



Institute On Governance



# Managing Identity:

An Essential Ingredient in Service Transformation in a Web 2.0 World

By Maryantonett Flumian

*The views expressed in this document are the views of the author and do not necessarily reflect those of the Institute On Governance or its Board of Directors.*



The Institute On Governance (IOG) is a non-profit organization founded in 1990. Its mission is to explore, share and promote good governance in Canada and abroad, and to help governments, public sector organizations, the voluntary sector, communities and the private sector put it into practice. From our perspective, governance comprises the traditions, institutions and processes that determine how power is exercised, how citizens are given a voice, and how decisions are made on issues of public concern.

Our current activities fall within the following broad themes: Modernizing Government; Board and Organizational Governance; Aboriginal Governance; Building Strong Partnerships; Health and Innovation; and International Programming.

In pursuing these themes, we work in Canada and internationally. We provide advice on governance matters to organizations in the public, private and non-profit sectors. We bring people together in a variety of settings, events and professional development activities to promote learning and dialogue on governance issues. We undertake policy-relevant research, and publish results in the form of policy briefs and research papers.

You will find additional information on the Institute and our current activities on our web site, at [www.iog.ca](http://www.iog.ca).

Institute On Governance  
122 Clarence Street  
Ottawa, Ontario  
K1N 5P6 Canada  
tel: (613) 562-0090  
fax: (613) 562-0097  
info@iog.ca  
www.iog.ca



The author acknowledges and thanks nGenera insight who provided financial support for this article. The work was originally undertaken for nGenera Insight's Government 2.0: Wikinomics, Government and Democracy Program.

Managing information about people and their needs will be critical to enabling responsive, personalized government services. However, issues of privacy, data security, and civil liberties are of major concern, and any approach to managing the “digital identity” of individuals must stand up to public scrutiny. Today, while advances are being made on many fronts in transforming service for citizens, the management of identity has become a cultural and practical barrier to collaboration—among service providers, intermediaries, and citizens—that is essential to innovation. Public policymakers and practitioners should be aware of the arguments, how they have been presented, and why they have become barriers to continuing innovation. Governments will need to find ways of dealing with this compelling public problem. As our digital footprints leave bigger and bigger tracks in this connected world, our concepts of privacy and security are undergoing their own evolution, challenging governments to provide direction.

**As a citizen I can choose to provide personal data once and to be served in a proactive manner. Government makes clear what records it keeps about me and does not use the data without my consent.**

— Jan Peter Balkenende, Dutch Prime Minister  
announcing the “e-Citizen Charter” in 2008

Governments have long played a vital role in establishing and managing the identity of citizens. Historically, governments issued travel documents, licenses and permits. And since the advent of the welfare state, governments have had to ensure that the right person received the right payment or benefit. In today’s world, the increasing concern for security, the potential for identity fraud, the increasing use of intermediaries in service provisioning, and the proliferation of technology have added new pressures to the domain of identity. Citizens have legitimate concerns about the privacy and security of their personal information.

It is against this evolving backdrop that citizens are continuing to pressure government to improve and transform service.

Even in a Web 2.0 world, the issues raised around the identity and privacy of individuals have stalled the adoption of a more holistic transformation of service. A new paradigm is required for the collection, sharing and protection of information. Governments are being called upon to play a greater role in the stewardship of identity and privacy regimes. And they must keep pace despite

increasing globalization and population mobility.

Privacy is a public good that in most societies is considered a fundamental human right. Personal information is the key to our identity and each citizen should have the right to ensure its accuracy and decide who uses it, how and for what purpose. Citizens need to feel secure about the management of their personal information. After all, trust and confidence in government are reinforced by privacy and security. Using personal information to improve service and ensuring its security and privacy need not be in conflict. Governments need to find the balance that recognizes that both sides of this coin have value.

## THE IDENTITY CONTINUUM

Governments must be the primary stewards, establishing the frameworks and the penalties for managing identity in this evolving world. For the citizen, identity begins with birth and extends beyond death. For governments, in any given country, an individual's personal identity is not managed on this birth/death continuum. Pieces of an individual's identity are to be found in many individual programs and in multiple jurisdictions, and indeed they spill outside the traditional boundaries of government. Therefore, identity should be managed the way it occurs—on the continuum of activities, interactions and relationships across a lifetime. When using or collecting the information, governments and citizens need to ensure its accuracy and respect individual privacy and security.

Recognizing this continuum and its management is the key to unlocking the door to future multi-party collaboration. It is the foundation for easy access, and tailored individualized service. This will form the basis of the new information architecture which will then become the backbone for the integration of service delivery and citizen engagement.

