IBM Global Business Services

IBM Institute for Business Value

Government 2020

Resolving the "privacy paradox"

Practical strategies for government identity management programs

IBM Institute for Business Value

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive brief is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realize business value. You may contact the authors or send an e-mail to iibv@us.ibm.com for more information.

Resolving the "privacy paradox"

Practical strategies for government identity management programs

By Dennis Carlton, Peter Graham and John Reiners

In today's digital age, citizens seeking greater convenience and security in their travels and transactions are demanding more effective identity management solutions from their governments. At the same time, there is strong opposition, on privacy and civil liberties grounds, to some proposed government initiatives. We call these apparently conflicting reactions the "privacy paradox" – caused by the power of technology to on one hand empower and on the other, raise concerns among some citizens that they could be controlled. We believe it's time for governments to recognize this paradox and, like their counterparts in the private sector, begin to respond to public demand for identity management solutions that not only deliver improved services, but that also engender trust and confidence that personal data will be protected.

Introduction

Many governments are at a critical stage in tackling identity management projects. In response to increasing international travel and the growing number of network-based transactions, new and improved approaches are in development, driven by digital-age technology. Yet many of these programs, such as Real-ID in the United States and the National Identity Scheme in the United Kingdom, face strong public opposition because of their perceived potential to compromise personal privacy and civil liberty. Public sensitivity to privacy concerns continues to grow in the wake of news stories about governmental losses and unauthorized use of personal data. Further advances in technology – including the ability to combine and analyze more information from more sources – are likely to intensify public reactions to identity management programs.

Data security lapses occur in both the public and private sectors. However, it is the *volume* of information collected across different government agencies – and the threat of what governments can do if they combine personal data and use it in new ways – that concern civil liberties and privacy advocates. For these reasons, government identity management programs will continue to be challenged and are likely to remain at the center of ongoing debates on privacy.

Many in government recognize that past errors have been made, perhaps by concentrating too much on identifying the benefits to government – rather than communicating the benefits of effective identity management to the public. We believe that new approaches are needed, based on an understanding of prevailing public attitudes about sharing personal data with government, and how these attitudes are evolving in response to the increased capabilities of the latest technologies.

Governments can take lessons from other industries, such as Healthcare and Financial Services, that have successfully implemented new identity management programs. In this paper, we identify three strategies that have contributed to the success of such private programs, and that we believe offer practical insights to help governments address both sides of the privacy paradox:

- Develop an underlying business model – based on an understanding of stakeholder requirements – that aligns accountability, encourages desired behaviors and respects privacy concerns.
- Exploit the latest technologies through an open and flexible approach to solution development that supports interoperability and helps build stakeholders' trust.
- Reassure the public that government has the capabilities to manage personal data; offer citizens solutions for dealing with situations that go wrong.

Many private sector identity management programs have been broadly accepted by the public. Significant benefits – many of which were not anticipated at the design stage – have been delivered to numerous stakeholders. We believe that government identity management programs could provide additional advantages. Through their sheer scale, governments can drive the adoption of identity standards, and develop a supporting business model for identity authentication and the use of personal data. If widely accepted, these advances would likely be welcomed by citizens, as well as by many organizations in the private sector. This could lead to the creation of an identity infrastructure that mitigates the privacy paradox, and opens the way for enhanced public safety and the continued growth of online commerce.

Resolving the "privacy paradox"

Practical strategies for government identity management programs

Privacy and identity management in the digital age

Governments around the world are pushing ahead with a range of identity management programs, applying advanced technologies like biometrics to improve the effectiveness of identity-based applications, including identity cards, drivers' licenses and passports. Digital technologies open up new possibilities for online transactions with governments – offering the promise of greater protection against fraud, higher efficiencies through automated processes and more effective information management. However, these initiatives also raise public concerns about whether governments can be trusted to responsibly manage and use personal information.

In our October 2007 white paper "Identity Management in the 21st Century,"[1] we reported on our survey of government leaders in identity management. We noted that good progress was being made in developing identity management strategies, but also sounded a warning – concluding that "Governments should take immediate action to improve data integrity, system security and constituent privacy."[2] Since publication of that paper, the debate on the impact of government identity management programs has intensified – fueled by well publicized security breaches and losses of government data.

