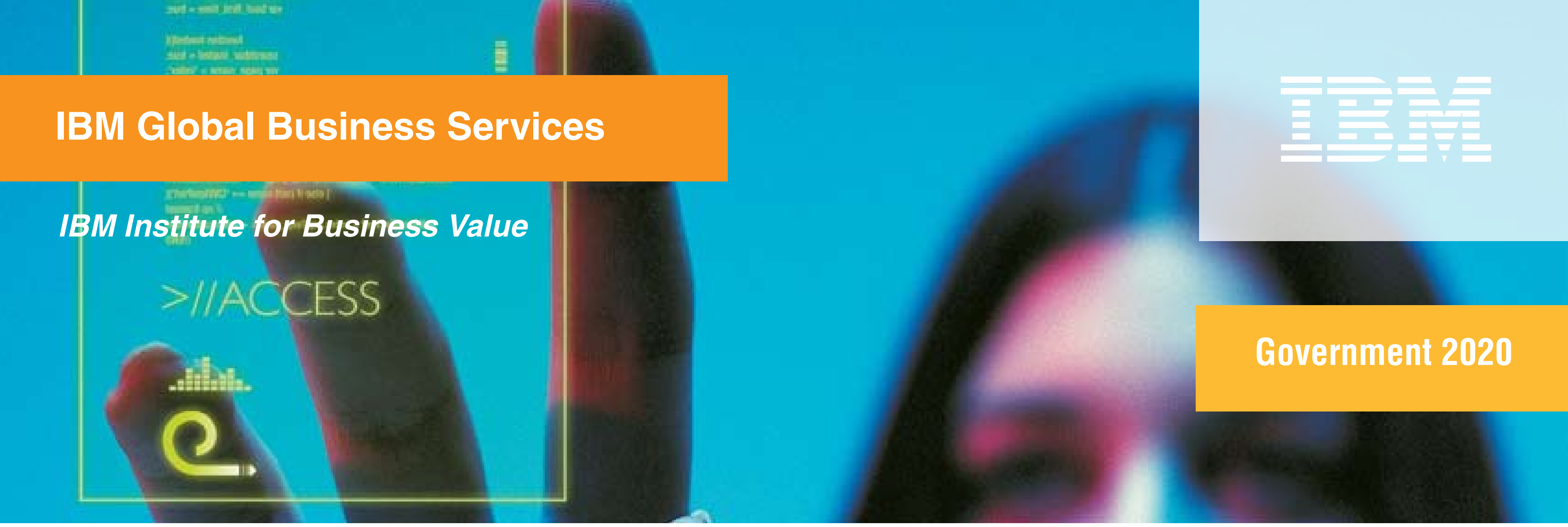

IBM Global Business Services

IBM Institute for Business Value

IBM

Government 2020

Resolving the "Privacy Paradox"

Practical strategies for government identity management programs

The digital age promises to deliver effective identity management solutions for governments, as citizens demand greater security in their travel and transactions. Yet at the same time, there is strong opposition, on privacy and civil liberties grounds, to some proposed government initiatives. This tension between the power of technology to both empower and control citizens is what we call the "Privacy Paradox." We believe it's time for governments to recognize this paradox and, like their counterparts in the private sector, begin responding to the public demand for identity management solutions that are both effective and engender trust and confidence that personal data is not being abused.

Many governments are at a critical stage in approaching identity management projects. New and improved approaches, driven by digital-age technology, are in development as a result of increasing international travel and the growing number of transactions carried out over computer networks and the Internet. Yet many of these programs, such as Real-ID in the United States, the national identity scheme in the United Kingdom and the rejected Australian Access Card, are facing 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 frequent news stories about governmental losses and abuse of personal data. Further advances in technology, and in how increased volumes of information from different sources can be combined and analyzed, are likely to intensify the "Privacy Paradox."

While data security lapses occur in both the public and private sectors, it is the threat of what governments can do if they misuse private data that concerns civil liberties and privacy advocates. For this reason, government identity programs 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 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. Such an approach likely will be welcomed by citizens, who increasingly demand improved services and added convenience, but want to minimize the aspects of their lives government can control.

Governments can take lessons from segments within the private sector, such as healthcare and financial services, that have successfully implemented new identity management schemes. We have identified three strategies that have contributed to the success of these private programs and that can, we believe, provide practical insights to guide governments:

1. Understand stakeholder requirements and develop an underlying business model to deliver the benefits and address concerns via aligning accountability, incenting desired behaviors and respecting privacy concerns.
2. Exploit the latest technologies through an open and flexible approach to solution development that encourages interoperability and builds stakeholders' trust.

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.

	Benefits		Costs	
	Authentication	Identity Management	Authentication	Identity Management
Citizens	• More secure authentication • More convenient (fewer accounts) • Reduced fraud	• Improved, joined up services • More control over personal data • Reduced fraud	• Fear consequences of stolen/lost identity • Loss of anonymity • Time consuming, costly	• Data will not be accurate, secure • Personal data will be used for other purposes
Government	• Increased security • More efficient processes • Reduced fraud	• Improved, integrated information • More efficient and effective service delivery • Reduced fraud	• Public opposition to more secure identity • Financial costs	• Public opposition to government use / sharing of personal data • How to manage across departmental boundaries
Private sector	• Improved visibility of customers • Increased security • Reduced fraud	• Increase volume of online transactions • Can deliver new services • Reduced fraud	• Costs of adopting new processes • Potential loss of user account data	• Cost of adapting to new processes • Loss of control over valuable customer data

Source: IBM Institute for Business Value.

3. Provide reassurance to the public that government has the capabilities to manage personal data and offer recourse through effective independent agencies for dealing with situations that go wrong.

These identity management solutions from the private sector have been broadly accepted by the public. Significant benefits have been delivered to many stakeholders, a number of which were not anticipated at the design stage. Successful government identity management programs similarly could provide many additional benefits. Governments, through their scale, could encourage the adoption of identity standards and a supporting business model for identity authentication and the use of personal data. If widely adopted, these advances would likely be welcomed by citizens and many in the private sector and could represent important steps toward creating the identity infrastructure that mitigates the "Privacy Paradox" and opens the way for enhanced safety and continued growth of online commerce.

To request a full version of this paper when it becomes available, e-mail us at iibv@us.ibm.com

How can IBM help?

- ***Strategy and Change:*** Help to define your identity management strategy, business case and roadmap.
- ***Government Trusted Identity Services:*** Help with implementation of identity management solutions, from design through implementation, including IT infrastructure, privacy-enhancing technologies and systems integration, using approaches such as component business modeling (CBM) and service-oriented architecture (SOA).
- ***Selected consulting services:*** Support in designing and implementing changes to organization operating models, detailed processes and training services to support the transition to a trusted organization.

Key contacts:

IBM Institute for Business Value:	John Reiners, *john.reiners@uk.ibm.com*
Government Trusted Identity Service:	
Global	Bryan Barton, *bbarton1@us.ibm.com*
	Peter Graham, *petergraham@uk.ibm.com*
Americas	Dennis Carlton, *dennis.carlton@us.ibm.com*
Europe	Norbert Kouwenhoven, *norbert.kouwenhoven@nl.ibm.com*
Asia Pacific	Martin Kenseley, *kenseley@au1.ibm.com*

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

Produced in the United States of America
October 2008
All Rights Reserved