### From the citizen's perspective

In a New Yorker article entitled, "Million Dollar Murray," Malcolm Gladwell describes the life of Murray Barr, a mentally ill, alcoholic homeless man, living in Reno, Nevada. He eloquently describes the close relationship Barr had with police officers, social workers and medical staff created over a decade of intoxication, recovery, rehab and relapse. "He would grin that half toothless grin. He called me 'my angel,'" said Marla Johns, the social worker who would manage Murray's case once he came into the hospital.

Even though he was charming, the level of service Murray required from the police, medical, and social services was incredible. Discussing Murray with one another, Patrick O'Bryan (a bike cop in downtown Reno) and Marla Johns realized that if you totaled up all his hospital bills for the ten years that he had been on the streets—as well as substance-abuse treatment costs, doctors' fees, and other expenses—Murray Barr probably ran up a medical bill as large as anyone in the state of Nevada. "It cost us one million dollars to do something about Murray," O'Bryan said.

Gladwell's story about Murray Barr is instructive: government services often exist in isolation from one another. These silos result in poor coordination, overlap,

and less than worthy outcomes for the people government is supposed to be helping. Confusion, frustration and expense in personal time and public money are the eventual consequence for citizens. Silos cost millions. And people like Murray aren't helped. Indeed, Murray is "treated" in a piecemeal fashion because every agency only "sees" a very small piece of who he is and what his needs are. Murray provides a real living example of how governments are not designed to provide holistic service that meets an individual's needs.

### From the government's perspective

Government, while looking monolithic to the average citizen, is a multiple set of complex organizations and jurisdictions, each holding a piece of an individual's identity. Whether filing taxes, getting a hunting license, starting a business, replacing identification from a lost wallet, or looking to transition back into the workforce after losing a job, citizens too often find this complexity daunting.

In recent times, most jurisdictions around the world have created a legislated agent whose sole task is to protect the privacy of citizens' individual information. These agents are generally not part of the problem. They raise appropriate issues in order to ensure that all the parties have thoroughly thought through the legal, privacy, and security aspects of capturing, managing, and using information about citizens. Their collective approach has, generally, been practical and pragmatic. Indeed, most of these agents have called for the development of a broader framework by government to deal with identity issues in a Web

2.0 world. These bodies have also called for better education of the general public so that citizens are better prepared to safeguard their own personal information.

Moving from simple transactions to a more holistic service approach requires a broader look at the outcomes that governments are trying to achieve. Given the structures of government and the siloed nature of service interactions, no one arm of government can effectively link the needs which actually affect outcomes. This is why managing identity along a continuum is paramount to ensuring holistic service and actually affecting outcomes.<sup>1</sup>

## CONSENT AND TRUST— BUILDING BLOCKS OF COLLABORATION

An ironic corollary to the siloed nature of information-holding in government is that bureaucracies have tried to turn this into a virtue! It is often claimed that citizens don't want specific programs and services to share information that would lead to better service. While research around the world has shown that citizens do find government complex, fragmented, and difficult to access, it also shows that governments are the most trusted when it comes to collecting, holding and using citizen information. Citizens will consent to sharing information if it is more convenient to transact with government. With consent this information can be used by multiple programs and jurisdictions, with the appropriate protection, to enable governments and others to serve citizens in a more transparent fashion while reducing costs and improving outcomes.<sup>2</sup>

Today, the problem is not only a lack of well-coordinated service delivery organizations, but also a lack of well-coordinated information management systems, building on a basic respect for, and protection of, personal identity. For example, in social welfare systems, this lack of coordination has led to sub-optimal effectiveness of social protection, avoidable administrative burden and related costs, possibilities of fraud, and the fragmented provision of service. Unfortunately, Murray is not alone.

As a foundation for continuing the transformation of government services to citizens, identity management must be approached in a practical and pragmatic way taking into account the identity continuum. Today, the siloed approach to identity information mirrors the siloed programmatic structures of government. These structures do not recognize the more holistic fashion in which citizens live and want to be served by their governments. Nor does this siloed reality allow for breakthroughs in how governments interact with citizens and other players. The silos discourage collaboration and reward duplication of effort, resulting in few improvements in outcomes.

## THE BREAKTHROUGH CHALLENGE: PRACTICAL AND CULTURAL

The challenge will be to support personalized, citizen-centered service while providing secure management of identity and protection of privacy. The practical barrier is that every program, department, and agency of

government at multiple levels feels the need to collect and manage its own information on citizens. Sometimes this is the result of a legislative mandate, but, most of the time, it is the result of wanting to own and control all the information. The cultural barrier is the inability to collaborate, providing the citizen with a holistic service experience. This leads to the collection of the same information from the same citizen thousands of times over a lifetime. This redundancy of effort reinforces the silos, leads to huge additional costs and prevents better citizen outcomes.