The public's concerns about government identity management schemes are complex, and will vary by country. It is likely to be a combination of concerns that governments will:

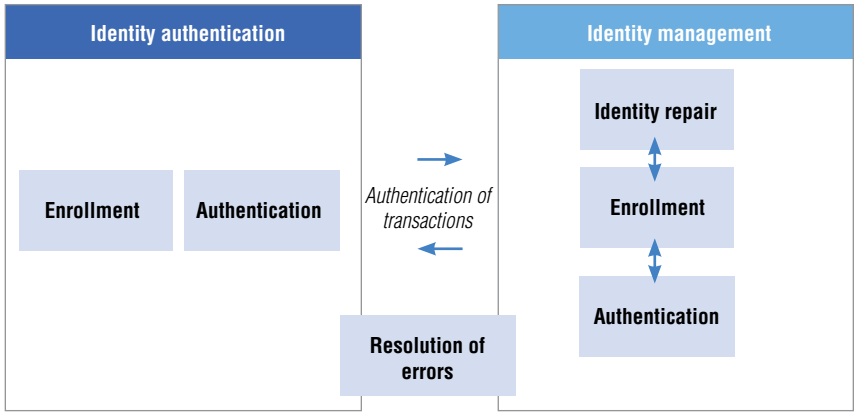
- Not be able to keep personal data accurate and up-to-date
- Not be able to keep information secure – making it vulnerable to loss, or access and use by others
- Collect and use personal information in ways not intended and not visible to the subject

These issues of data integrity, security and privacy are all closely related, and can be hard to disentangle. Data integrity and security can be tackled by a combination of smart technologies and rigorous policies and procedures (though there are still many complexities that are subject to ongoing research – some discussed in recent IBM papers).[3]

This paper concentrates on privacy – an issue that is particularly challenging, since it is dependent on public attitudes, and is more resistant to technical solutions and internally focused management disciplines. We also believe that overcoming privacy concerns is fundamental to the question of trust, and must be resolved before convincing the public to fully embrace identity management solutions.

Identity management is employed in many different situations, including face-to-face interactions using paper-based identity credentials. Most of the concerns relating to privacy have to do with the digital recording of personal data, which can form a permanent record that can be shared, combined with other data and used in ways not intended by the subject (see Figure 1).

FIGURE 1.
Different privacy issues are relevant at different stages of the identity management process.



Source: IBM Institute for Business Value.

Identity management can best be viewed as a series of interconnected processes relating to the handling of personal data. Each of these processes raises different privacy concerns. For example, in the case of identity authentication (confirming that an individual is who they say they are), privacy concerns primarily relate to impersonation. For identity management (when personal data is used for transactions, or maintained and shared with others), privacy advocates seek to make it harder to misuse or compromise this data.

Understanding the privacy paradox

Governments can draw insight from a number of surveys that track citizens' evolving attitudes toward personal data and privacy. For example, in 2008 the IBM Institute for Business Value carried out a survey of 4400 consumers of insurance products in eleven countries. The goal was to understand their behaviors when releasing personal data.[4]

The results suggest that individuals see a trade-off between the increased value of a service and the consequent erosion in their privacy. Citizens favor a service when it is more convenient, saves them time or money, or provides some other benefit (such as a reward program) or a combination of these. They will want to reduce the cost to them, whether it is financial, inconvenience or a perceived reduction in their freedom to act. We would expect a very similar trade-off with public sector identity management schemes.

However, because of the potentially more severe consequences of unauthorized use, and perhaps a lack of trust in government's capabilities to keep the data accurate and secure, we would forecast the trade-off to be more pronounced – with larger sections of the public reluctant to hand over personal data, and more needing compensation or reassurance via improved services, stronger protections or other benefits.

The essential nature of the privacy paradox – trade-offs between the growing demand for online services, for example, and the demand for protection of personal data – compels governments to weigh such potentially conflicting demands when developing identity management programs.

