Privacy and Government 2.0:
The Implications of an Open World

Ann Cavoukian, Ph.D

Information & Privacy Commissioner
Ontario, Canada

May 2009

Story in Brief

Profound technological and social forces are reshaping the public sector, its governance structures, and constituent relationships. Government adoption of Web 2.0 "social" technologies will empower citizens on an unprecedented mass scale. What does this mean to privacy and personal data protection? This paper explores what could happen to government and its institutions; what it means to the massive amounts of personal information it collects, uses, discloses and retains; and what the implications of this new way of governing may be for individuals and their personal information. Since January 1, 1988, the IPC has acted independently of government to uphold and promote open government and the protection of personal privacy in Ontario.

As governments consider whether or not to embrace these forces in whole or in part, they will need to seriously consider any implications to privacy. But it doesn't stop there. To be successful, governments will also be responsible for identifying the means to "build privacy in early" to ensure continuing and enduring public trust.Since the mid-1990s I have been advocating this proactive *Privacy by Design* philosophy and approach as the most effective way to ensure privacy protection AND meet the operational requirements of a given information technology, system or ecosystem. No trade-offs are necessary if we recognize the value of addressing privacy, apply universal privacy principles, and build privacy in early making it the default. This could mean citizens co-managing their personal information held by public sector organizations.

Introduction

The advent of the Internet and information and communication technologies has, in one generation, radically changed the ground rules for managing personal and other data. Recently, through the confluence of technological, demographic, social and organizational forces, the World Wide Web has ushered in an age of participation where billions of people can now play active roles in their workplaces, communities, national democracies and the global economy at large. Whether it's Facebook or Wikipedia, Flickr or YouTube — Web 2.0 is a world where Internet users are creators just as much as they are consumers.

A growing number of governments around the world are currently deploying Web 2.0 technologies in the workplace, the design and delivery of public services, and their processes for engaging with citizens to increase efficiency and transparency, and to foster richer interactions with the citizens they serve.

A new breed of public sector organization could subsequently emerge: one that opens its doors to the world; co-innovates with everyone, especially citizens; shares resources that were previously closely guarded; harnesses the power of mass collaboration; and behaves not as an isolated department or jurisdiction, but as something new — a truly integrated and open-networked public sector organization.

This shift to co-creation and collaboration goes much beyond e-government initiatives to transform the role and processes of government and governance. Web 2.0 promises to transform e-Government into Government 2.0.

> Traditional structures of government — typically top-down hierarchical models and silo approaches — are being called into question. They're just not as compelling as they once were. With the new, function-rich infrastructure of Web 2.0, government no longer needs to work on its own to provide public value.

To achieve this, governments need to shift from silos of information to greater sharing of data, not just within government but also outside of government and even beyond jurisdictional lines. Such a dramatic shift in the norms of information management undoubtedly raises large questions related to privacy. Enhanced efficiencies, service innovation and democracy are desirable goals of government adoption of Web 2.0 technologies. But where these novel uses of Web 2.0 technologies by governments involve personal information, privacy must be addressed very early in the design to ensure the long-term success of Government 2.0 transformation efforts. In the Web 2.0 era, information may very well "want to be free," but not necessarily personal information!

Privacy Defined

Informational privacy refers to the right of an individual to exercise control over the collection, use, and disclosure of his or her personal information. Personal information (also known as personally identifiable information or "PII") is any information relating to an identifiable individual. Specific PII can include, for example, an individual's name, address, telephone number, date of birth, photo, marital or family status, and financial status.

It is also important to note that almost any information (e.g., a set of numbers on a RFID tag or the sequence of points that make up a biometric template), if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. Hence, the definition of "privacy" can be quite broad in scope and the challenges for privacy and data protection are equally broad.

Efforts to manage and control personal data focus on observing a set of universal information management principles called the Fair Information Practices (FIPs). Developed in the late sixties and early seventies in response to growing concerns about computerization of personal information by public and private entities, the FIPs express the right of informational self-determination by requiring organizations that collect personal information to:

- be accountable for their personal information management practices;
- minimize PII throughout the entire life cycle, from collection to destruction;
- implement data security appropriate to the sensitivity of the personal information; and
- involve the data subjects in the management of their personal information.

