp. 359-364, 2006.

[10] P. Giger, "Participation literacy. part 1: Constructing the web 2.0 concept," Blekinge Institute of Technology, Sweden, Tech. Rep. 2006:07, 2006.

[11] S. Clauß and M. Köhntopp, "Identity management and its support of multilateral security," *Computer Networks,* vol. 37, pp. 205-219, 10. 2001.

[12] T. O'Reilly. (2005), What is web 2.0. *2007(12/01/2007),* Available: http://www.oreilly.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=5

[13] Google. (2007), Welcome to AdSense. *2007(Oct/30),* Available: https://www.google.com/adsense/www/en_US/adsense_casestudy.html

[14] C. J. Bennett. (2001), Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology 3(3),* pp. 195. Available: http://www.springerlink.com/content/nj747m13l58450w2/fulltext.pdf

[15] Government of Ontario. Information technology: Making it happen. *2007(10/29/2007),* Available: http://www.gov.on.ca/mgs/en/IAndIT/STEL02_046928.html

[16] Canada Health Infoway, "2015: Canada's next generation of health care at a glance," Canada Health Infoway, Ottawa, 2006.

[17] P. Wood, "Implementing Identity Management Security - An Ethical Hacker's View," *Network Security,* vol. 2005, 2005.

[18] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns," *IEEE Security and Privacy,* vol. 1, pp. 33 - 42, 2003.

[19] K. R. Foster and J. Jaeger, "RFID Inside: The Murky Ethics of Implanted Chips," *IEEE Spectrum,* vol. 44, pp. 24-29, 2007.

[20] Anti-Phishing Working Group. (2007), Anti-phishing working group. *2007(10/31/2007),* Available: http://www.antiphishing.org/

[21] L. Beslay and B. Clements, "Privacy - Tomorrow's Bottleneck in the Information Society," *Communications and Strategies,* vol. 44, 2001.

[22] Google. (2007, Google privacy center: Privacy policy. *2007(10/30/2007),* Available: http://www.google.com/privacy.html

[23] R. Newbould and R. Collingridge. (2003), Profiling—Technology. *BT Technology Journal 21(1),* pp. 44.

[24] Amazon.com. (2007), Amazon.com: Help > privacy & security > privacy notice. *2007(10/31/2007),* Available: http://amazon.com/gp/help/customer/display.html/002-4137837-5161613?ie=UTF8&nodeId=468496#gather

[25] S. Zanero, "Smart card content secuirty," Politecnico di Milano, Milan, Italy, 2000.

[26] F. Corradini, E. Paganelli, A. Polzonetti, L. Forastieri and D. Settimi. Smart card distribution for E-government digital identity promotion: Problems and solutions. Presented at International Conference on Information Technology Interfaces.

[27] M. Rothman, "Public-key Encryption For Dummies," 2007, 1999. Available: http://www.networkworld.com/news/64452_05-17-1999.html

[28] C. Ellison and B. Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure," *Computer Security Journal,* vol. 16, pp. 1-8, 2000.

[29] R. Sanchez-Reillo, L. Mengibar-Pozo and C. Sanchez-Avilla, "Microprocessor Smart Cards with Fingerprint User Authentication," *IEEE Aerospace and Electronic Systems,* vol. 18, pp. 22-24, 2003.

[30] EU JRC, "Biometrics at the frontiers: Assessing the impact on society," Eurpean Commission Joint Research Centre, Seville, Spain, Tech. Rep. EUR 21585 EN, 2005.

[31] D. Graham-Rowe, "Privacy and prejudice: whose ID is it anyway?" *New Sci.,* vol. 187, pp. 20-23, September 17. 2005.

[32] Q. Xiao and M. Savastano, "An exploration on security and privacy issues of biometric smart ID cards," in *IEEE Workshop on Information Assurance,* 2007,

[33] D. Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.* New York: Routledge, 2003, pp. 287.

[34] K. Michael and M. G. Michael, "The social, cultural, religious and ethical implications of automatic identification," in *Seventh International Conference in Electronic Commerce Research,* 2004,

[35] T. Baier, C. Zirpins and W. Lamersdorf, "Digital identity: How to be someone on the net," in *E-Society* , vol. 2, P. Isaias and palma dos Reis, A., Eds. Lisbon, Portugal: IADIS Press, 2003, pp. 815-820.

[36] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Second ACM Workshop on Digital Identity Management DIM '06*, 2006, pp. 11-16.

[37] P. Bramhall, M. Hansen, K. Rannenberg and T. Roessler, "User-Centric Identity Management: New Trends in Standardization and Regulation," *IEEE Security and Privacy,* vol. 5, pp. 84-87, 2007.

[38] N. J. Hoover. (2007, Sept. 22). Analysis: Social networks may become interoperable. *2007(11/8/2007),* Available: http://www.informationweek.com/news/showArticle.jhtml?articleID=201808173

[39] Privacy International. (2007, Sept. 6). A race to the bottom - privacy ranking of internet service companies. *2007(11/8/2007),* Available: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961

[40] M. Casassa Mont, P. Bramhall and J. Pato, "On adaptive identity management: The next generation of ID management technologies," Hewlett-Packard, Cambridge, MA, 2003.

[41] C. A. Ardagna, E. Cremonini, S. Damiani and P. Samarati, "Towards identity management for E-services," in *TED Conference on E-Government. Electronic Democracy: The Challenge Ahead,* 2005,

[42] J. Stoddart, "PIPEDA review discussion document: Protecting privacy in an intrusive world," Office of the Privacy Commissioner of Canada, Ottawa, 2006.

[43] C. Berzins, "Three Years Under the PIPEDA: A Disappointing Beginning," *Canadian Journal of Law and Technology,* vol. 3, pp. 113-126, (2004).

[44] A. Cavoukian and F. Carter, "7 laws of identity: The case for privacy-embedded laws of identity in the digital age," Office of the Information and Privacy Commission of Ontario, Toronto, ON, 2006.

[45] K. Cameron. (2005, Microsoft's vision for an identity metasystem. *2007(Nov/22),* Available: http://www.identityblog.com/stories/2005/07/05/IdentityMetasystem.htm

[46] R. Clarke. (2001, Person location and person tracking: Technologies, risks and policy implications. *Information Technology & People 14(2),* pp. 206.

[47] G. Roussos, D. Peterson and U. Patel, "Mobile Identity Management: An Enacted View," *International Journal of Electronic Commerce,* vol. 8, pp. 81-100, 2003.

[48] L. Persuco, K. Michael and M. G. Michael, "Location-based services ad the privacy-security dichotomy," in *3rd International Conference on Mobile Computing and Ubiquitous Networking,* 2006, pp. 91-98.

[49] J. Ellul, *The Technological Society.* New York: Vintage Books, 1964,

[50] R. Herold, "Building an Effective Privacy Program," *EDPACS,* vol. 33, pp. 9, 2005.

[51] Privacy Commissioner of Canada. (2001, Fact sheet: A day in the life - privacy commissioner of canada. *2007(12/12/2007),* Available: http://www.privcom.gc.ca/fs-fi/02_05_d_01_e.asp

[52] Wikipedia Contributors. (2007, Radio-frequency identification. *2007(12/12/2007),* Available: http://en.wikipedia.org/wiki/radio-frequency_identification?oldid=177377421

[53] K. Cameron. (2007, Feeling fragmented? Available: http://www.identityblog.com/blog.php/#post-893