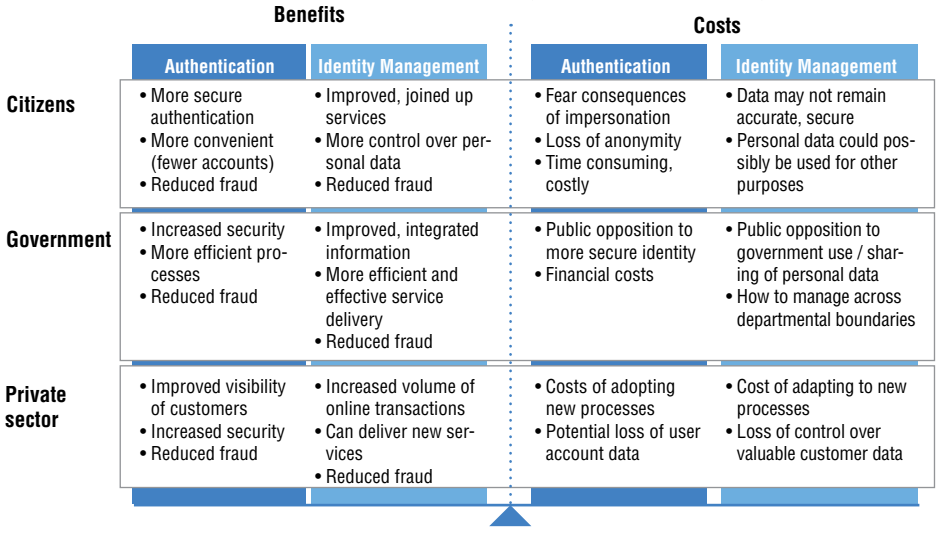
Similar trade-offs between the benefits sought from new online services and the costs of increased control can be expected of other stakeholders in authentication and identity management (see Figure 2).

While different stakeholders will have different perspectives, the benefits of reducing online fraud and enjoying better, cheaper and more conveniently delivered services are sought by all. Yet there are fears that this could lead to an erosion of users' privacy and concerns over the costs and implications on existing business models. We call this complex series of trade-offs the privacy paradox, best explained as the result of the dual nature of digital communications – to empower and raise public concerns of increased control.

As new capabilities for collecting, storing, manipulating and analyzing information emerge, attitudes regarding the use of personal data will evolve. Likewise, as more people conduct online transactions for various purposes, new privacy-related issues are coming to light. For example:

- The combination of cheap, efficient and pervasive sensors, mobile and high-speed networks, and more powerful data mining and analytic software increases the capability for surveillance.
- Web 2.0 applications have increased the volume of personal information on the Internet – information that can be widely shared and "mashed" with other applications, such as mapping or facial recognition software.
- Government agencies increasingly seek access to privately held personal data (such as phone records, e-mail traffic, closed-circuit television recordings or Internet searches).

FIGURE 2.
Different stakeholders will have their own trade-offs between the benefits and costs of government identity management programs. Governments will need to address both sides, delivering benefits while addressing their concerns.



Source: IBM Institute for Business Value.

Growing public concerns about privacy are reflected in the media; yet the volume of online transactions in both the public and private sectors continues to grow as a larger percentage of the public conducts business and social networking online. So we expect the essential nature of these trade-offs to remain – compelling governments to develop more practical identity management programs that "build in" privacy solutions.

A practical approach to identity management

The controversy over privacy and identity management polarizes opinions. Some believe that privacy concerns will simply go away as people become accustomed to releasing their personal data without any adverse consequences. On the other hand, privacy advocates can be blind to the capabilities of new technologies that enhance privacy and security.

We argue that both sides of the controversy make valuable points. New technologies offer the potential for vastly improving identity management applications – providing substantial benefits to citizens in terms of more convenience, better services and greater efficiency. Privacy concerns are very real, and are likely to increase as technologies advance and public awareness grows.

To build public support, approaches should tackle both sides of the privacy paradox – delivering benefits to citizens while reducing the impact on their privacy. Following are practical strategies that governments can use to achieve this objective.

1. Develop an underlying business model that delivers benefits to all stakeholders.

Governments are increasingly urged to make their identity management solutions more citizen-centric. This mirrors an emerging trend towards "citizen centricity" across public sector services. Yet citizen centricity is more than a slogan or a way of presenting programs to the public; it means that solutions have been fundamentally designed with the interests of the citizen at the forefront. To go further, identity management solutions should be developed in a collaborative and transparent way, with implementers held fully accountable for the results.

It is important to remember that government identity management applications are part of a complex ecosystem. While citizens are paramount, there are a number of other important stakeholders – public sector agencies, private sector organizations, other national governments and international bodies – whose requirements must also be considered (see sidebar, *Danish healthcare: Engaging with stakeholders*).

