Guided Literature Review:

Identity Management Systems

jennifer barrigar

Commissioned by the Office of the Privacy Commissioner of Canada

February 2011

Table of Contents

Background 1
Caveat: Analogizing the Payments System and Identity Management Systems 1
Mandate 1
Introduction 2
Background: Identity Management Systems 2
Literature Review: Themes 5
Interrogating the User 5
Security / Safeguards 8
Data Sovereignty / Globalization 9
Governance / Regulation 10
FIdM Systems and Canada 12
Conclusion 12
Appendix A 13

Background

A Payments System generally, and the Canadian Payments Landscape specifically, may be thought of as the overarching structure within which consumers, businesses, merchants, financial institutions, payments networks, regulators, processors, new entrants and service providers intersect as they initiate, process, receive or regulate transfers of value within the system.

The [Canadian] Task Force for the Payments System Review was formed in June 2010 by the Department of Finance Canada. Their objective is to review the existing Canadian Payments System and to provide recommendations to the Department of Finance. It was felt that such a review was necessary in light of technological and technosocial change and its potential impact on both the use and scope of the payments system. Accordingly, the Task Force was asked to: (1) map the existing Canadian payments system; (2) detail the roles of all players; (3) identify the various regulatory regimes that govern participants; (4) discuss trends and significant changes over recent years; (5) elucidate on any new and/or emerging payment types that have not previously been covered in detail. This project was, to some extent, preliminary, a first step in a process that should ultimately move through a public consultation and into recommendations for any changes deemed necessary or desirable.

Caveat: Analogizing the Payments System and Identity Management Systems

It should be noted that this review does not contend that the Canadian payments system is itself an identity management system. If we define the payments system as being inherently complex, having multiple payment options, multiple players with sometimes divergent goals, overlapping or non-existent regulatory regimes and evolving consumer choice, however, it becomes evident that the Canadian payments system must be understood as mirroring or at least analogous to the larger topic of identity management systems.

OPC has identified identity management as one of its priorities for this year, and it is my understanding that they hope to develop and release some kind of best practices/public education materials about identity management systems. In order to maintain consistency of position/analysis, therefore, OPC requested this literature review focus more broadly on identity management systems rather than strictly on the payments system.

Mandate

The Office of the Privacy Commissioner (OPC) intends to participate in the review process. It is my understanding that the Privacy Commissioner has already made representations to the Task Force on the integral role that privacy must play in any such examination, but intends to provide further written comments. To this end, they have requested a quasi-guided literature review be prepared, focussed on identity management issues.

At the end of the review, the researcher had two deliverables →: (1) a written guided literature review on identity management systems; and (2) a follow-up discussion with OPC staff in order to review both the document and potential OPC positions with regard to identity management.

Accordingly, this document reviews (1) the documents identified by the OPC as integral to such a project; and (2) other relevant documents.

Introduction

Reviewing selected information about Federated Identity Management Systems (FIdM), it quickly becomes clear that this technology has an almost Schrödinger[1] – ian quality to it – that is, online identity management, by virtue of potentially falling into either state, may be said to be simultaneously incredibly beneficial and terribly detrimental.

A properly designed and implemented FIdM system has, in theory, the capacity to enhance privacy, facilitate meaningful anonymity, and subvert behavioural tracking. Equally possible, however, is the risk that an improperly designed and implemented FIdM system could exacerbate existing problems and, by virtue of creating a new repository of data and process of sharing, create new ones.

Background: Identity Management Systems

Although recent discussion of identity management has tended to focus on the problems leading to and potential benefits of creating online identity management protocols or systems, it is in fact important to recognize that identity authentication and trust are not issues unique to online environments.

Traditionally, communities were small and localized. This meant that participants in a relationship were likely to know each other and thus there was little uncertainty. Even where participants might not directly be acquainted, small communities meant that each individual's social and kinship connections were known to some degree, and so although technically a stranger, the individual was still "known" in some fashion that reduced uncertainty. Indeed, not only would the individual be "known", but as a member of a shared community they could be expected to adhere to a set of recognizable norms. This, in turn, led to trust.

Trust itself is an extremely nuanced term, with multiple definitions. The two most relevant for our purposes here are: "Assured resting of the mind on the integrity, veracity, justice, friendship, or other sound principle, of another person; confidence; reliance; reliance" and "Assured anticipation; dependence upon something future or contingent, as if present or actual; hope; belief."[2] Essentially, trust allows us to feel confidence in the reliability of another, and/or to therefore trust that the desired outcome will be achieved.