FIPs have since become the "international DNA Code" for public- and private-sector information privacy laws, regulations, policies, practices and norms around the world. By becoming embedded in this way, the FIPs accommodate the growing needs for, and uses of, personal information in modern society with appropriate safeguards to prevent misuse and harm.

A number of factors must be taken into account when implementing privacy practices, including legal requirements, available technologies, social norms and business processes. We need to ensure that privacy provisions are applied in a practical manner that takes into account a balancing of these varied interests, benefits and risks. Critical to this is an understanding that security does not equal privacy. While information security is extremely important, the term privacy subsumes a far greater set of protections than security alone.

Government as Citizen Data Custodian

The creation of information is accelerating, and this data is being replicated everywhere. We can no longer speak meaningfully of information destruction, as we once did with paper records, because digital bits and bytes have now attained near immortality on the Internet, thwarting efforts to successfully remove them from the public domain. At the same time, the practical obscurity of personal information — the default privacy protection of yesteryear — is also fast disappearing as data becomes digitized. With so much data available electronically, we rely more on advanced searching and mining, rather than sorting techniques to enhance data analysis and information management to make disparate data elements become valuable knowledge.

These trends carry profound implications for information privacy. As large scale information systems become more common, there is so much information stored across an ever-growing number of databases worldwide that individuals have no way of knowing of, or controlling, all of the information about themselves that others may have access to. Such information could potentially be sold to others for profit and/or be used for purposes not known to the subject individual — surveillance, profiling, re-identification of anonymized data, discrimination, fraud, identity theft. The concept of information privacy has become more significant as more systems controlling more information appear.

Governments have important roles to play in this evolving privacy landscape as active custodians of citizens' personal data used for delivering services. Government activities are becoming more data-intensive and connected than ever. As custodians of personal data, governments are not subject to the same market disciplines as the private sector. With government, the role of individual consent and choice is often diminished. There is no competition, and governments can compel collection and disclosure of personal information to make decisions affecting those individuals.

Jonathan Zittrain, a professor of Internet law at Harvard Law School and a faculty co-director of Harvard's Berkman Center for Internet & Society, has noted that:

> "We are still concerned about databases with too much information that are too readily accessed; databases with inaccurate information; and having the data from databases built for reasonable purposes diverted to less noble if not outright immoral uses. Government databases remain of particular concern, because of the unique strength and power of the state to amass information and use it for life-altering purposes. The day-to-day workings of the government rely on numerous databases, including those used for the calculation and provision of government benefits, decisions about law enforcement, and inclusion in various licensing regimes."[i]

The accuracy issue deserves special consideration. Privacy principles require that personal information be accurate and up-to-date for the purposes specified. Outdated and inaccurate information, when used to make decisions affecting people, can have profoundly negative consequences, as anyone who has been a victim of financial identity theft and had his or her credit rating compromised can attest. Worse, the effects of bad data are compounded as this data is propagated throughout a given information ecosystem. Web 2.0 technologies that expand routine sharing and dissemination of information will likely expand this ecosystem

and the velocity of incorrect personal data; one unflattering Facebook posting can affect job prospects for years. Regrettably, the effects of bad data often fall primarily upon individuals who are left to figure out the causes of the problem, and burdened with sorting out the resulting consequences.

In the government context, the best known examples involve the inclusion of citizens on "no-fly" or other "suspicious persons" watch lists.[ii] In such instances, it becomes difficult for the affected individuals even to verify that they are on the list at all. Because of their special relationship with citizens, governments must take exceptional care to verify the accuracy of information that they collect, use, share and retain about citizens. Emphasis should be placed on establishing the trustworthiness and integrity of information sources, an accountable "chain-of-custody" for upstream and downstream data uses, and effective remediation processes should the data be incorrect or in dispute.

A Positive-Sum Approach

Some may view existing privacy laws as barriers to governmental structural reform efforts. For example, privacy laws make it clear that information collected for one program or purpose cannot be used for other, secondary purposes without additional consent by the individuals. As a result, efforts to create whole-of-government services have been difficult because departmental silos of personal information cannot be easily linked or combined without, in many cases, changes in program legislation (not to mention the problems of legacy systems and lack of interoperability).