## SECURITY VS. SERVICE: THE TWO ROADS TRAVELED

After two decades of discussion, debate and improvements delivered by e-government, the management of identity has taken two very different directions:

- One is driven by security concerns and the development of a single centralized database, as exemplified by projects such as National ID Cards in Hong Kong, the United Kingdom, and more recently across the European Union. Citizen reactions are often colored by the view that the state is protecting itself at the cost of individual civil liberties. The underlying principle is that the state assumes a role for the good of the citizen. The model does not depend on collaboration. It is focused on security of the state, and service is, at best, an afterthought. This is a viable approach to identity management, but it places many hurdles in the way of citizen acceptance and significant service improvements.
- The second focuses on putting citizens at the center of government interactions—improving service and transforming its nature while enhancing accuracy, privacy and security. It speaks to a collaborative engagement between government and its citizens. It is championed by Belgium and Canada amongst others. The citizens' response is to implicitly place more trust in government to do the "right" thing in looking after the needs of citizens. It is based in large part on consent and trust.

These two directions are driven by two very different views of the role of government in an evolving, information-driven world. These two directions, however, are not irreconcilable. The part of government that protects the public good and the part of government that serves the public operate in the same space and at the same time.

These two roles need to interact to strengthen each other—helping to build and reinforce the social contract and the implicit protection it implies—one service interaction at a time. The debates, unfortunately, are still raging amongst practitioners as if a clear winner must emerge. However, as we will see, the approach chosen significantly conditions the debate, as well as trust and acceptance by citizens.

## THE FIRST ROAD: SECURING THE STATE THROUGH NATIONAL IDENTITY CARDS

### Hong Kong: Convergence of history and culture

Some countries have started to address the challenge of managing identity through the development of a National Identity Card. Proponents of this approach have developed “access” cards together with centralized databases of citizen information.

For example, in Hong Kong every resident is provided with a National Identity Card that functions both as a means to verify identity and to access government services. The now-Chinese region has had a long history of utilizing identity documents. Starting in 1980, it became compulsory for citizens to carry identity cards with them when in public areas and produce them when requested by a police or immigration officer. This law was passed in order to halt the waves of illegal immigrants flowing into the city. This has

### THE UK ID CARD INITIATIVE

The UK ID card initiative is built on the premise that ID cards are the “connection points of a national identity scheme, which calls for an easy to use and extremely secure system of personal identification for UK residents.” Each card will hold unique biometric data and a “biographical footprint.” This data will in turn form the basis of the national identity system held in the National Identity Register (NIR). The UK Home Office forecasts that “265 government departments and as many as 48,000 accredited private sector organizations” would have access to the database, and that 163 million identity verifications or more may take place each year. Importantly, government departments and accredited organizations will only be able to access the identity records of a citizen with the citizen’s permission.

slowly evolved into a much more dynamic system built on smart ID cards that facilitate service access.

Thanks in part to this long history and cultural norms, identity cards have not aroused much controversy.

### The United Kingdom: Different history and culture, different outcomes

In a country with a very different history and culture, efforts in the United Kingdom have ignited a fiery debate on the role of government as an overseer of personal information. A proposal for national ID cards, to be called “entitlement cards,” was initially raised following the terrorist attacks on September 11, 2001. Political support for a system of ID cards focused on the growing risk of identity theft and the misuse of public services. In introducing a national ID card program, the government stated that as a result of the recent advances in technology and the still-fresh security threats, its goal was “to improve border controls and security, make travel safer, and facilitate the availability of benefits for those entitled to them.” It linked the ID card to passport issuance, thereby automatically ensuring quick coverage of 80% of the population. The additional 20% would be included over time.

The proposal and legislation, however, led to much public debate and controversy throughout the UK, prompting opposition from human rights and civil liberty groups who believe that the ID card will violate civil liberties. The government had to expend much political capital to see it passed. The House of Lords originally voted against the Bill, only approving it once concerns regarding usage and access by the government were satisfactorily addressed.

Government polls in 2003 showed 61% of UK citizens in favor of identity cards. In July 2006, an ICM Research poll found 51% opposed. In December 2006, a You/Gov poll done for the *Daily Telegraph* found that while 50% of the population supported ID cards, 78% were unhappy with the notion of a “national database.”<sup>3</sup>

Citizen concerns resulted in the creation of the National Identity Scheme Commissioner whose mandate is: to scrutinize how the scheme is implemented, to oversee how ID cards will be used by both the public and private sectors, and to ensure personal data is held securely while reporting on any breaches in its protection. As a result of ongoing debate and consultation, citizen data is to be held in three databases instead of the one originally proposed.