As societies progressed and became more complex and more dispersed, however, it became less possible to rely on co-presence and extended relationships, and thus trust became more difficult. The lack of co-presence did not correspondingly decrease the need to make such assessments – if anything, it increased it. As

---

[1] Schrödinger's Cat: A cat, along with a flask containing a poison and a radioactive source, is placed in a sealed box shielded against environmentally induced quantum decoherence. If an internal Geiger counter detects radiation, the flask is shattered, releasing the poison that kills the cat. The Copenhagen interpretation of quantum mechanics implies that after a while, the cat is *simultaneously* alive *and* dead. Yet, when we look in the box, we see the cat *either* alive *or* dead, not both alive *and* dead.

[2] trust. (n.d.). *Webster's Revised Unabridged Dictionary*. Retrieved October 30, 2008, from Dictionary.com website: http://dictionary.reference.com/browse/trust.

societies become increasingly complex and more dispersed, however, it became less possible to rely on co-presence for the derivation of assessments, and thus co-presence began to give way to other markers of trust.

> Modes of interaction began to alter radically in modern times, as transport and communication allowed people to be more mobile, and social institutions helped to mediate their relationships. So the signature, for instance, became more important as a guarantee of legitimate identity and was accepted by organizations such as banks. These organizations extended the range of human actions, as did artefacts such as the telephone, so that more and more could be done at a distance without the co-presence of bodies in relation. A token of trust, such as a personal identification number, became a proxy for the kind of trust that arises from an ongoing relationship of co-present persons.[3]

Proxies for co-presence are only half the equation. If co-presence creates trust because it allows people to rely on their own assessment(s) of the other, then a proxy that confirms the identity of an individual still leaves open the question of how to make an assessment of trustworthiness of that authenticated individual. As Stephen Nock writes:

> When we make a purchase, for example, we do so from strangers, who need some token to show that we can be trusted and have the resources to pay. But this raises acutely the question of who can be trusted if the stranger – or the institution – has not had the opportunity personally to check the reputations, credentials and credibility of those with whom they must nonetheless interact day to day.[4]

Just as the waning of co-presence required the development of proxies, so too does the increasingly anonymous (and anonymized) urban technological culture necessitate some new form of identification/identifiability.

As David Lyon remarks:

> Since the 1960s, bodies have been disappearing at an accelerating rate. Communication and information technologies enable not only fax and fixed phone communication, but also email, credit card transactions, cellphones and the Internet. This means that many other relationships become possible without co-presence. Bodies and personal experience part company, and a significant portion of that personal experience is social. The ties that bind are not electronic cables or satellite signals themselves, but they are increasingly mediated by electronic means. As the spread of such relationships picks up speed, so too does the quest for substitutes for traditional modes of integration.[5]

Perhaps it is understandable then, recognizing that mere geographic dispersal necessitated the creation of and reliance upon credentials as proxies for identification and authentication, that the increasing participation on and reliance upon online interactions for personal, commercial and even governance reasons similarly creates a need for some system of identity claiming, authentication and authorization. Thus, when we speak of Identity Management (IdM), we are speaking of such a system,[6] where "identity" means "a claim or set of

---

[3] David Lyon "Surveillance Society: Monitoring Everyday Life" (Open University Press, 2001) at 15
[4] Stephen Nock, cited in Lyon "Surveillance Society" at 21
[5] Lyon "Surveillance Society" at 16.
[6] Center for Democracy & Technology, "Issues for Responsible User-Centric Identity", November 2009, v. 1.0, <http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf>, at 1

claims about the user",[7] authentication is the process by which some level of confidence about the claim may be established,[8] and authorization is the granting of permissions of privileges to the authenticated identity.[9] A federated IdM (FIdM) is simply one where service providers are able to rely on trusted third parties selected by the user to authenticate services on the user's behalf.[10]

Traditionally, this has taken place on a 1:1 basis that is, between a service provider and a user. While this may have sufficed provisionally, with the expansion of users, of service providers and of information requests and provision, user profiles have multiplied, creating disadvantages for both users and organizations. For users, multiple log-in screens, passwords and identifiers to remember, and various levels of information demand and provision for each access are inconvenient and time-consuming. Organizations, on the other hand, struggle both the costs of managing and storing those profiles[11] and redundancy of the profiles themselves.[12]

Although there may be multiple players, at its most basic there are four (4) essential entities within a FIdM:

> USER: the end user who wishes to interact with an online service
>
> USER AGENT: Typically a browser, this is the means through which the user conducts the interaction
>
> SERVICE PROVIDER/RELYING PARTY (SP/RP): The online application or service with whom the user wishes to interact and who requires some certainty about the user prior to such an interaction, and
>
> IDENTITY PROVIDER (IdP): A web-based entity that conducts the authentication process and/or stores User information. This information may be shared in various ways with different RPs. Some FIdM's allow for multiple IdPs to exist within a 'circle of trust'.[13]

Just as there may be one of many IdP's, so too are there a variety of mechanisms recognized within the literature for structuring a FIdM →: three (3) that are universally recognized, with a fourth (4th) increasingly being added to the list.