But privacy and data protection laws have always had dual purposes — while seeking to recognize the rights of individuals to protect them from harm, such laws also seek to:

- ensure the free, uninterrupted and responsible flow and uses of personal data;
- promote business and commerce;
- ensure that public agencies are held accountable for their actions;
- ensure that personal data is collected, used, retained and shared in a manner that is open, transparent, equitable, in accordance with the interests of individuals; and
- ensure that the approach chosen serves redeemable ends (e.g., improving efficiency, delivering new and innovative services, promoting competitiveness and continuous quality improvements, or even catching criminals).

Nonetheless, maintaining an organizational culture of privacy that incorporates, among other elements, solid data protection practices is essential to successful governments (and businesses) because they help foster necessary trust and confidence. Privacy can and should always be built into information systems and architectures as early as possible, at the earliest design stages. When operationalized in a systematic way, building effective privacy into a given information system should always enhance the achievement of other, non-privacy-related, program goals, and never pose a hard restriction or trade-off: a true positive-sum result.

Government 2.0 as defined by enhanced service delivery and a more collaborative governance process looks to:

- bring a new agility, responsiveness and flexibility to the way societies are governed and services delivered;
- create and deliver services and policy that deliver optimal public value;
- leverage innovation, value and commitment from a broader group of participants;
- distribute power more broadly and appropriately amongst stakeholders; and
- instill greater transparency and legitimacy into political decision-making.

The associated governance and accountability challenges will apply across the entire spectrum of government activities, up to and including the front-office domains of providing services, engaging citizens in political dialogue, and enforcing compliance with the laws that protect citizens' personal data through data sharing agreements or memoranda of understanding.

Data Accountability

Tapping into voluntary, self-serve or automated processes offers government organizations considerable scope to improve efficiencies. A leading example is the Peer-to-Patent collaborative community that aims to improve the process for reviewing patents, which is made slower and less effective by the high number of patents to be processed and the technical knowledge required. This innovative project shows how the patenting process could be opened up using the collaborative gathering and filtering of existing evidence by voluntary, self-appointed experts, in order to assess the inventive step of a patent application. The most relevant references are then submitted to the US Patent Office for the official review, which is made simpler by the contributions, selection and comments made by the participants.[1]

Internal fragmentation between institutional levels, agencies, departments, often referred to as the "silo effect," can reduce the efficiency and effectiveness of government actions. Promoting greater collaboration across agencies, or 'joined-up' government, has been one of the key objectives of government modernization. Wikis in particular are starting to be used by government to enhance cooperation within and across organizations.

Internal deployments of Web 2.0 technologies and processes offers much potential for enhancing efficiencies, as barriers within and among government are broken down in the spirit of "whole of government" cooperation and sharing, as department information silos are connected, compared, and coordinated, and as the data stores and key processes are reused. For example, Intellipedia is a wiki-based platform which enables the direct collaborative drafting of intelligence reports by analysts from different intelligence agencies, with little or no hierarchical filtering.[iii,iv]

The benefits of applying the same collaborative approach, however, to personal data are unclear given potential privacy risks.

In this new world of collaboration, existing information silos and other barriers to data sharing will have to be dismantled. New non-governmental actors will be added to emerging governance Webs, and data will increasingly stretch across organizational boundaries, raising new questions about who has access to whose data, how much, when, for what purposes, for how long, and with whose permission.

Collaborating on service delivery with the non-profit or private sectors offers efficiency gains to governments, but with a potential price tag of weakened accountability and data security.

Public sector agencies seeking efficiencies by hosting their e-mail and other software services with Google, for example, can save considerable sums of money in upfront IT expenses and operating costs, but must wrestle with the prospect of large volumes of sensitive personal data and communications being hosted in other jurisdictions, controlled by non-governmental

1. See nGenera Insights report: "The Future of Collaborative Governance" by Dr. Beth Noveck and David R. Booth.

third parties, and subject to foreign inspection. Canadian public sector organizations such as universities, hospitals and government agencies are banning Google's innovative tools outright to avoid the prospect of U.S. intelligence agencies combing through their data. Security experts say many firms are only just starting to realize the risks they assume by embracing Web-based collaborative tools hosted by a U.S. company.[v]

Web 2.0 technologies such as RSS feeds and podcasts allow government organizations (and politicians) to create powerful and cost-effective new channels for direct-to-citizen and viral transmission of customized news and information. Some government agencies are beginning to stake a presence in Facebook or MySpace, deploy more multimedia content, and even set up outposts in virtual online worlds in their efforts to extend outreach. From a privacy point of view, such outreach efforts are largely benign, and may even be privacy protective as they allow citizens to consume information most relevant to them more effectively without divulging their own personal information in return, as subscription or mailing lists would.

