

CROSSING BOUNDARIES:

PRIVACY, POLICY, AND INFORMATION TECHNOLOGY

By:

Harvey Schachter

Freelance Writer



New Directions – Number 5

©L'Institut d'administration publique du Canada, 1999
The Institute of Public Administration of Canada, 1999

ALL RIGHTS RESERVED/TOUS DROITS RÉSERVÉS

The Institute of Public Administration of Canada

The Institute of Public Administration of Canada (IPAC) is the leading Canadian organization concerned with the theory and practice of public management. Its scope covers governance from the local to the global level. It is an association with active regional groups across the country. The Institute recognizes and fosters both official languages of Canada

IPAC/IAPC
1075, rue Bay Street
Suite/bureau 401
Toronto, Ontario
M5S 2B1 CANADA

Tel./tél: (416) 924-8787
Fax: (416) 924-4992
e-mail/courriel: ntl@ipaciapc.ca
Internet : www.ipaciapc.ca

L'Institut d'administration publique du Canada

L'Institut d'administration publique du Canada (IAPC) est la principale institution canadienne qui s'intéresse à la théorie et à la pratique de la gestion publique tant au niveau local qu'au niveau mondial. C'est une association composée de groupes régionaux actifs à travers tout le pays. L'Institut reconnaît et promeut les deux langues officielles du Canada.

ACKNOWLEDGEMENTS

The Institute of Public Administration of Canada gratefully acknowledges the support of the following departments of the Government of Canada in making possible this sharing of information:

Department of Finance
Department of Health
Department of Industry
Department of Justice
Department of Revenue
Treasury Board Secretariat
Department of Human Resources Development



Crossing Boundaries: Privacy, Policy, and Information Technology

EXECUTIVE SUMMARY

Computers have become ubiquitous in society and government. The old mainframes have given way to personal computers that were once networked in offices but that are now linked through much of society thanks to the Internet. That has profoundly changed the way in which we work and relate to one another.

But government has changed less than one might imagine. Hierarchy has not been flattened by computers; vertical is still the rule in an age where computers encourage horizontal linkages. And while the federal government has brought in new privacy legislation to cover the private sector, it has yet to investigate whether in this new era of databases and information-sharing, privacy rules within its own sphere need to be sharpened.

The Crossing Boundaries roundtable chaired by Reg Alcock, parliamentary secretary to the minister of intergovernmental affairs, considered these issues in four half-day sessions on Parliament Hill. Our ranks included MPs, civil servants, academics, journalists and privacy advocates who jostled about a proper agenda for privacy, policy and information technology. The bulk of our attention was on the federal government, but we also explored connections to other levels of government, and our findings apply to all governments in Canada.

We called the project Crossing Boundaries because we knew from earlier research that the ability to share information more broadly was a key enabler of much of the structural change we observe in large private-sector organizations. Sharing data across traditional barriers is taking place between departments of the same government, between governments, and between governments and citizens.

The consensus at the roundtable was that the sharing of information was critical to the further development of systems and that privacy is the mainspring. On a practical level, expansion of information technology will only take place comfortably if citizens are assured that adequate privacy rules are in place and are being strictly adhered to. But we also came to realize that this is more than a practical matter, since it cuts fundamentally to the heart of democracy and the relationship between the state and citizenry. Privacy is an essential right, and in democratic societies intrusions by the state must be guarded against.

Thus, both practically and philosophically, government must ensure that informed consent is at the heart of its information technology policies. Transparency is also vital. And it is important to highlight these values now, at a relatively early stage in technological development, because systems will be more effective and cost-efficient if they are built according to such precepts at the outset.

It is also important, at this early stage, for government to develop a road map for information technology and decide whether it currently has – and wants – an information highway or country roads.

Government has barely scratched the surface on the possibilities for service delivery made possible by modern technology. Instead of automating control systems, government needs a vision of seamless delivery to the citizenry. People relate to government holistically, not by “silos,” and government must respond accordingly. If someone moves their residence, for example, why can’t he or she send in a change of address that will automatically be applied to all personal data held by government – not just at the federal level but also at the provincial and municipal levels? If someone has a problem with two government ministries, why can’t he or she call one number and have it dealt with by one representative of their government?

On the policy side, government has been even slower to consider the implications of information technology. Policy formulation is increasingly horizontal. Accountability is also increasingly horizontal, as are information networks. What does this trend suggest for the structure of government? What changes are needed?

There are other important issues as well, from the impact of information technology on equity, to learning, and to the unanticipated consequences of technology on political and social relations. Nobody underestimates the importance of technology. But government has yet to understand that information technology is a leadership issue.

Only leadership at the highest level can provide the necessary mandate for examining the opportunities of shared data on better service delivery to citizens. The House of Commons and – through the House – the public should also be engaged. It is essential that a philosophical starting point be accepted and that further investigation of these issues take place, if government is to manage technology rather than be managed by it.