While the Identity Card Act of 2006 is law (the first round of implementation covering airport workers), the debate continues. Following public consultations, secondary legislation to shape the regulatory environment is being drafted. The debate has been rekindled by the recent loss of fifteen million records at Her Majesty's Revenue and Customs office. Unsurprisingly, opposition to the plan continues amongst human rights lawyers, activists, security professionals and IT experts—all of whom point to data losses and security breaches as the palpable risks of a national ID card system. The ongoing debate and its periodic escalation of significant public concern erodes trust and requires considerable effort that diverts attention from providing more collaborative approaches to serving citizens.

## The European Union: The cross-border challenge

The European Union is also taking a closer look at the national ID card approach. During the UK Presidency of the EU in 2005, a decision was made to “agree to common standards for security features and secure issuing procedures for ID cards,” that would reach beyond national or jurisdictional boundaries and thus allow a more networked approach to cross-border movements and service provision.

In 2008, the European Commission began testing cross-border electronic identity systems in an effort to create pan-European recognition of the 30 million national ID cards currently used in 13 member states. The EC has announced that EU citizens will be able to prove their identity and use national electronic identity systems—which include electronic passwords, ID cards, PIN codes and others—throughout the EU, not just in their home country.

The European Commission has said the new system will allow citizens to identify themselves electronically in a secure way and deal with public agencies either online or “ideally” from mobile devices.

“Electronic Identities do not yet do enough for mobile EU citizens,” said Viviane Reding, Commissioner for Information Society and Media. “By taking advantage of the development in national eID systems and promoting mutual recognition of electronic identities between member states, this project moves us a step closer to seamless movement between EU countries that Europeans expect from a borderless Single European Market.”<sup>4</sup>

While only 13 of the 28 EU member states are participating in the pilot, the solutions developed and the experience gained by the project team will be shared with all states with the view to establishing a number of trans-border pilot projects based on existing national systems.

## The national ID card—the citizen's report card

The national identity card approach to dealing with identity management has run into significant citizen concerns. Centralized identity management also means consolidation of information from a number of different parties. This raises the specter of one party having access to explicitly linked data that governments will do “who knows what with.” “One database” also raises issues of security if it is penetrated.

Meanwhile, the implicated agencies are not particularly happy to be replaced or to “give up” data. As a result, those that take on these kinds of centralization projects find themselves putting more effort into agency reorganization than into finding the right model of service for citizens. In fairness, most of these schemes were never intended as the building blocks for service transformation. Service gets thrown into the mix only when the schemes run into controversy!

One of the many challenges facing national identity cards in democratic countries is the concern raised by critics about “Big Brother” and how identity information will ultimately be used. The relationship between the government and its citizens hinges upon trust. The proponents of identity cards (and what they represent) must deal with the issue of trust on an ongoing basis. While the UK has gone a great distance to mitigate fears and build support for adoption, the view continues that the individual is subservient to the state. While governments will often tout the ID card as improving access to service, the reaction from citizens has significantly colored the adoption of the card for service transformation.

Politically, this road has many red lights—including questions about civil liberties and the erosion of trust between citizens and government—stalling the progress of many travelers. It is also missing some significant bridges to the future, as it does not build on collaboration. And the recent controversies in the United Kingdom, Australia and Japan regarding their cards and losses of centrally-held citizen data have done little to help the ID card cause. More importantly, how would an ID card help Murray access better service?

## THE SECOND ROAD: DEVELOPING COLLABORATIVE SERVICE NETWORKS

An alternative and more robust solution for government is to develop collaborative frameworks for identity management that capitalize on the knowledge resident in the extended network of service provisioning. Every service provider has a stake in the outcome. Such a framework would address issues of trust and consent, and include the organizational behavior and practices of information management and standard setting which reinforce trust. The identity management framework and its implementation would need to bridge governmental silos while respecting lines of authority currently prescribed in legislation. This approach to identity is intended to enhance and transform service by leveraging the existing information and trusted “identity intermediaries” for greater purpose. Adopting the framework is required to improve how Murray is both served and protected.

### Identity intermediaries—connection, consent, trust and risk in context

In the financial sector, the concept of “identity intermediaries” or stewards is well established, especially in a world where the majority of transactions are conducted by credit or bank cards. Identity is confirmed and validated by trusted third parties. The role of the intermediary arises from consent, which is the basis of trust. The “need” starts with a transaction—buy a laptop, get a mortgage for my condo, book a trip—with a specific provider, and the intermediary has trusted relationships with both parties. The intermediary also brings context to the transaction, based on ongoing observation of the individual's transactions. How many times have you received a call asking if you indeed made that expensive purchase? The call came in response to behaviors outside of the established norm. These intermediaries have grasped the power of collaborating across networks to validate identity in context.