While the emergence of less-than-official informal dialogue and networks with the broader community is a refreshing trend, some limits must be applied and enforced. The most obvious concerns center around potential breaches of confidentiality. From a privacy perspective, clear limits — or at least clear guidance — should be placed on public officials' freedom to disclose identifying information about colleagues, clients, and citizens. A model of such guidelines was developed in 2005 by IBM.[vi]

Data Minimization

Enthusiasm for mass online participation in democratic processes should be tempered by the sobering realization that such online activities can generate enormous volumes of personal data — data about opinions, conversations, preferences, habits, activities, and relationships that may be collected, used and disclosed for many unrelated purposes. Online participation of identifiable citizens could potentially expose them to new forms of surveillance, profiling, social engineering and discrimination by governments and other known or unknown entities.

Web 2.0 "social" technologies enable two-way communication with citizens, clients and stakeholders. Direct citizen feedback can be achieved via innovative new forms of registering opinions and expertise in diverse and arcane policy areas. For example, regulations.gov is a one-stop website for citizens to find, view, and comment on U.S. federal regulations and other federal actions. Online social media can also facilitate online public meetings, aggregate online responses and opinions, and establish collective ratings and rankings. At the same time, citizens can also self-organize, take collective action, and create e-petitions in an effort to force public debate or action on critical issues or topics.

At this point, the privacy risks of over-collecting the personal data mentioned above begin to take on a new and potentially ominous character. Citizens may well wonder what their governments know about them, and what decisions are being taken about them based upon that information.

The French EDVIGE example illustrates the negative public reaction to revelations of wide-scale harvesting of personal information by government agencies. Similar reactions have occurred in other Western democracies, for example, against the failed U.S. "Total Information Awareness" program proposal,[vii] and the Canadian HRDC longitudinal database, subsequently disbanded in the wake of public backlash.[viii]

Callout: The Proposed EDVIGE Database in France

On July 1st, 2008, the Office of the French Information Commissioner forced the Government to publish a hitherto secret decree, authorizing the creation of a new security database to track anyone over the age of 13 who has been "active in politics or the trade unions or who has a significant role in business, the media, entertainment or social or religious institutions" and who the authorities believe are "likely to breach public order". This database would contain information ranging from telephone numbers and details of taxes and assets to sexual orientation.

The new database, known as EDVIGE, sparked a firestorm of opposition from French unions, non-profits, and civil liberties groups. A massive petition drive against the program has already garnered over 170,000 signatures. Hervé Morin, France's secretary of defense, has called the database a "strange mixing-up of categories," Morin has questioned whether it is "useful to gather data such as telephone numbers, sexual orientation, and details of taxes and assets and the like without knowing exactly what the point is." A former member of the French data protection agency declared: "The Edvige database has no place in a democracy... The electronic Bastille is upon us."[2]

As Michael Zimmer observed:

"While it might be useful and fun to have locational data automatically associated with your images, considerable privacy concerns emerge as an externality. For instance, law enforcement officials can simply search for all photos online matching the location and timing of a certain political rally in order to broaden their ability to keep records of who was present."[ix]

Whether carried out by government organizations or by private sector actors and agents, online personal data aggregation can lead to forms of discrimination when decisions about that individual are involved. It may be a job application denied because of the contents of a Facebook page, or a service benefit delayed because of an imputed ineligibility, or the quiet imposition of some new and subtle restrictions.

Asymmetries of knowledge tend to foster asymmetries of power. Armed with greater and more detailed knowledge about its citizens, government organizations can embark on social engineering and manipulation on an unprecedented scale. Indeed, in November 2007, the U.K. Information Commissioner published some advice for government bodies that want to share information but think data protection laws prevent them from doing so. The advice note gives a rough idea of the mindfulness public bodies ought to have for human sensibilities when they start shunting data between computer systems. The U.K. government itself had a review done of how data protection law might prevent it from realizing its grand vision for information sharing — the rough conclusion was that an omniscient state might know enough about people's lives to justify its interference in their private affairs even when no laws were broken![x]

2. Source: www.theregister.co.uk/2008/09/11/france_database_tumulte/. Decree: www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019103207&dateTexte= . Online petition: http://nonaedvige.ras.eu.org/ .