1. An operating system-based IdM system, such as Microsoft's Cardspace;[14]
2. An omni-directional and scalable system such as OpenID, which is grounded in open source;[15]

---

[7] CDT at 2
[8] Clarke: Sufficently Rich Model of (id)Entity, Authentication and Authorization http://www.rogerclarke.com/ID/IdModel-1002.html#MAc
[9] Clarke
[10] CDT at 2
[11] Especially in jurisdictions which have privacy and/or data protection legislation which imposes obligations on the organization with regard to that information.
[12] G.-J. Ahn & J. Lam, "Managing Privacy Preferences for Federated Identity Managemetn", in V. Atluri, P. Samarati, & A. Goto, *Chairs*, (2005) *Digital Identity Management '05: Proceedings of the 2005 ACM Workshop on Digital Identity Management* 28, <http://portal.acm.org/citation.cfm?id=1102492>, at 28
[13] S. Landau, H. Le Van Gong, & R. Wilton, "Achieving Privacy in a Federated Identity Management System", in R. Dingledine & P. Golle, *Eds.*, (2009) 5628 FC LNCS 51, <http://www.springerlink.com/content/b149n4u255u3n378/fulltext.pdf>. at 64
[14] E. Maler & D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management", (2008) March/April *IEEE Security & Privacy* 16, <http://www.xmlgrrl.com/publications/IEEESecPriv-MarApr2008-MalerReed-Venn.pdf>, at 22
[15] Maler & Reed at 21

3. Security Assertion Markup Language (SAML) as used by the Liberty Alliance protocols and which provides perhaps the most diverse and comprehensive IdM metasystem;[16] and arguably
4. Social Network Sites, which are increasingly (especially in the case of Facebook and Twitter) coming to function as de facto identity providers for multiple RPs.[17]

Literature Review: Themes

In attempting to create an overview of the literature perused, 4 major topics have been identified:

1. Interrogating the User
    a. User-centric design
    b. Anonymity, pseudonymity and de-identification
2. Security / Safeguards
3. Data Sovereignty / Globalization
4. Regulation

This guided literature review makes it evident that the literature around IdM and FIdM does not provide any easy solutions. Indeed, the perspectives seem inevitably to resolve into dichotomous views on each of the identified themes.

Interrogating the User

User-Centric Design

In articulating the benefit of FIdM for individual users, the user-interface and the affirmation of user informational self-determination are often put forward. User-centric identity or design in a system allows the individual user the power to control (access to) their identity credentials just as we do in the offline world, holding our own identity tokens and choosing which one to present and to whom.[18]

At the user interface level, this is expected to result in pronounced improvements in efficiency and ease of use for the user →. S/he is able to demand and expect solutions that are easily understood and accessible, the process is streamlined by minimizing or erasing the requirement that users manage multiple logins and passwords for their various desired services.

By approaching FIdM from this user-centric perspective, individuals are (theoretically) accorded the power to conduct transactions online without sacrificing their privacy, whether they transact with one or many service providers. Not only is the user able to deal with multiple service providers, but ideally there will be no single central identity provider, but rather a variety of them offering diverse services, allowing individuals to select one or many providers to best meet their needs. Such competition, it is argued, not only facilitates user

[16] Landau et al
[17] M. Melanson, "Facebook Wants to be Your One True Login", ReadWriteWeb.com, February 10, 2010, online: <http://www.readwriteweb.com/archives/facebook_wants_to_be_your_one_true_login.php>. See also CIPPIC Comments on OPC Draft Report on the 2010 Consultations on Online Tracking, Profiling and Cloud Computing at 12
[18] CDT at 2

choice but may also enhance security and privacy awareness on the part of identity providers with market competition functioning to encourage and enhance these protections. Within the relationships with individual identity providers, user choice continues to be facilitated, with the user able to select the desired level of credential to be provided to a given service provider without fear of uniquely identifying herself unless s/he so chooses.

Beyond the micro level of user choice, user-centric design continues to benefit the individual user, argue its proponents. The system facilitates security via strong identification and authentication for transactions, as well as providing a secure repository for user information.

User privacy is also facilitated, because keeping the user information in a secure repository protects the user privacy by preventing service providers from collecting, using or sharing personal information beyond that which is required while also working to ensure that information is not linked or linkable from various sources unless or until the user desires it to be.

Unfortunately, the analogy to offline identity tokens carries through into both the positive and the negative →. User-centric design may facilitate user control, but in so doing it may also negatively impact users and prove to be a burden.