### Identity intermediary pathfinder—the Belgian Crossroads Bank for Social Security

#### Social services at the crossroads

In the mid-1980s, Belgium's social sector was spread out among local, regional and federal governments, as well as among not-for-profit and private institutions—3,000 agencies in all. It was no surprise that this spaghetti bowl

of agencies and organizations was having a difficult time talking to one another, even though many of them shared the same clientele. In fact, for these agencies, it had never been a priority to see their services from their clients' point of view.

An in-depth analysis of social security organizations showed that the processes used by the social sector were full of complexities and duplication. Citizens attempting to process an entitlement found themselves filling in pages of paper forms in multiple offices, discovering that each office had its own forms and procedures to determine whether to grant entitlement. In total, hundreds of different paper forms were used between citizens and employers on the one hand and social security offices on the other. In total there were some 2,000 pages of instructions used in processes across the country.

At the time, there was no means for sharing information between social security offices. This meant that the same information had to be provided by citizens to each one of the offices, even to the point where one social security office asked citizens and employers to produce a form used by another. Repeated manual inputs of information further raised the possibility of error and inefficiency.

Other problems with this disconnected system included the fact that even when two social benefits were linked—so that in receiving one benefit, another entitlement was triggered—citizens and employers had to do the work of claiming that new entitlement themselves.

Citizens and their employers were also put at a disadvantage because they did not have the necessary tools for checking the quality of their information before it was reported to the social security offices. This resulted in more errors and numerous subsequent contacts for the correction of errors, all of which could have been avoided with a self-directed or citizen-controlled system.

Much of the social security system in Belgium is designed around employers and their information about employees (e.g., whether people are employed, what they are contributing to the benefits system, what they are earning); however, there is no automated way for employers to interact with these offices and service providers. Thus, much of the administrative burden for social services fell upon employers, sucking significant resources from their core work, and creating a hurdle to economic growth. The system had become a brake on entrepreneurship, growth and productivity for the country.

## Empowering the network to build the intermediary

As we discuss fully in a companion case study, the Crossroads Bank for Social Security (CBSS) was created to deal with the inefficiencies and to capture the opportunities of the existing organizations and social actions. The CBSS has a mission “to stimulate and to support the actors in the Belgian social sector to grant more effective and efficient services with a minimum of administrative formalities and costs for all those involved.” It has become a full-service data management organization that allows the nearly 3,000 responsible government agencies and non-governmental organizations to manage information about clients, while maintaining client privacy, security, and confidentiality. It is a model of how to manage information to radically improve public services for citizens and employers.

With a client base of 10 million citizens, and with 220,000 employers, the Belgian social sector delivers a complex array of benefits to the public—collecting social security contributions, delivering social security benefits (e.g., child benefits, unemployment benefits, old age pensions, guaranteed minimum income, and benefits for the disabled), and delivering supplementary social benefits, such as bus passes for the elderly.

The CBSS allows clients of the social system to identify themselves to the social sector once when their circumstances change (such as when one leaves a job, has an accident, or a death in the family). The system then moves their information to the appropriate agencies to begin delivering services based on that person’s entitlements. It is literally at the “crossroads” between

different agencies to ensure information finds its way to the right place in the right ways. It is the most effective public/private sector “identity intermediary” in existence.

## Building trust through governance that federates, not isolates

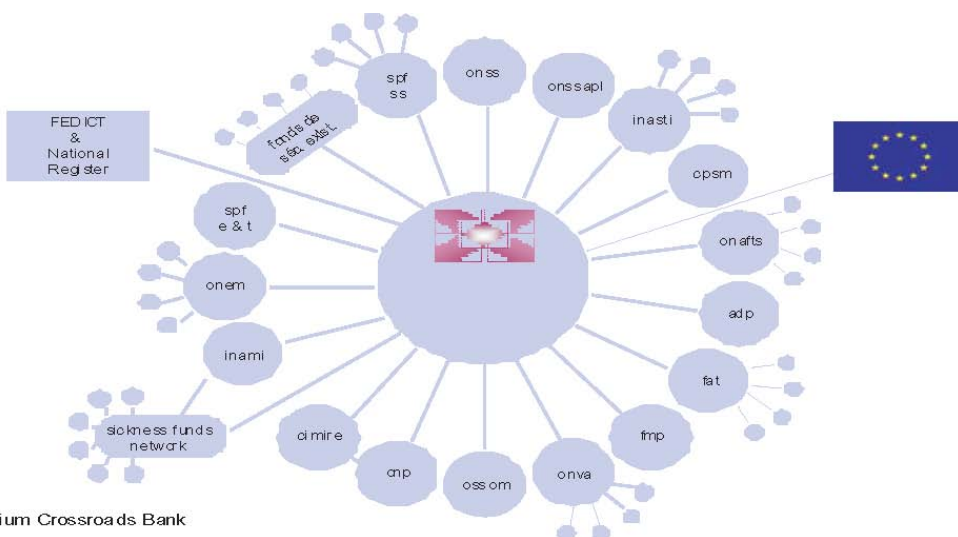
The CBSS is not a centralized databank of citizen information. Rather it is a network that facilitates access to information. CBSS holds no information itself. Its main work is to manage information sharing between agencies who have the legislative authority to hold or view information about an individual or employer. The CBSS’s role is to ensure that access happens by agreed-upon rules and procedures. It is a trusted third party that simplifies access to the various social agencies in Belgium. These agencies in turn use the CBSS to eliminate forms, and improve the convenience and effectiveness of their services.