Data minimization is the answer, and it must be applied by government organizations thoroughly at every stage of the information life cycle, from collection through use and disclosure to retention. The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

Whether you are in government, or run an ISP, a search engine, or a research project, the principle of Data Minimization should rule. Universal privacy practices require that strong limits be placed on the processing and storage of personal data. In today's online world of constant data availability, privacy requires data minimization at every stage of the information life cycle: If you don't need the data, don't collect it in the first place; if you don't need it any more, then destroy it securely — don't keep it any longer than you need to. Full stop.

Data Security

Highly decentralized, participative information structures needed to facilitate more efficient service provision bring with them serious implications for data security — a critical component of privacy and trust. Data security refers to ensuring confidentiality, integrity and availability of (personal) data. Of course, good data security alone does not guarantee good privacy, but it is nonetheless an essential sine qua non element of privacy. All governments that are subject to public sector privacy legislation are bound by strong commitments to ensure strong data safeguards. These commitments will be challenged in new ways by Web 2.0 values, applications, and technologies.

U.S. Justice and Commerce department representatives are recommending a "defense-in-depth" protection for their agency websites. "The Web is a collaboration method, but the benefits of collaboration will not be realized unless that collaboration is done securely," said Michael Castagna, U.S. Commerce's chief information security officer. "We must understand the promise and peril of technology. Criminal syndicates are targeting intellectual assets such as credit card data and personal information and then are selling that information."[xi]

> Enhanced democracy, convenience and efficiency will not be features of Government 2.0 if the security (confidentiality and integrity) of personal data involved in the transactions cannot be assured or trusted.

While it may be efficient to connect, aggregate and centralize large volumes of data, it also becomes more efficient to lose that data, have it stolen or accidentally disclosed. The scale of security risks becomes magnified. Uses of open source software, open standards and protocols also offer efficiencies, but with unknown or uncertain security price tags. Such actions can create significant points of vulnerability, risk and failure. At the same time, with so many different participants and data touch points involved, accountability for data protection can become diluted and harder to assure. Governments in the U.K. and U.S. have been rocked by revelations

about poor data security practices involving the loss or theft of millions of sensitive personal records.[xii] Putting this data online will compound the security risks. Public confidence and trust hangs in the balance.

Police in Canada, the U.S. and the U.K. have been using YouTube in order to disseminate video footage, with a view to identifying criminals caught by surveillance cameras.[xiii] While such collaborative efforts by law enforcement may be justified in specific cases, other efforts may open the doors to discrimination or abuses, especially where excessive personal information is revealed, is factually incorrect, or may be interpreted wrongly and out of context — with potentially devastating consequences for the affected individuals. Efficiency should not come at a price of justice and due process, nor the security and liberty of the individual involved.

The same caution should apply to decisions by public organizations to make available its information storehouses to the public for further use and value-added processing.

Thanks to Web 2.0 technologies, the voluntary sector can take on a growing share of certain public service responsibilities or tasks, such as reporting facts, situations or crimes or mobilizing societal resources in support of worthwhile public goals (e.g., public health and disaster relief). The power of Web 2.0 technologies and Web-based architectures of participation is that the many eyes, ears, minds of citizens — wherever they are — can be more easily engaged in new forms of collaborative governance.

Key to such collaborative efforts, however, is the release of structured government data on economic, social and socio-economic indicators. Applications such as sense.us, gapminder.org and chicagocrime.org use the collaborative effort of individuals to build upon, analyze and enhance large amounts of public data, not just introducing efficiencies but also helping to create new value-added information products.

But here, too, there are data security and privacy risks as "public" or "anonymized" data may become re-identified or otherwise associated with individuals. Again, caution is warranted. A recent example from the private sector offers a cautionary tale: in 2006, an employee at AOL posted 19 million search queries by 658,000 AOL subscribers so that computer scientists could use them for research. The data had no names attached. But individual AOL subscribers were able to be identified, along with their search profiles, and even confronted by reporters. AOL pulled the data down and apologized, but copies had already been made. They continue to be available online.[xiv]

The question of whether personal information has been sufficiently de-identified prior to public release is a critical privacy matter in light of the tremendous growth of data being collected and disseminated on the Web. The identifiability of individuals in prescription and other health records, census documents, court documents, crime statistics, and even Internet protocol (IP) addresses, among others, remain the subject of intense scrutiny and contention.[xv] Public sector organizations traffic in all these data areas, and must be especially vigilant in ensuring that personal data has been effectively de-anonymized to the fullest extent whenever released to the public for further uses.