OVERVIEW

The Crossing Boundaries roundtable began with an illustration of a rocket ship suspended in the air after lift-off. The illustration captured an exhilarating moment but also an instant of great vulnerability, when danger is at its peak.

It was an apt metaphor for the current explosion of information technology. This is an exciting time in history, with many Canadians mesmerized by the technological prowess of modern software, the Internet, and the splendour these advances seem to promise. In a recent book, *Cyber Rules*, Thomas M. Siebel and Pat House, executives with Siebel Systems, a leading American software applications firm, say that the advent of the World Wide Web is one of the great watersheds of history and that it ranks with the discovery of writing and the appearance of metal currency: “We will inhabit a world where distance no longer matters and where communication and data transfer will be virtually instantaneous,” they note.¹

But the rocket ship metaphor also failed to capture some important elements of this transformation that further underscore our vulnerability and danger. Every aspect of a rocket ship’s launch has been carefully planned. By contrast, the information explosion propelling governments, business and the general public today is anything but planned. Much is serendipitous, reactive or instinctive. Haste is common; indeed, it is considered a prerequisite for success.

More importantly, the rocket ship's trajectory is meticulously plotted. The crew knows exactly where it is heading. Information technology, on the other hand, is a frenetic scramble. We have little idea of the destination towards which we are soaring as a society, even less of how to steer.

Four laws underpin our uncontrolled flight:

1. Grosch's Law, which covered the period from 1940 to 1981, decreed that computer power increases as the square of the cost. That means if you doubled the computer investment, you got four times the power. That law drove the mainframe era.
2. Moore's Law, which covered the transition to personal computers, initially declared that the speed and capacity of the computer chip doubled every two years. But the time-frame had to be revised downward to eighteen months in order to keep up with the speed of innovation.
3. Metcalfe's Law, which took effect about 1985 and which will drive us until about 2005, focuses on transmission. It says that a network expands linearly with increases in size, but the value of the network increases exponentially. More simply, it is saying that the cost of adding one person to a network is minimal and that the benefit is exponential. And it contradicts the notion that value comes from scarcity, which shaped the industrial age mindset.
4. Moschella's Law of Transformation, which is expected to begin in 2005 but which is already affecting us today, says that when an organization becomes automated the transformation is not linear but a multiple. We will soon enter an era in which we will have minimal limits to processing power, communication power and memory. This will transform organizations and society.

Governments cannot control these laws. Governments have also been slow to take advantage of the possibilities these laws offer. Traditionally, government bureaucracies have been built by specialization and transferred completed portions of work to others. The boss handled conflict and coordination, giving shape to the standard hierarchical structure. But with computers and technology, staff can carry out more wide-ranging work, because the rules and information required are easily accessible from the computer memory. That opens the door to a case-worker framework: employees get broader responsibility; hand-offs and conflicts are reduced; and the hierarchy is compressed. It also encourages more out-sourcing and one-stop service.

The roundtable grew out of these changes and the need for government to better comprehend the implications. It drew together a diverse set of policy experts from both inside and outside government, with MPs, civil servants, academics, journalists, and privacy advocates gathering for four half-day discussions on Parliament Hill, under the auspices of the Institute of Public Administration of Canada. The sessions were chaired by Reg Alcock, parliamentary secretary for intergovernmental affairs, and were sponsored by

Health Canada, Human Resources Development Canada, Industry Canada, the Departments of Justice and Finance, Revenue Canada, and the Treasury Board Secretariat.

Jerry Mechling, director of the Program for Strategic Computing and Telecommunications in the Public Sector at the John F. Kennedy School of Government, Harvard University, was one of the introductory panellists who helped us understand these changes. His own position at Harvard, he notes, illustrates the problem: It was only in 1987 that university officials agreed that strategic communications and telecommunications are leadership issues and should be part of a school that is teaching governance. Governments have been even slower to grasp the strategic importance and leadership elements of information technology.

He observes that information technology in time will lead to a powerful transformation in government work design, with huge productivity pay-offs. But many issues will have to be settled first, as government deals with its own systems and the impact of information technology on society in general.

These issues include the following:

1. *Equity*: Information technology has the power to accentuate gaps in society between the rich and poor. How are we to ensure equal access to information and to the knowledge that technology makes available?
2. *Security*: The concern over the Y2K phenomenon highlights the growing dependence of government and society on information networks and the dangers we face. How do we preserve the security of data and the systems in which they are stored?
3. *Privacy*: Efficiency in a networked world is driven by re-utilization of information that is captured once and re-used time and time again. "But if it's my data, I may have valid concerns about who is using that data," noted Mechling. And people today, he said, have highly unrealistic notions: much more data is being stored than people realize.
4. *Crossing Boundaries*: Does information technology demand a re-thinking of government structures and a re-definition of how policy is developed and carried out? How do we align programs and information technology over multiple agencies and budget years – indeed, across different levels of government? How do we re-design government to take advantage of technology and provide greater efficiencies and enhanced service? Can government emulate the private sector in developing long-term partnerships with technology providers? How do we design government structures to handle the failure that technological innovation requires at times? Gaylen Duncan, president and CEO of the Information Technology Association of Canada, said, "Developing solutions is long-term, expensive, multi-department and multi-government. We can't even get it right in individual departments."
5. *Learning*: Governments will face huge investments in learning, both for its own staff and for society in general.