Trust is a key component of the system. The CBSS’s governance model involves stakeholders from across the social sector, government agencies as well as employer organizations, trade unions and a number of policymakers at the highest level. As “bank governors” they oversee the CBSS’s activities.

The Belgian model recognizes that information does not need to be consolidated to be used. Instead, it can be assembled and managed between trusted sources that collaborate through networks linked for a common purpose. This also makes the holdings more secure.

This collaborative model of information management meant that there was no need for a centralized database. Instead, efforts went to developing standards for the collection and exchange of information between different organizations. Someone had to be put into a leadership role to develop new standards and ensure that existing ones are strictly enforced. The model needed a way to manage the “crossroads” between the information flow from different organizations, making business processes and technology in different organizations interoperable.

Such a model offers more flexibility and trust because it encourages shared responsibility for data security, privacy and service among all stakeholders in the network. All are empowered to be a



Belgium Crossroads Bank

part of success. Government would not be in a command and control position. It would be a partner with companies, civil society organizations and others with whom citizens had a trusted relationship. Having a trusted broker between all these groups' interests helps keep everyone honest, effective, and transparent.

At its heart, the design of the CBSS builds on the idea that lifelong relationships are the surest way of understanding and verifying a person's identity in its appropriate context and for the intended purpose. From the time we're born to the day we die, we encounter different organizations and institutions where we leave a record—be it with banks, governments or the local video store.

## THE DUTCH E-CITIZEN CHARTER

The Dutch Prime Minister, Jan Peter Balkenende, in his 2008 speech outlining his government's commitments to improved service delivery to citizens in their "e-Citizen Charter," undertook to spell out the need to ensure open and transparent principles with respect to government use of personal information, and the consent of citizens for its use. For example, one of the Ten Principles he committed his government to was: "As a citizen I can choose to provide personal data once and to be served in a proactive manner. Government makes clear what records it keeps about me and does not use the data without my consent." This is a profound declaration which places the onus on the various Dutch departments and agencies to network and work together as one enterprise.

### The citizen has a direct role

The CBSS's role is to find a way for employers and organizations within the social sector to interact with one another to share relevant information for improving a service without having to share everything they know. More importantly, the subject of their sharing—the citizens—are empowered to watch what is shared about them, change information about themselves, and ensure its accuracy. The citizen has a direct role. As a result, privacy is enhanced because the parties to an individual's information and their use of it are clear and traceable.

### Benefits for all

The work of the CBSS has resulted in dramatic reductions in forms, decreased burden on employers, and streamlined access to better social services. It is estimated

that since 2002 the system has saved companies 1.7 billion Euros a year in administrative costs.

Fraud is also reduced. The shared nature of the network requires transparency to be designed into the system. And since all information exchanges and uses are recorded, any nonstandard uses of information show up immediately. So, for example, when the system was first introduced, it became clear that some individuals were drawing double benefits because agencies were disconnected. Once they were able to share information, the fraud was detected and stopped.

The project began in the 1980s when the Web and collaborative social technologies were unheard of. It began as an initiative aimed at reducing the inefficiency of a system which had become a brake on entrepreneurship, economic growth, and productivity for the system. Now with the help of Web 2.0 tools, the CBSS uses relationships, trust, and technology to continue to transform citizen services in Belgium.

## A PAN CANADIAN STRATEGY ON IDENTITY MANAGEMENT AND AUTHENTICATION

Canada's path to federated identity management began in June 2006, at the first inter-jurisdictional meeting of Deputy Ministers of Service Delivery Collaboration. The meeting saw senior officials from all federal and provincial levels of government agree to make identity management and authentication the lead area for cooperation. In April 2007, the final report, "A Pan-Canadian Strategy on Identity Management and Authentication" was issued. Among its main conclusions, it recommended the essential need "to leverage the various existing identification and authentication infrastructures in many jurisdictions." It further notes that "collaborating on identity and authentication standards will also facilitate a shift toward identity centered service delivery, help focus attention on improving government services and create a more efficient means to deliver service."

This collaboration rendered the silos of government irrelevant to services transformation. Departments and agencies far too often devote valuable energy, resources and people to fighting the reorganization of silos and fiefdoms. The leadership at the Crossroads Bank recognized that outcomes, not the structure of government, was key to transforming service. The challenge was: What would it take to help 3,000 organizations talk to one

another, in order to put citizens at the centre of what they did? Murray would be far better served!