Data Access

What is new and exciting is the potential reinvigoration of the "access principle." Expressed by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)[xvi], access is defined as follows:

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time;

- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

> "The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard"[3]

The Guidelines go on to note that "The right to access should as a rule be simple to exercise" and be subject to as few exceptions as possible. The concept relating to online access and security was the focus of a U.S. Federal Trade Commissioner committee report issued in 2000.[xvii]

Modern technologies make it feasible, on a scale never before imagined, to allow citizens to directly access information held about them, to learn of its uses, and to play a more direct role in the care and management of this data. In an era of Government 2.0, initiatives that fail to understand this access principle, and fail to engage citizens in a more direct and participatory role, will have higher hurdles to overcome in order to establish enduring confidence and trust in their information management practices.

3. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html, para 58

The Big Idea: Individual Participation and Control

> The privacy principle of individual participation seeks to involve the data subject as directly as possible in the care and management of his/her own personal data held by others throughout the data life cycle.

The Web 2.0 phenomenon is defined by an overriding ethos of enabling user participation and collaboration, the opening up of hitherto closed processes, user-generated and user-controlled content, and innovation on a mass scale. We should expect, then, that Government 2.0 will become more open, accountable, and "citizen-centric" than ever before. Yet, most e-government initiatives are often conceived, developed, hatched and run with minimal direct involvement or participation of the citizens themselves. The results have been mixed, at best. For privacy, closed and unaccountable data management practices can result in overcollection, misuse and loss of ever growing stores of citizens' personal data, undermining public confidence in public institutions of governance at a time when trust is more critical then ever to successful projects.

Fortunately, privacy can help rather than hinder this process.

Individual participation is the fundamental privacy principle. It includes (informed) consent, rights of access and correction, and of control. Government organizations that collect, use and disclose personal data can enable these individual rights of participation through open and accountable information management practices.

Web 2.0 technologies and applications can make personal information directly available to citizens on a scale never before seen in history, allowing them to review and edit their data, to set preferences, to direct uses, and to learn how their data has been disclosed and used. By participating more directly in the management and direction of personal information used by governments, citizens may become empowered in ways never before dreamed. They can hold governments accountable for uses, and go farther to shape government services in innovative, customizable and unique ways.

Empowered citizens are ones that can fully exercise informational self-determination, that is, the right or ability to exercise control over the collection, use and disclosure of their personal information.

Data Co-Management

We are already seeing the beginnings of a more participatory role for citizens in the management and care of their personal information held by government organizations, resulting in improved efficiencies, data accuracy and relevance — and trust.

One EU award-winning initiative in Norway is doing exactly this: providing a self-service online government account that remains relevant and up-to-date, which engages citizens directly in the care and management of their personal information, and which takes transparency, openness and accountability to new levels.[4]

Similarly, the Government of Estonia has gone even further to make available all its citizens' personal information to them online via use of a special e-identity cards, citizens' accounts, and a government portal. "The eID cards allow an Estonian citizen to access all data held on them. By inserting the ID into the smart card reader on a computer and keying in two security codes, a person may - through just one portal — pull up details held on approximately 20 databases which contain a wide range of information including personal insurance policies, entries on the land registry, or registration number and model of car."[5] The entire system of access is reinforced by strict legal, technical and procedural safeguards against unauthorized access and misuse.

The trend towards vesting people with direct access, aggregation, and control powers over their personal data held by multiple entities is illustrated by the emergence of online personal health records (PHRs) and consumer access services designed to help individuals make secure connections with health data sources in an electronic environment. Two of the most prominent PHR initiatives, Microsoft HealthVault and Google Health seek to put the patients in control of their own personal data and allow them to become the data aggregators. Grad Conn, Microsoft's director of health solutions group, observed that "There are silos of information about you or me spread everywhere. Different organizations have a little piece of you, so it's difficult to get a clear longitudinal view of your health history and issues."[6] What is remarkable is that these new patient-centric "infostructures" or networked platforms are being created outside of — but connected to — established institutional health data repositories. By providing the means to patients to play an active central role in managing their own health data, Microsoft, Google and others anticipate profound transformative impacts across the entire health care sector.