Private sector identity management solutions routinely recognize that to part with personal information, the consumer must be offered something in return, such as shopping discounts. Many successful public sector programs also deliver benefits (for example, frequent travelers who provide their biometric details enjoy time savings when passing through immigration controls).

The underlying business model needs to fulfill stakeholder requirements by aligning accountability, encouraging desired behaviors and respecting privacy concerns.

Danish healthcare: Engaging with stakeholders

The Danes benefit from one of the most sophisticated medical information systems in the world. A common network, electronic health records and a portal provide citizens with a wide range of online health services – from booking appointments, renewing prescriptions and purchasing prescriptions from pharmacies, to in some cases enabling electronic consultations with doctors.

Key to success of the project was an active approach to engaging the multiple stakeholders, including citizens, general practitioners, pharmacies, hospitals, clinicians and health administrators at local and national levels. An organization, Medcom, was created to manage the implementation, which was jointly funded by central and local health authorities, pharmacies and other health organizations. As it was seen as independent, it was effective at involving a large number of stakeholders in developing and agreeing to the standards underpinning the system.

The interests of these different stakeholders were considered throughout implementation. For example, clinicians received incentives to invest in systems and were rewarded with quicker reimbursement. The levels of adoption across different authorities were reported to encourage take up. Vendors were encouraged to upgrade to Medcom standards, with promises that their applications would be bought. Citizens were offered a range of new services that could be accessed easily.[5]

Refining the business model

The insights generated by a deeper understanding of the privacy paradox will need to be applied to the business model of the identity management program – designed to motivate desired behaviors among all participants, at all stages of the identity management process. People should be encouraged to enroll in the system, take responsibility for supplying accurate data, help to verify its accuracy over time, and facilitate the effective use and sharing of that data, all in the context of overcoming privacy concerns.

Much research is being done in the areas of behavioral economics to understand consumer behavior relating to privacy, and how incentives can be used to encourage desired behaviors.[6]

For example, it is important that accountability for providing and maintaining the accuracy of data be assigned to those who are best placed to verify it is correct and have an interest in keeping it accurate. Transaction flows will work best if the party that benefits from the transaction provides incentives to the provider of information.

Effective ways of influencing behaviors and aligning incentives include using pricing (for example, subsidizing the cost of enrollment) and legislation, such as the California Senate Bill 1386, which requires organizations to notify all citizens if there has been a security breach of unencrypted data. An innovative concept is to create a market for personal information. While a substantial market already exists, the property rights are currently held by those

who collect, compile and manage personal information – rather than the individuals who provide it. These third parties can actually impose costs on individuals by passing information on for other purposes, without the individual being involved in the transaction.[7]

If this market was reversed, and people were able to (in effect) "lease" their data to others for a specific use in exchange for a fee or other benefit (and with restrictions on reuse), a number of positive results could follow. For example, the providers of the information would be encouraged to supply data. Since they receive payment or a reward, they would feel responsible for its accuracy. The buyer would feel more confident in the quality of the data, could ask to be reimbursed if its quality was poor, and would be motivated to protect it, since loss or misuse would incur costs or other penalties.

Effective identity management programs should incorporate additional principles to help assure that individuals maintain control over their personal data. For example:

- Personal data must be obtained by lawful and fair means and, when appropriate, with the knowledge or consent of the data subject.
- Personal data should be relevant to the purposes for which it is to be used.
- The purposes for which personal data is collected should be specified no later than at the time of data collection; subsequent use should be limited to the fulfillment of that purpose. Consent should be obtained if personal data is to be used for other, unrelated purposes.
- Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.
- Personal data should be protected by reasonable security safeguards (against risks such as loss or unauthorized access, destruction, modification or disclosure).
- Means should be readily available for establishing the existence and nature of personal data and how the data is being used.
- An individual should have the right to view data relating to them, and to challenge data they believe to be incorrect. If the data is incorrect, it should be rectified or erased.
- An organization holding personal data should be accountable for complying with these principles, and have a nominated point of contact for dealing with related issues.