First, the interface itself must be useable and it should be accessible. Recognizing that some current systems require the user to leave a webpage to sign in elsewhere, it is suggested that a user-centric approach would include a consistent interface both for ease of use[19] and to reduce opportunities for phishing attempts.[20] Consistency should not, however, become synonymous with oversimplification so that users are not making rigorous decisions.[21]

In order for user information self-determination to be meaningful, users must not simply be able to make choices, but must be able to make informed and knowledgeable choices[22]. As various studies have shown, this is not always the case. First of all, the default setting on the any interface will be strongly determinative of user selections →. Users are far less likely to opt-out of a default than they are to opt-in to something different. Thus, where the defaults are privacy and security protective, then users will be most likely to stay at that level or even customize the levels to provide higher levels of security and privacy. Experience with social network sites and various other online entities suggests, however, that a privacy-protective default is not necessarily to be expected. Other studies have explored user comprehension of privacy policies and terms of use agreements, and demonstrated that many users do not read such documents, and even among those who do the documents are often phrased inaccessibly, leaving the user with a confused or incorrect understanding of the parameters of the agreement. Finally, the user must have access to the FIdM policies and procedures as well as to her own information in order to crystallize the meaningfulness of her consent.[23]

Even where comprehension is not an issue, others have pointed out that while in theory this kind of user micro-control over information is a positive thing, in actual fact it can lead to a kind of determinative paralysis,

---

[19] Maler & Reed at 21

[20] R. Dhamija & L. Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges", (2008) March/April *IEEE Security & Privacy* 24, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4489846> at 27

[21] Dhamija & Dussault at 26

[22] Landau et al at 64

[23] K. Cameron, "The Laws of Identity", May 12, 2005, Kim Cameron's Identity Weblog, <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>, at 6

a situation where the user is so overwhelmed by choices that s/he becomes unable to make any. Even where paralysis doesn't result, far from facilitating information self-determination, the existence of and responsibility for multiple choices may result in the user coming full-circle and feeling burdened by the very system that purported to streamline her online relationships.[24]

Anonymity, Privacy and De-Identification

Binary opposition can also be seen in the literature in relation to the role of anonymity, privacy and de-identification. Interestingly, this opposition seems to be grounded not so much in a critique of FIdM itself, but rather in fundamental conceptions of the Internet. That is, where Cameron argues that identifiability is an essential component that was sadly (the implication is) missed by the original Internet architects and must therefore be lateralled in,[25] others see the lack of an identification mechanism as fundamentally liberatory[26] and perhaps even integral to what Zittrain has termed "generativity".[27]

This difference at such a fundamental level cannot help but shape the different approaches to issues around anonymity, privacy and de-identification. Interestingly, however, the shape that this influence takes is quite different from what might be expected. Indeed, those who are pro-FIdM are in fact those who are invoke pseudonymity as a positive thing facilitated by FIdM, arguing that it becomes an important tool to protect privacy and thwart data mining, interception, and data linkage.[28] In order to make this meaningful, however, the controls for each pseudonym must be sufficiently granular to allow the user to select different levels of tracking, protection etc. Similarly, some authors continue to put forward technologies and strategies for anonymization or de-identification as a legitimate step in the management of information.[29]

Conversely, others argue that a presumption about the immunizing effects of anonymization and/or de-identification has had a negative effect on privacy, resulting in regulatory approaches that focus on identifiability and exclude from their scope information that has been presumptively stripped of identifiability.[30] Even where the presumptive efficacy of anonymization and/or de-identification has not impacted the scope of privacy law, some argue that the language of anonymization/de-identification creates its own dangers on multiple levels, seeming to absolve organizations from their responsibility to safeguard and treat information appropriate, while simultaneously encouraging or at least potentially encouraging

---

[24] B. Masiello & A. Whitten "Engineering Privacy in an Age of Information Abundance" Intelligent Privacy Management Symposium, 2010 at 122

[25] Cameron at 1

[26] OPC "Identity, Privacy and the Need of Others to Know Who You Are" at 3

[27] Zittrain "Future of the Internet and How to Stop It", as cited in L. Church & A. Whitten "Generative Usability: Security and User Centered Design Beyond the Appliance" NSPW '09 Proceedings of the 2009 workshop on New security paradigms workshop at 2

[28] Maler & Reed at 18

[29] Privacy Analytics, "De-Identification: Reduce Privacy Risks When Sharing Personally Identifiable Information", 2009, Privacy Analytics Inc., <http://www.ehealthinformation.ca/documents/deidwhitepaper.pdf> at 9

[30] K. El-Emam & P. Kosseim, "Privacy Interests in Prescription Data, Part 2: Patient Data", in E.M. Powers & R.L. Trope, *Eds.*, *Privacy Interests*, March/April 2009, <http://www.ruor.uottawa.ca/fr/bitstream/handle/10393/12985/El_Emam_Khaled_2009_Privacy_interests_in_prescription_data_2.pdf>, at 75

individuals to lower their guard over their information, presuming themselves safe from re-identification and linkages. This means that both organizations and individuals are more likely to share information or consent to it being shared under the (mis)apprehension that it is not a matter of concern. As Ohm argues extensively, the "security" putatively granted by anonymization or de-identification is not only illusory, but dangerous. Re-identification is increasingly possible, not only because more and more data is becoming publicly available and more computing power is available to work with, but also because reidentification techniques are not as difficult as users would like to believe and because there are great financial incentives to be found in reidentification and/or linkages.[31]

Security / Safeguards

Again, at the level of security and safeguards, FIdM appears to evoke different responses.