Similarly, Facebook — the largest social networking platform in the world — already empowers users to manage their personal information with fine-grained privacy settings and preferences, providing evidence of what is possible in personalization and control options to over 100 million online users.

If, thanks to Web 2.0 technologies, managing health care data is becoming more patient-centric, and managing personal activity data online is becoming more user-centric, then is it just a matter of time before the management of personal data by governments will become more citizen-centric?

Co-managed approaches to government interactions allow citizens to, for example, directly and securely input and/or verify personal data online rather than rely on intermediaries (paper, post office, bureaucrats) to process the data over a longer time cycle. In 2008, for the first time, a majority of North Americans e-filed their income tax returns using free or inexpensive

4. Details of the MYpage Self-Service Citizen's Portal at: www.epractice.eu/cases/mypage

5. "Security and Privacy in Estonia," by Lodge Juliet, Mayer Terry, A Research Project Funded by the Sixth Framework Research Programme of DG Research (23 May 2006), at: www.libertysecurity.org/article959.html

6. Rosie Lombardi, "Consumer control over personal medical data is coming to Canada," *InterGovWorld.com*, 08 September 2008, at: www.itworldcanada.com/a/search/42adc562-c0a8-0006-001d-88f64bbf545d.html

Web-based tax software that validated results before filing, and received their refunds quickly and directly into their bank accounts. This example illustrates the considerable efficiency gains for both governments and citizens made possible by new online self-serve tools.

Certainly, the prospect of enhanced efficiencies by allowing citizens to directly access their personal records in order to easily verify, correct and even attach conditions to their data is tantalizing. Projects to allow citizens to verify electoral roll status or advise of address change via Web-based tools are being piloted.

In the U.K., a new social care "operating system" pilot is showing promising results. Part of the "Putting People First" initiative, the in Control project allocates budgets to social care recipients so they can shape, with the advice of professionals and peers, the support they need. This participative, self-directed approach "delivers personalised, lasting solutions to people's needs at lower cost than traditional, inflexible and top-down approaches, by mobilising the intelligence of thousands of service users to devise better solutions."[7]

But to succeed, citizen-centric co-management of personal data will depend critically upon two enabling conditions:

1) A secure "citizen-relationship management" infrastructure. Governments must establish trusted back-end data systems that are capable of bringing personal information from disparate government silos together in real-time, and of making it available to citizens in a wide range of formats. They must also be able to receive and carry out citizen requests and operations on the data.

2) Robust privacy-enhanced systems of citizen identification and authentication. Governments must ensure that the right people are viewing, accessing and managing the personal data in question. However, without the ability to verify the identity of citizens, the data security risks associated with online access are enormous, and potentially unlimited. Clearly, there are significant challenges ahead in order to realize the Government 2.0 vision, and to ensure the continued protection of individual privacy in the Web 2.0 era.

7. J. Bartlett, C. Leadbeater, and N. Gallagher, *Making It Personal*, Demos Group (January 2008), at: www.demos.co.uk/publications/makingitpersonal

Conclusion

Governments must protect personal information within their care against privacy breaches and ensure control by minimizing personal data at every stage of the information life cycle, from collection to retention and including secure destruction and protecting the data against unauthorized access, tampering or inappropriate disclosure.

How these privacy meta-principles — data accountability, data minimization, data security, data access, data co-management — are to be operationalized in any given Government 2.0 context will vary. Simply put, personal data must be managed responsibly and credibly by trusted public authorities. As governments experiment with Web 2.0 technologies they will need to consider the implications for their data governance and management practices. Clear, self-imposed limits on the collection, use, disclosure and retention of all personal information must be established and observed. Regardless of program objectives, all personal data must be effectively secured against unauthorized access, tampering and misuse. New Web 2.0 values, applications and technologies may increase the risk, but do not change the privacy imperative or the applicability of longstanding privacy principles.

The use of Web 2.0 technologies in government to foster transparency and facilitate richer interactions between service providers and citizens needn't come at the expense of personal privacy. In fact, this report argues that Web 2.0 technologies could even be part of the solution. Given the appropriate public policy framework, readily accessible information technologies could empower citizen clients to co-manage their own personal information. A permission-based system can enable citizens to exercise informational self-determination by applying their online privacy preferences — as consumers and, equally, as creators.