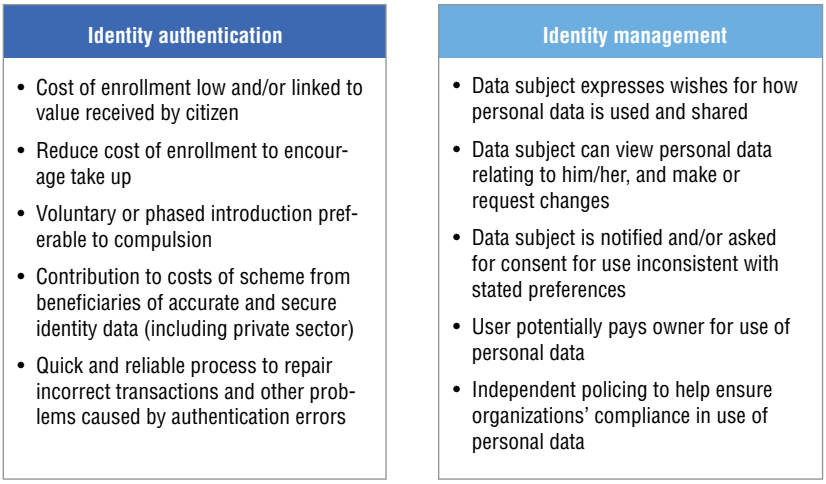
Some governments are already adopting some of these principles. For example, the Netherlands e-government program establishes the principle that personal information is the property of the individual, not the state.[8]

Figure 3 shows the potential implications of applying identity management principles (accountability, encouraging desired behaviors and safeguarding constituent privacy) to the different stages of the identity management process.

The design of the actual identity management business model will of course be much more complex. In practice, it will not always be possible to follow all of these principles. There may be existing legislation that imposes restrictions on how personal data can be used. Governments can hold some identity-related

Governments can also improve identity management by exploiting the latest technologies and by using approaches that can support interoperability and help build stakeholders' trust.

FIGURE 3.
These principles need to be applied to all stages of the identity management process.



Source: IBM Institute for Business Value.

data, such as offenses committed, against the owner's will. In rare cases (undercover surveillance, for example) an individual should not be aware of its existence.

The identity management process must also account for those in society who won't be motivated through incentives, such as those who lawfully object to identity management programs, or criminal elements who actively seek ways to undermine or exploit them.

For these exceptions, and to help ensure that the government does not abuse its position as a monopoly and custodian of data, there must be further checks and controls (for example, from trusted independent authorities) that citizens can access if they have a concern about how their personal data is being used.

Adopting these principles would have implications for the design of the identity management system. Individuals would need a way to store and communicate their privacy preferences, and associate those preferences with the data (in the metadata, or "data about the data").The transactions between the owner of the data, the holder of the online data and the ultimate user of the data will also need to be fundamentally different, particularly if payments may ultimately be made.

Realistically, the scope and scale of such an identity management system mean that it could only be undertaken by a government; however, by facilitating a market-based approach based on secure identity authentication, the benefits could spread to the private sector.

2. Develop standards-based solutions that build stakeholders' trust

A range of new secure Privacy Enhancing Technologies (PETs) can help with both face-to-face and online identity authentication and identity management, and are being successfully deployed in both the public and private sectors (see Figure 4).[9]

FIGURE 4.
Privacy enhancing technologies are becoming available for all stages of the identity management process.

Identity authentication	Identity management
• Biometrics (facial, fingerprint, iris) • Radio Frequency Identification (RFID) • Smart cards • Identity tokens and bank card readers for online transactions • Completely Automated Turing Test To Tell Computers and Humans Apart (CAPTCHA)	• Data anonymization (use of pseudonyms) • Data minimization (only supplying essential data) • Digital signatures for digital messages, transactions and data transfers • Enhanced encryption of data held in databases and other media (such as flash drives) • Data matching

Source: IBM Institute for Business Value.

While PETs can offer individuals more control over their personal information, it is important that governments build public confidence and trust through the way they design and implement identity management systems. This involves adopting an open and flexible approach to solution development, supporting identity management protocols and standards, and building privacy measures into the design of software.

By championing open standards, governments can:

- Help build trust in government solutions, since they will be more transparent to members of the public.
- Encourage interoperability with other identity management solutions, other government agencies, the private sector and internationally.
- Avoid becoming "locked in" to particular vendors.

A services oriented architecture (SOA) is particularly suitable for identity management systems, since it provides a standards-based approach for managing data from multiple legacy systems, with the potential to increase flexibility and significantly lower operating costs.