At a purely infrastructure level, it should be recognized that there are technological and procedural challenges inherent in setting up such a system, especially one that is by definition inter-operable and modular. Similarly, there are economic issues related to the cost of deploying, coordinating and using FIdM systems. These concerns must be acknowledged when considering security and safeguard issues for the simple reason that both of these factors will place extra pressure on those seeking to design and implement (or even to join) an FIdM system. Compounding that pressure is the fact that even after the infrastructure has been paid for and created, this increases rather than resolves the security/safeguard issues that arise.

First off, even as FIdM is touted as privacy protective and providing increased security, it must be acknowledged that in fact it is a model that is predicated on the collection, storage, use and transmission of information, and accordingly that there are risks inherent in it for the user, the identity provider and the service provider. Additionally, the identity provider and the service provider may also need to be aware of regulatory standards for safeguarding and keeping the information secure.

Negotiating these different interests and risks can be a fraught situation. It is also possible, however, to think of this situation as analogous to both the Cloud and to trans-border data flow, and as such to be ideal for negotiating a clear set of rules, obligations, expectations and permissions contractually in order to safeguard all parties as well as to provide a clear framework for dealing with the information appropriately.

Once the basic information management has been addressed, the authentication process which is key to FIdM must be understood to carry its own risks. The effectiveness of FIdM, ultimately, is measured by the effectiveness and reliability of the authentication. Again at this level we can see that all the major parties are implicated →: appropriate and effective authentication is desired by the user and the service provider, while both the service provider and the identity provider must balance the need to ensure the information exchanged is accurate and applicable, while trying to structure their use/storage of the information so as not to open themselves to liability.

Again, this need not be a concern that makes FIdM automatically unworkable – on the contrary, it too can be negotiated by the parties and, as we will see in a future section, potentially shaped by approaches to regulation/governance.

---

[31] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", 2009, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>

As mentioned earlier, both the service provider and the identity provider must also take pains to secure themselves and their processes against liability which could arise from faulty identification or authentication inadequate procedures or security to safeguard the information and its use, or even from the misuse or abuse of information entrusted to them. As well as opening the service or identity provider to liability, these occurrences also make the user vulnerable to a variety of consequences including identity theft, improper disclosure or even denial of access to desired services.

Finally, especially in light of the economic investment in infrastructure, the parties must also be conscious of a duty to safeguard more than the information – on some level, there is an obligation to safeguard the FIdM itself. The system must have wide distribution to be effective, and every party to the system must be able to trust in the other parties in order for the process to be effective. Thus, the question of safeguards and security must be understood systemically, with each actor concerned not simply with protecting their own interests but also with maintaining the integrity of the whole.[32]

Interestingly, this again is a situation where, far from invalidating the FIdM system, appropriate attention paid to these issues could not only resolve them but in so doing actually strengthen the FIdM and assist in creating the advantages that its supporters attribute to it. The appropriate use of some form of privacy impact analysis in order to ascertain all possible risks to the information, for instance, leads naturally to employing privacy by design principles[33] to ensure that the design of the infrastructure, both on a component level and in the larger dynamic model having been built to address these risks is able to properly guard against them or mitigate them.

Data Sovereignty / Globalization

The global scope/impact of FIdM systems again demonstrates that dual nature that appears consistently in the literature around IdM. Recalling that trust via authentication of proxy identity marker is endemic to systems that are geographically diverse, it is unsurprising that IdM is touted by many for the way(s) in which it will help to globalize commerce, facilitate access to information and commerce, and streamline online interactions. If many of these recommendations sound familiar, it is because the language in which IdM is discussed in this context very much echoes the literature around cloud computing.

To link the globalization rhetoric to cloud computing should not be read as dismissing the import of IdM. Indeed, the June 2010 "Plan for a Digital Canada"[34] sets out a number of key themes[35] all of which, at least arguably, resonate with the creation of and support for FIdM systems within Canada. Doing so requires recognition that geographic boundaries are being muted and their meaning diminished by technology, with multiple information economies and digital nations converging in online spaces.