Endnotes

i. Zittrain, Jonathan. *The Future of the Internet and How to Stop It*. (2008, Yale University Press). p. 201

ii. "Terrorist Watch List Tops 1 Million", July 14, 2008. See also the ACLU Watch List Counter at www.aclu.org/privacy/spying/watchlistcounter.html and also Audit of the U.S. Department Of Justice Terrorist Watchlist Nomination Processes, U.S. Department of Justice Office of the Inspector General Audit Division, Audit Report 08-16 (March 2008) at: www.usdoj.gov/oig/reports/plus/a0816/final.pdf

iii. McConnell, M. E. (2007). "Overhauling Intelligence" Foreign Affairs. at http://www.foreignaffairs.org/20070701faessay86404/mike-mcconnell/overhauling-intelligence.html

iv. Intellipedia is a project of the Office of the Director of National Intelligence, which is the head of the U.S. intelligence community. Analysts belonging to the 16 agencies of the community participate. Intelligence agencies of the U.S. were under pressure after failing to prevent 9-11. Investigation pointed to the failure of internal coordination as one of the reasons. Strong reform was then launched from the top, using wiki as a tool. At the same time, younger analysts demanded this reform from the bottom. This Wikipedia-like software allows analysts from different agencies to produce joint reports, which are more robust as they also include dissenting voices.

v. Avery, Simon, "Patriot Act haunts Google service" *Globe and Mail* (March 24, 2008) at www.theglobeandmail.com/servlet/story/RTGAM.20080324.wrgoogle24/BNStory/Technology/ and "US Patriot Act deters Canadians from Google service," Out-Law News, 28 March 2008, at: www.out-law.com/page-8988

vi. See "IBM Social Computing Guidelines" at www.ibm.com/blogs/zz/en/guidelines.html

vii. For further information, see discussions and links available at: http://epic.org/privacy/profiling/tia/ and www.aclu.org/privacy/spying/14956res20040116.html

viii. See Privacy Commissioner of Canada, "News Release: Privacy Commissioner applauds dismantling of database," May 29, 2000 at: www.privcom.gc.ca/media/nr-c/archive/02_05_b_000529_e.asp

ix. Zimmer, Michael. "Privacy and Surveillance in Web 2.0: Unintended Consequences and the Rise of 'Netaveillance'" at: www.anonequity.org/weblog/archives/2007/05/privacy_and_surveillance_in_we.php

x. Ballard, Mark. "U.K. regulator urges caution on data sharing," *The Register,* 29 May 2007, at: www.theregister.co.uk/2007/05/29/data_sharing_stopgap/

xi. Campbell, Dan. "Justice, Commerce warn of Web 2.0–and 3.0–security risks" Government Computer News 03 April 2008 at www.gcn.com/online/vol1_no1/46063-1.html

xii. See, for example, the July 2006 report of the U.S. Department of Veterans Affairs, Office of Inspector General, "Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans," at: www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf and the independent Poynter Review final report (June 2008) on the U.K. government's loss of 25 million confidential personal data on Child Benefit recipients at: www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm.

xiii. For example, see: http://technology.canoe.ca/Internet/2006/12/15/2806655-cp.html

xiv. See "AOL apologizes for release of user search data" and "AOL's disturbing glimpse into users' lives", CNET News, August 7, 2006, at: http://news.cnet.com/AOL-apologizes-for-release-of-user-search-data/2100-1030_3-6102793.html and http://news.cnet.com/AOLs-disturbing-glimpse-into-users-lives/2100-1030_3-6103098.html

xv. Research by Dr. Latanya Sweeney (http://privacy.cs.cmu.edu/people/sweeney/publications.html) and by Dr. Khaled El Eman (www.ehealthinformation.ca) has been critical. See Dr. El Emam et alia "Overview of Factors Affecting the Risk of Re-identification in Canada" (May 2006) accessed at: www.ehealthinformation.ca/documents/HealthCanadaReidReport.pdf and www.ehealthinformation.ca

xvi. See: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

xvii. U.S. Federal trade Commission, Final Report of the FTC Advisory Committee on Online Access and Security (May 2000), at: http://www.ftc.gov/acoas/index.shtm

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
CANADA
M4W 1A8

Telephone: (416) 326-3333
Toll-free: 1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): 416-7539
Website: www.ipc.on.ca
E-mail: info@ipc.on.ca