Considerable progress is being made by standards bodies and others in developing identity management standards. For example, in January 2008, the Identity Theft prevention and Identity Management Standards Panel (IDSP) – part of the American National Standards Institute – created an inventory of current standards and guidelines. Its report documented progress achieved and the gaps that need filling.[10]

Because of their scale, governments are uniquely positioned to establish standards in the area of identity authentication by creating secure, multi-factor online authentication processes. Private sector organizations handling particularly sensitive personal data could benefit from using the same approach. In fact, the potential for government to provide solutions to private sector challenges in this way was highlighted in the IDSP report and Sir James Crosby's report for the UK government on identity assurance, published in March 2008.[11]

Increasingly, software suppliers are developing open solutions that provide safeguards in the way that personal data is handled. For example, the open source Higgins project is creating an identity framework that is

The public will need reassurance about governments' capabilities to manage personal data, as well as solutions for dealing with situations that go wrong.

encouraging software suppliers to develop a number of interoperable, privacy-enhanced identity related applications (see sidebar, *The PRIME project: Ongoing research into privacy-enhancing identity management*).[12]

The PRIME project: Ongoing research into privacy-enhancing identity management

Privacy and Identity Management for Europe (PRIME) is a European Union (EU)-funded research project that is working closely with international standards organizations (ISO, W3C and ITU-T). It focuses on solutions for privacy-enhancing identity management that supports end users' sovereignty over their private spheres while facilitating enterprises' privacy-compliant data processing. PRIME aims to demonstrate viable solutions to privacy enhancing identity management by delivering a reference framework, requirements, an architecture, design guidelines, protocols and prototype implementations. The guiding principles of the Prime Project are to put individuals in control of their personal data.

A follow-on project, PrimeLife, has two goals: to provide scalable and configurable privacy and identity management in new and emerging Internet services and applications (such as social networking), and to develop tools that will protect individuals' privacy throughout their lives.[13]

3. Provide reassurance and recourse when things go wrong

Governments will need to convince citizens that their personal data is well managed by implementing rigorous, transparent internal policies and procedures for how they handle and manage personal information.

Many private sector organizations recognize the importance of demonstrating best practices in this area to reassure their customers and staff. For example, IBM is considered one of the pioneers in implementing specific measures to clarify its position on handling personal data – establishing a Chief Privacy Officer accountable for all issues relating to personal data across the corporation.[14,15]

To create public trust, government identity management programs must also recognize that exceptions occur, and that effective safeguards exist to quickly rectify mistakes and support citizens when things do go wrong.

Providing legislative support and independent oversight

To reinforce the message that identity management systems are to provide services to citizens, rather than provide information to government, there needs to be independent scrutiny, such as a requirement for systems to be subject to regular independent audit. Citizens need to have legal rights relating to their personal information. There also needs to be effective policing of these rights by an independent authority, such as an ombudsman, who can effectively penalize transgressors and to whom citizens can turn when seeking reassurance on how their personal data is being used (see sidebar, *Payment Card International: Driving industry good practices and enforcing compliance*).

Payment Card International: Driving industry good practices and enforcing compliance

The Payment Card International Data Security Standard is an example of leading corporations in a particular industry sector (in this case payment cards) getting together to establish a set of rules and good practices relating to security and privacy of data.

The Data Security Standard was launched in 2004 and updated in September 2006. A further version is due in late 2008. It aims to protect the interests of all stakeholders in the payment card industry by giving accreditation to merchants who follow best practices. The Data Security Standard contains 12 core guidelines. Merchants need to receive independent assessment from a qualified security assessor that they have complied, and undergone regular audits. Small merchants are exempted.

According to Visa Inc., 75 percent of the largest merchants had complied and almost two-thirds of medium-sized merchants had done so by the end of 2007.[16]

Most countries have some legislation relating to data privacy. Although different, these laws are loosely based on the guidelines set in place by the OECD in 1980. The European Union's directive 95/46/EC (EC 1995) on the protection of personal data has produced overarching principles that countries must comply with.[17] In the U.S., a more devolved approach has been followed, with particular states and industries advancing policies and supporting legislation.

However, there are two threats to current legislative approaches. First, the adoption of legal privacy protection is uneven internationally, which may create difficulties in managing and sharing data across borders. The IBM Institute for Business Value calculates an annual ranking of nations' Internet legislation. The latest report showed pockets of excellence, yet large disparities between and within regions.[18] While efforts are underway (such as the Asia Pacific Economic Co-operation's [APEC's] privacy framework[19]) to tackle these constraints, the volume of cross-border information continues to grow – calling for further harmonization of standards to protect personal data.