---

[32] T.J. Smedinghoff, Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate (August 21, 2009). Available at SSRN: http://ssrn.com/abstract=1471599 at 15-24

[33] Office of the Information and Privacy Commissioner of Ontario, Submission of the Information & Privacy Commissioner, Ontario, Canada - Response to the FTC *Framework for Protecting Consumer Privacy in an Era of Rapid Change* at 2

[34] Senate Standing Committee on Transport and Communications, Plan for a Digital Canada, June 2010 at http://planforadigitalcanada.ca/index.php?option=com_content&view=article&id=4&Itemid=13&lang=en

[35] Fostering innovation, establishing a world-class infrastructure, expanding the tech industry and positioning Canada for digital success now and in the future. Plan for a Digital Canada at 14

Given this mirroring, it is not surprising that many of the same concerns that we are familiar with in the cloud realm are being raised with regard to IdM. As discussed previously, the core of FIdM is in fact the collection, storage, use and sharing of information across networks. This, in turn, raises many concerns. The increasingly global nature of the Internet, for instance, raises concerns about jurisdiction, both in terms of the regulation of the space and of access to justice. As discussed under security / safeguards, the dispersed method of information storage also evokes worry about protection of the information itself by means of appropriate safeguards, limitations on uses and retention and the necessity of rights of access and correction. Finally, as is increasingly of concern when dealing with outsourced storage of information, concerns are raised about the potential of third party access to the information, as well as the necessity to ensure that appropriate safeguards are in place so that not only is the information safe as it travels to and from the identity provider, but that it is stored in such a way within the identity providers organization that data cannot be manipulated or mined for linkages or new information.

Similar to those concerns surrounding globalization are concerns about data sovereignty that are also potentially raised by the FIdM system. These concerns too operate dually – both concerns about the exercise of influence by foreign states over Canadian data by virtue of the fact that it is within an online space as well as the increased concern about foreign ownership of telcos in order to retain the Canadian ownership, filtering and inspection of traffic within Canada.[36]

Governance / Regulation

Interestingly, one of the only areas in which the literature seems homogenous is in its agreement about the necessity for governance of the FIdM systems that extends beyond the merely technological, as well as suggestions for what approach might be most effective.

First, the global aspect of FIdM (both internationally and domestically) ensures that such systems, if regulated at all, will likely be governed (or covered by) a patchwork of organizational privacy policies, a situation that can create uncertainty for all concerned. As a result, there is clear agreement within the literature that a homogenous approach to governance/regulation of these systems is necessary in order to insert reliability and concurrency between system participants at any level.[37]

This need to reify the governance is not simply the product of a desire for reliability. Instead, it hearkens back to the recognition that all members of the system have a duty not only to protect their own interests, but to bolster the system as a whole. In the case of FIdM, we understand intuitively that governance aimed at supporting or protecting only one of the interests (be it user, service provider, or identity provider) would not be workable nor provide the kind of scalability necessary for FIdM to be successful. The legitimate concerns and interests of all the parties must be recognized and appropriately addressed in any system of governance.[38] Consistently the call is heard for the development of a governance framework that would guard the interests of all and form a baseline of protections to which any user of a FIdM could safely assume they were entitled to and receiving.[39] To that end, many have suggested that the project of appropriate governance must begin with something like a Privacy Impact Assessment →: a careful analysis of the interests of all who are involved with the system in order to begin to structure a framework able to meet and balance those interests. The

---

[36] M. Moll, Trading Sovereignty for Surveillance" Canadian Centre for Policy Alternatives (December 2010) "http://www.policyalternatives.ca/publications/monitor/trading-sovereignty-surveillance
[37] Ahn & Lam at 32
[38] Smedinghoff at 24
[39] Smedinghoff at 27; CDT at 7

benefits of this approach are many – not only does it ensure a careful and balanced approach, but it also facilitates the development of a FIdM system that is balanced and accountable from the ground up, instead of remaining reliant on outdated methods or technologies simply because they are familiar.[40]

The literature reveals some design principles that merit consideration for inclusion in such a framework. For instance:

- FIdM systems should be designed to disclose as little information as is absolutely necessary, and should have anonymity as their default setting; [41]
- Systems should be capable of accommodating multiple unique identifiers across different services in order to prevent unintended linkage and re-identification across service providers;[42]
- Recognition that while the FIdM is in a position to track user activity and/or aggregate user information, this is not acceptable and is, in fact, antithetical to the project;[43]
- The user-centric model should be retained in order to facilitate informational self-determination and (most importantly) meaningful consent to the collection, use, retention and sharing of information;[44] and
- Secondary uses of information within the FIdM system must be identified to the user and require explicit opt-in consent before they will be appropriate.