The CBSS example highlights how increasing the level of consent and control held by citizens, the level of trust and confidence in the institutions which hold that information can be greatly improved. Citizens can see that government is working hard for them individually and in a very personalized fashion. This dramatically colors their attitude, their acceptance, and their direct engagement. Managing information on identity was essential to service transformation.

Bob Blakley, a noted identity management expert, writes: “If you try to manage their identities yourself, you’ll do a bad job, and you’ll spend a lot of money doing it. Find another organization which has the intimate relationships you don’t, and federate with that organization. Be sure to spell out the terms of the federation so that you understand the source and quality of the identity assurances you’re relying on as well as what remedies you have in case those assurances turn out to be unreliable.”<sup>5</sup>

## Identity intermediary pathfinder— Canadian Newborn Registration Service

Canada drew heavily from the progress made by the Crossroads Bank in its federated approach to information management in its newborn registry service. The registry is helping to create a cradle-to-grave continuum for identity management. The pilot was aimed at testing whether citizens would consent to sharing information if it contributed to more convenient and efficient transactions. The benefits of such consent are numerous and can allow for multiple jurisdictions, with the appropriate protection, to serve citizens in a far more transparent fashion while reducing the overall costs to government.

In the past, registering a birth was time consuming, inefficient, and did little to enable collaboration or effective service delivery by government agencies. And yet it is with birth that the process of establishing a citizen’s identity begins.

The process crossed departmental and jurisdictional boundaries. Some of the process had traditionally had to be undertaken in person and some by mail. The application and issuance of documents had to follow a predetermined sequencing that is not entirely obvious to the citizen.

At a minimum, parents had to complete three separate paper applications to three different levels of government for birth registration, birth certificate, and a Social Insurance Number for their baby. After submitting the birth registration to the municipality, they had to wait to receive confirmation before they could apply for a birth certificate from their province. Then they had another wait for the birth certificate to arrive, and only then could apply to the federal government for the Social Insurance Number.

As part of the Canadian government’s inter-jurisdictional attempts to improve service delivery through more effective identity management, the province of Ontario and Service Canada introduced the Newborn Registration Service—an innovation that enables parents to register their baby’s birth and apply for the child’s birth certificate and Social Insurance Number all at the same time. Before parents leave the hospital, they are provided with a birth information package which encourages them to do all this online and without having to duplicate the required information.

By streamlining the three application processes into one integrated online service, the Newborn Registration Service has cut the time for processing important identity documents in half. Continuing improvements in the processes will result in enhanced speed of service, further cutting the processing time from months to weeks.

In addition to increasing operational efficiencies and speed of service, the Newborn Registration Service offers parents the assurance that the privacy of their personal information is protected. The service has the advantage of enhancing the quality of data captured and maintained in provincial and federal registers. The electronic application process greatly reduces the number of errors that tend to plague paper-based processes with manual processing of documentation.

As confidence has grown as a result of this success, the parties are increasingly looking for ways to increase the members to the partnership. Programs and services under consideration include health cards, passports, child education savings grants, child tax benefits and child care payments. The possibilities are endless.

In the process, two levels of government working together have also created the foundation for managing identity on a continuum that begins at birth and includes services and programs throughout one’s life.

This was achieved by understanding that managing identity in a collaborative fashion would provide the backbone to “joining up” services from many jurisdictions. The management of information was the key breakthrough. Understanding that each party had something that the other relied on, and trusting them to do their part for everyone, unlocked the door to a massive improvement in service.

## WHERE DO THE TWO ROADS LEAD US? SECURITY AND SERVICE

Having traveled down these two roads, we find that the second road takes us to a far better destination in transforming service for citizens. It engages the citizen, empowers the network, changes the culture of government, and creates consistent standards and security for the holders and protectors of personal information. At the end of the day, it also does a better job of securing both individual identity and protecting the state—by managing individual identity along the entire continuum. It requires greater collaboration, consent and trust from all the parties, including citizens, and finds a better balance between several in the process.

### The way forward—federated identity

Implementation of collaborative identity management is enabled by the advancement of Security Assertion Markup Language (SAML) 2.0. SAML 2.0 passed a series of interoperability tests early in 2005 and was approved as a formal standard by the Organization for the Advancement of Structured Information Standards (OASIS).

The technology allows richer integration of partners, faster and cheaper coupling through standards, simplified customer experience, deeper service offerings, and better protection of customer information. “Federated identity,” the exchange of information within and between enterprises, provides authentication and authorization capabilities. Federation enables loosely coupled identity management across autonomous business domains and extends the reach of applications. It is now becoming a strategic requirement for most enterprise infrastructures, and adoption continues in multiple industries.