Secondly, privacy legislation is struggling to keep pace with the ways people interact online, and how data can now be combined from various sources. Web 2.0 technologies, social networking and the explosion of online communications channels present a new set of challenges – the implications of which are still unclear. "The essence of Privacy 2.0 is that governments and corporations, or other intermediaries, need not be the source of the surveillance," writes Jonathan Zitrain in *The Future of the Internet and How to Stop It*. "Any activity is subject to recording and broadcast."[20] Databases holding personal information are no longer owned and managed only by governments and organizations, and are now widely distributed.

With many governments now at a critical stage in tackling identity management projects, both technological advances and lessons from private sector counterparts can help address the privacy paradox.

Legislators face many questions. For example, how do you apply different national privacy policies to data that frequently crosses borders and is often held in "the cloud" (actually large data centers often off shore)? How do you protect an individual's right to correct false or damaging personal data when it is fellow citizens who are producing and sharing this data? When do governments have the authority to access personal data from private sources (telephone records or online searches)?

As lawmakers address these challenges, further legal safeguards concerning the use of personal data in the digital environment can be expected. Practically speaking, this means building flexible identity management solutions that place privacy concerns at the core of systems and process design, rather than bolting them on as an afterthought.

Conclusion

The time is right for governments to invest in identity management programs. Privacy concerns will not go away and will probably increase. Technical solutions are becoming available now that if implemented thoughtfully, can deliver effective identity management while offering protections to personal data. There are several successful examples to follow.

We recommend some immediate steps that governments can take to get started with their identity management project:

- Engage cross-sections of stakeholders at an early stage.
- Establish a collaborative and open project structure to encourage an ongoing dialogue on project objectives and proposed solutions.
- Identify relevant good practices from other countries and other sectors.
- Develop a high-level business model to encourage intended behaviors, maintain privacy and deliver stakeholder benefits.
- Identify current and future technologies that can help improve identity management and enhance individuals' privacy.
- Understand technical standards (existing and under development) related to identity management.

Governments are in a unique position. Because of their scale and status as a respected authority, they can drive through solutions that mitigate the privacy paradox. If they are bold in developing flexible solutions with the interests of many stakeholders in mind, they can set the path for a more broad-based identity infrastructure that *can* benefit governments, the private sector and, most important, citizens, for many years to come.

About the authors

Dennis Carlton is Global Director of Government Trusted Identity Management Services, IBM Global Business Services, where he oversees the development of Identity Management solutions. Denny has over 20 years of experience leading the development of complex IT systems and products, including the development of automated fingerprint identification systems. He is a regular platform speaker on the subject of identity management. Denny can be reached at *dennis.carlton@us.ibm.com.*

Peter Graham is Global Director of Border Security and Immigration, IBM Global Business Services. He has over 15 years of experience working with the UK Government in implementing solutions in the areas of border security, immigration and home affairs. He was Strategy Director of the e-borders program and Director of Special Projects for UK Border Control. Peter can be reached at *peter.graham@uk.ibm.com.*

John Reiners works for the IBM Institute for Business Value, where he researches, writes and deploys studies on issues of importance to the public sector. He has eighteen years of experience as a managing consultant, including roles in business transformation programs for both the public and private sector. John can be reached at *john.reiners@uk.ibm.com.*

Contributors

Bryan Barton, Vice President, Global Industry leader, Customs, Borders and Revenue Management, IBM Global Business Services

Kent Blossom, Vice President, Trusted Identity Solutions, IBM Tivoli®

Tim Corcoran, Identity Management Subject Matter Expert supporting IBM Global Business Services, U.S.