With the project of building such a framework comes the questions of whether and how the framework is to be translated into practice. Various suggestions have been made, ranging from a free market approach that would allow identity providers to set and enforce their own standards, through the possibility of governing the relationships via contract as is done with transborder data flow and outsourcing generally. The final suggestion is the move towards an actual regulatory approach.[45]

Again there is remarkable consensus among critics in how to best approach regulation. Two alternatives are posited →: either regulation that attempts to articulate and control every aspect of the existing system, or a regulatory approach based on principled flexibility.[46] The disparate voices are united in the dismissal of a tightly focussed legislative attempt to control the process, while at the same time striving to reconcile a principled flexibility with a Nissenbaum-influenced recognition of the importance of context in appropriately balancing and managing the risk of any given use of sharing of information.[47]

---

[40] Discussion Paper on Identity Issues" at 30
[41] The Public Voice, "Civil Society Background Paper", Recommendations and Contributions to the OECD Ministerial Meeting of 17-18 June 2008 from Civil Society Participants in the Public Voice Coalition, <http://www.oecd.org/dataoecd/45/47/44686738.pdf>, at 30; Discussion Paper on Identity Issues at 32 and CIPPIC Comments on the OPC Draft Report at 15
[42] See for ex. Civil Society Backgrounder; Ahn & Lam at 30; Maler & Reed at 18; Clark et al "Exit Node Repudiation for Anonymity Networks"
[43] CDT at 4
[44] Civil Society Backgrounder; Dhamija & Dusseault at 26
[45] Smedinghoff at 28
[46] Ohm at 35
[47] Ohm at 50

FIdM Systems and Canada

Potentially of interest to the OPC is the way the conclusions about governance and regulation map on to the existing Canadian privacy framework. Theorists and critics appear to agree that the preferable approach in seeking to regulate FIdM systems would be one that that is flexible and capable of making assessments of proportionality. To this end, language emphasizing the necessity of a technology-neutral approach that also contained the flexibility to address the force of context in shaping appropriate collection, use, retention and sharing of information.

The Canadian privacy framework currently consists of the 1983 *Privacy Act* and *Access to Information* Act, as well as the *Personal Information Protection and Electronic Data Act* (PIPEDA) of 2000. PIPEDA incorporates the Canadian Standards Association Model Code, which was developed as a model for self-regulation in the area. The Code itself was based on the 1980 OECD Guidelines for Governing the Protection of Privacy and Transborder Flows of Personal Data, a document that represents the first internationally agreed upon set of data protection principles and which is intended to support both the goal of protecting the informational privacy of the individual while preventing any undue obstacles to the free flow of data. As such, PIPEDA is built upon a recognition both of the importance of balancing (potentially) competing interests, and rather than being technology or industry specific, is technology neutral, focussing on information flows rather than the means by which they flow.[48] PIPEDA has been recognized as technology neutral, a quality that has enabled the OPC to apply its provisions to emerging technologies and business models,[49] something that might not have been possible with a more narrowly focussed law.[50]

Conclusion

Throughout the literature review it was clear that FIdM systems are riddled with potential contradictions. Third party authentication and reliable online identity markers has the potential to reduce the risk of identity theft and fraud, and in so doing enhance people's comfort with e-commerce. Nevertheless, it must be recognized that those same features, implemented poorly, could have the opposite effect, facilitating rather than preventing criminal access to information. Similarly, having a single information repository and a single password/access token has the power to increase security, but the flawed implementation of security could grant access to an unprecedented collection of information to anyone.

Accordingly, it must be recognized that FIdM is not an area that can be self-regulating or that can be easily technologically regulated. Rather, it is imperative that all users of the infrastructure be fully cognizant of the process and full participants in the production of the system. To this end, flexible regulation that focuses on the information rather than the technology is important, as is the focus on knowledge and consent that is integral to such a system.

At the conclusion of this guided literature review, therefore, it is impossible to make any concrete recommendations as to whether FIdM is beneficial or harmful or even how to ensure that it is one rather than the other. Instead, it remains in potential simultaneously good and bad until the system is fully designed and implemented. Accordingly, it is at these early stages of design that privacy and security must be assessed and

[48] OPC "Privacy Trust and Innovation" July 2010 at 4
[49] OPC Draft Report on the Consultation at 34
[50] See, for example, the US Video Privacy Protection Act, 18 U.S.C. § 2710 (2002)

factored in in order to bolster rather than attack the privacy of information that will be held and shared within the system.

Appendix A

Some of the literature offers concrete suggestions for identifying issues and shaping an appropriate regulatory framework.

At perhaps the most meta level, Masiello & Whitten identify four (4) concepts that, in their opinion, are important starting points for conceptualizing privacy in these circumstances: reputation; ephemerality; secrecy and contextual integrity.[51]

More specifically, Smedinghoff offers 5 goals that he feels must be present in any effective legal framework in order to appropriately balance the needs/goals of all participants:

- It must clearly define the rights and responsibilities of all the participant roles so that the process works properly, effectively, and reliably to establish the required level of trust;
- It must operate in compliance with all existing laws governing the privacy and security of personal information, and requirements for the authentication of individuals in online transactions;
- It must fairly allocate among the participant roles the key legal risks;
- It must provide some basis of ensuring, before the fact, that all roles (particularly the Identity Providers) have the necessary processes and technologies in place to properly perform their obligations, and are currently implementing those in an appropriate manner (e.g. via an appropriate audit); and
- It must provide a realistic enforcement mechanism and remedy in the event that a participant fails to act in the required manner (e.g. terminate its participation, provide for the recovery of damages, etc).[52]