## FEDERATED IDENTITY

Boeing has tested and designed an early federated identity management infrastructure that will scale as more companies and organizations adopt the technology. Boeing’s initial federation efforts addressed the company’s account management costs. Boeing saved money by standardizing and eliminating multiple accounts and passwords per user. Federated identity management has also allowed Boeing to easily integrate with its external business partners. It has eliminated the need for users to remember separate user IDs/passwords for various service providers. And by using federation-enabled links, developers are able to build company-branded portals that have a good look and feel.

## CAN GOVERNMENT KEEP UP WITH CITIZEN EXPECTATIONS?

Today, citizens have already demonstrated their ability and ease of access to online services in the commercial world, through such entities as eBay and Amazon.com. As electronic commerce continues to expand, numerous intermediaries are being established which deal with personal identity. Can governments keep pace?

“At issue is whether governments will establish an identity policy framework and assume the necessary stewardship for citizen identity before the private sector and citizens find too many alternative intermediaries. At which point it may be difficult, if not impossible, to protect citizens from identity theft and breaches of personal privacy.”<sup>6</sup>

### Who will fill the gap?

Organizations and online collaborations have begun to compensate for the lack of a government policy framework for identity management. The Liberty Alliance ([www.projectliberty.org](http://www.projectliberty.org)) is a consortium developing operating standards for a secure and privacy-respecting Internet identity layer across applications and industries. The Identity Commons ([wiki.idcommons](http://wiki.idcommons)) is a virtual online working group that addresses social, legal and technical issues that arise regarding identity data and the social layer of the Internet.

## A necessary role for government

The issue facing governments should not be whether to have a role in citizen identity management, but rather how much of a role they should perform. The US government has recently passed legislation entitled Real ID, thereby imposing an identity management framework on state authorities in their interactions with the national government. The rationale and driver for this initiative appears to be more around public safety and security than citizen service and entitlements.

However, if identity management is foundational not just for public safety and security but also for service delivery, then can a framework be developed which is founded on a trust relationship between government and the citizen? And if trust is to be at the heart of such an identity management system, then the first challenge for any government is building a relationship of trust among its various departments and agencies.

## IDENTITY MANAGEMENT 2.0

Simply put, Identity Management 2.0 is the federated framework which allows multiple institutions to identify Million Dollar Murray as one person and for Murray to consent to his identity information to be shared to ensure he gets the services and benefits he is entitled to.

With federated identity management, identity is established and validated through collaboration. What begins with the need to conduct a transaction ends up adding to a custodial relationship built on trust and consent with each party. The Crossroads Bank in Belgium and the Canadian Newborn Registration Service did not need to re-collect or centralize information already held in multiple databases by multiple agencies. They concentrated on standard setting, the accuracy of information, the health and robustness of the network, the consent of citizens, and the necessary investments in management and technology. As a result, they were able to eliminate forms; reduce the compliance burden and its costs for businesses, individuals, and governments; and become a catalyst for transforming service delivery.

In a Government 2.0 world, multi-dimensional collaboration across agencies and governmental jurisdictions will demonstrate the leadership capacity of governments. In this way, governments will be able to assume the mantle of stewardship for identity management. Only then will they be able to become truly citizen-centric and fully transform citizen services.

# ENDNOTES

- 1 Maryantonett Flumian, "Citizens as Prosumers: The Next Frontier of Service Innovation," nGenera Insight, 2007.
- 2 Research undertaken for Service Canada by EKOS Research, Ottawa, Ontario.
- 3 [www.yougov.com/uk/archives/pdf/TEL060101024\\_3.pdf](http://www.yougov.com/uk/archives/pdf/TEL060101024_3.pdf).
- 4 Commissioner Viviane Reding Speech, <http://europa.eu/rapid/pressReleasesAction>.
- 5 Ibid.
- 6 Bob Blakley, "A Relationship Layer for the Web... and for Enterprises, Too," Identity and Privacy Strategies In-depth Research Overview, Burton Group, June 20, 2008.

# ABOUT THE AUTHOR



As the President of the Institute On Governance, **Maryantonett Flumian** is responsible for the development of the Institute's vision and strategic direction, project and partnership development, and the fostering of programs to promote public discussion of governance issues. She is a seasoned senior executive at the Deputy Minister level in the Canadian federal Public Service with more than 20 years of large-scale operational experience in the economic, social and federal/provincial domains.

She is internationally recognized for her work as a transformational leader across many complex areas of public policy and administration such as labour markets, firearms, fisheries, and environmental issues. She was the first Deputy Minister of Service Canada. Her current research focuses on leadership, collaboration, governance, and the transformational potential of technology primarily in the area of citizen-centered services.