Peter Dare, Identity Management Subject Matter Expert, IBM Global Business Services, UK

Martin Kenseley, Senior Managing Consultant, IBM Global Business Services, Australia

Norbert Kouwenhoven, European Industry Leader, Customs, Borders and Revenue Management, IBM Global Business Services

Yu Kit Lee, Executive IT Architect, Public sector, IBM Sales and Distribution

Dr. W. Russell Neuman, John Derby Evans Professor of Media Technology in Communication Studies and Research Professor at the Institute for Social Research, University of Michigan

References

1 Barton, Bryan, Dennis Carlton and Dr. Oliver Ziehm. "Identity Management in the 21st Century." IBM Institute for Business Value. October 2007. https://www-304.ibm.com/jct03004c/easyaccess/fileserve?contentid=128886

2 Ibid.

3 For data integrity, see "Building Public Trust: the role of Information Assurance in UK public sector transformation." IBM, June 2008. https://www-304.ibm.com/jct03004c/easyaccess/publicuk/gclcontent/!!/gcl_xmlid=141899/. For security, see Neuman, Dr. W. Russell. University of Michigan. "The demand for security." Prepared for IBM Global Business Services, October 2008. ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/gbw03065usen/GBW03065USEN.PDF; "Security and Society." IBM Global Innovation Outlook, September 2008. http://ibm.com/gio; "At the cutting edge of strategic solutions for the Global cyber challenge – anticipating and meeting the Government's cyber needs." IBM Global Business Services, October 2008. http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=pm&subtype=br&appname=GBSE_GB_MS_USEN&htmlfid=GBB03020USEN&attachment=GBB03020USEN.PDF

4 Maas, Peter, Albert Graf and Christian Bieck. "Trust transparency and technology: European customers' perspectives on insurance and innovation." IBM Institute for Business Value. February 2008. http://www-935.ibm.com/services/us/index.wss/ibvstudy/gbs/a1029260?cntxt=a1000058

5 The Computerworld Honors Program, 2007. http://www.cwhonors.org/viewCaseStudy.asp?NominationID=299

6 For example, see "The economics of privacy." Maintained by Alessandro Acquisti. Carnegie Mellon Heinz College. http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm#new

7 Anderson, Ross and Tyler Moore. "Information Security Economics and Beyond." University of Cambridge. http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf

8 Cross, Michael. "What a National Identity Scheme Should Do." *The Guardian*. October 2008. http://www.guardian.co.uk/technology/2008/oct/02/cross.idcards

9 Camp, L. Jean and Osorio, Carlos A. "Privacy-Enhancing Technologies for Internet Commerce." August 2002. KSG Working Paper No. RWP02-033. http://ssrn.com/abstract=329282 or DOI: 10.2139/ssrn. Also see "Promoting Data Protection by Privacy Enhancing Technologies (PETs)." European Union. May 2007. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/598&format=HTML&aged=0&language=EN&guiLanguage=en

10 "Findings and Recommendations. The Identity Theft Prevention and Identity Management Standards Panel (IDSP)." Final report, Volume 1: January 2008. http://www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx

[11] Crosby, Sir James. "Challenges and Opportunities in Identity Assurance." HM Treasury. March 2008. http://www.hm-treasury.gov.uk/identity_assurance.htm

[12] "Higgins: Open Source Identity Framework." Eclipse Foundation. http://www.eclipse.org/higgins/index.php

[13] "PRIME – Privacy and Identity Management for Europe." The PRIME Consortium. https://www.prime-project.eu/

[14] McCreary, Lew. "What was Privacy?" Harvard Business Review. October 2008. http://discussionleader.hbsp.com/hbreditors/2008/10/what_was_privacy_1.html

[15] "Security and Society." IBM Global Innovation Outlook. September 2008. http://ibm.com/gio

[16] See http://en.wikipedia.org/wiki/PCI_DSS. And Visa Inc., "PCI Compliance Continued to Grow in 2007" press release. http://corporate.visa.com/md/nr/press753.jsp. Also see "Escaping PCI Purgatory – compliance roadblocks and stories of real world success." IBM. April 2008. ftp://ftp.software.ibm.com/software/tivoli/whitepapers/SEW03004-USEN-00_HR.pdf

[17] "EC Directive 95/46/EC." European Commission. http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[18] "E-readiness rankings 2008." IBM Institute for Business Value. April 2008. http://www-935.ibm.com/services/us/index.wss/ibvstudy/gbs/a1029550?cntxt=a1000055

[19] "APEC Ministers Endorse Privacy Framework for Information." Washington Law. November 16, 2005. http://news.findlaw.com/wash/s/20051116/20051116170043.html

[20] Zitrain, Jonathan. *The Future of the Internet and How to Stop It.* Allen Lane. 2008.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2008

GBE03114-USEN-00