In their July 2007 report, the Inter-jurisdictional Identity Management and Authentication Task Force themselves identified three main areas of difficulty/challenge that needed to be addressed in order to establish a Pan-Canadian Identity Management and Authentication framework: (1) Capacity challenges dealing with the ability of jurisdictions to engage in identity management and authentication activities at a pan-Canadian level as well as baseline participation; (2) the difficulties of accurately identifying and authenticating clients to the required level of assurance, particularly over remote challenges; and (3) inter-jurisdictional relations and trust.[53]

Finally, and on the most granular level of these collected sources, CDT suggests the creation of a Trust Framework which, they suggest, would "impose as a condition of participation, some minimum terms that would govern the interactions among all three parties – the Identity Provider, the Relying Party and the User.[54]

---

[51] Masiello & Whitten @ 121
[52] Smedinghoff at 28
[53] Inter-jurisdictional (Pan-Canadian) Identity Management and Authentication Task Force IATF Final Report, July 2007, Executive Summary at 6
[54] CDT at 6

Further, while designing such a Framework, they put forward four (4) groups of questions/concerns that must be addressed in order to appropriately implement the system. The points are as follows:

Trust framework providers

- *Admitting identity providers:* On what basis will the trust framework will [sic] certify identity providers as meeting a minimum standard? Will the assertions made by the identity provider be trusted, or will an audit of identity provider practices be performed? On what basis could a trust framework decline to admit a new member?
- *Auditing identity providers:* If identity providers must be audited, who will do the audit, what independence criteria might apply, and to whom will the auditor owe an obligation?
- *Showing compliance:* Will the framework give identity providers a way to show compliance with the framework, such as a mark or a seal? With what resources and how will compliance be policed?
- *Setting framework policy:* How will the trust framework policy be set, and by whom? How will user interested [sic] be taken into account, and how will policies be communicated to users? How will policies evolve?
- *Breach of service:* If an identity provider were to breach its obligations within a trust framework, what would be the consequences?

Minimum rules for identity providers

- *Trust framework requirements:* Will the trust framework require some minimum contract with the identity provider in order to constrain the terms that the identity provider can provide the user?
- *Relationship to trust framework:* What will the relationship between the identity provider and the trust framework provider be? Will it be contractual, and will it also involve the user and relying party?
- *Relationship to relying party:* Will identity providers exercise any discretion regarding with which Relying Parties they will deal? Will the provision of authenticated information to Relying Parties carry with it any obligation or potential liability for relying parties or identity providers (other than an obligation to provide information believed in good faith to be accurate)?
- *Relationship to user:* Will identity providers be subject to some minimum requirements regarding the privacy and security of information regarding users? Will there be data retention or use limitation policies?
- *Obligations with information passage:* Will relying parties be subject to some obligations as a condition of getting access to information about the user?

Recourse and Liability

- *Liability of and obligations to the user:* If an identity provider fails to provide the expected services or fails to meet their obligations under the trust framework and users are harmed, will there be any user recourse? If user information is misused or disclosed without authorization, what rights does the user have? Does the user bear liability or providing false identity information?
- *Liability of the identity provider:* What is the liability of the identity provider of a faulty identification or faulty authentication? For failing to adequately protect user information against unauthorized use or disclosure?

- *Liability of the relying party:* What is the liability of the relying party for relying on a faulty authentication (for example, in the case of identity theft) or [sic] rejects a valid credential it mistakenly believes is compromised? For failing to adequately protect user information against unauthorized use or disclosure?
- *Obligations to trust framework:* If the trust framework imposes minimum contractual obligations, who will be entitled to enforce the contract? Will there be any obligation to enforce the contract?
- *Dispute resolution procedure:* What dispute resolution procedures would be available for disputes between identity providers and trust framework provider? Between identity provider and trust framework? For the user, with respect to any of the parties?
- *Accuracy:* Is there a method in place to allow the accuracy of information to be determined? Is there a way for a user to correct the record?

Privacy and Security

- *Data minimization:* Is there a limit on the scope of information that may be collected (by any party) about the user? Is there a limit on the length of time that data is retained and how is it destroyed?
- *Purpose specification and use limitation:* Are there limitations on how information collected can be used by any party?
- *Transactional authorization:* Will identity services provider the User with the option to approve or decline submission of authenticated information to a relying party in every instance? Can uses [six] prohibit particular users of certain information?
- *Security:* Will identity providers or relying parties be subject to minimum requirements on the security of data? What governance mechanisms will be imposed to prevent against unauthorized use or disclosure?

Courts: What standards apply to law enforcement access or disclosure associated with civil litigation?[55]

[55] CDT at 7-8