6. *Governance*: What is cyberspace? Who has jurisdiction? How do we handle pornography downloaded by a Canadian from a server, say, in Holland and paid to a server in Argentina owned by a California company? Whose laws apply? How is it coordinated? How do we handle the cross-border movement of data? “The next twenty years will be as important in constitution writing as 200 years ago,” Mechling said.
7. *E-commerce*: Canadian governments have a role in fostering this country’s transition into the e-commerce economy, now on the horizon. But Duncan warned that transformation will not be linear but exponential. Are we prepared? Can government move quickly enough? How do we develop government as a partner with the private sector in this quicksilver world of e-commerce?
8. *Unanticipated consequences*: When automobiles first appeared on roads, the major fear was that they would scare horses. Nobody sensed the implications for highway construction, the environment, or even the sexual mores of teenagers. It is equally difficult today to recognize the ultimate social implications of technology. But it is important for government, and the citizenry, to pay attention, since technology will affect political and social relationships.

Canada, of course, is not alone in this transition. The impact will be felt worldwide. South of the border lies a country that has been instrumental in the changes of the silicon era. The U.S.’s instinct is to avoid regulation and to allow freedom to flourish.

By contrast, Europe has been moving towards a regime of privacy protection and expects equivalent treatment by its trading partners. Its 1995 privacy initiative included the following guidelines:

- Permanent data must be treated in a legal and loyal manner.
- Data must be collected for a legitimate purpose.
- The information must be adequate to the purpose and not excessive.
- The information must be accurate and, if necessary, updated.
- The information must be conserved for a period appropriate for the purpose.

The individual involved must be informed about the process; have the right of access to the information; and have a right to refuse to give it. The treatment of the information must be confidential and secure. Excluded information includes personal data that reveals racial or ethnic origin; political opinions; religious or philosophical convictions; union connections; and details on health or sexuality. A national control authority must be in place to oversee privacy.

The private sector would have to indicate the contents of the data it collects and how data will be used. When executing a contract, the information collected must be legitimate. The individual must have a right to refuse to give information; must be informed clearly about how information will be used; and should be able to prevent it from being passed to third parties.

Traditionally, government proceeds in small steps. But in recent years the private sector has responded to the information technology revolution by taking great leaps, because companies fear that, even if *they* don't change, their competitors will change, and those companies that don't change will swiftly slide out of business. A prominent sentiment in our discussions was that government must learn to move more quickly, to respond to the same forces. And this will be difficult, Mechling reminded us, because "in government there's lots of pressure but not the fear you will go out of business."

Clearly, leadership will be required.

GOVERNMENT STRUCTURE AND SERVICES

Government is built on "silos," a configuration that has worked well over the ages but that does not conform naturally to the networked world of the future, let alone to the mindset of citizens. When seeking federal services or trying to fulfil requirements, citizens see themselves relating holistically to the Government of Canada, not to individual departments. And government does not conform well to the reality of policy-making, which generally spills beyond one department to units at all levels of government.

Information is the currency for much of this interchange. And as Moore's, Metcalfe's and Moschella's laws carry us into the future, it is important that we not let the segmented nature of government prevent us from imagining and developing the best possible structure.

It is also important that we not let the traditional budget processes become an obstacle. Governments operate in one-year cycles. Information technology is so expensive, and the consequences of investments so profound, that we must think long-term and develop budget procedures that enable rather than prevent such an outlook. Information technology also involves some gambling since systems change so quickly. Yet, governments are conservative forces.

Mechling argued that governments will have to make information technology a focus of attention in budget-setting, ensuring a horizontal, cross-cutting approach rather than one that confines outlays to single-year, single-department frameworks. Funds must also be created to ensure experiments in technology. These will ultimately be paid for by the savings produced, he argued.

In making these investments, we must remember that information technology is inextricably linked to what kind of government we want – centralized or decentralized. We have to ensure that information technology does not unwittingly determine the outcome. Information technology should be an enabler, allowing us to choose.

Presumably, whatever model we choose, we will still want to take advantage of the integrative opportunities that information technology allows. Certainly we will want to look at information across all departments. It is the only way to ensure we are getting value for money and that the systems fit together, with duplication eliminated. As Marlene Catterall, the MP for Ottawa West-Nepean, noted, government must ask of itself "Do we have an information highway or a whole bunch of back-country roads?"

We looked at some of those back roads and sleeker highways, trying to gain an under-

standing of the topography. In our minds was an observation by Gaylen Duncan that government is fundamentally automating control systems instead of building a relationship with the individual. If someone goes to their bank, for example, they do not want to have to give information to several people. He or she expects to provide information once and to have it accessible when needed. But with government, hand-offs and repeating information are all too common. "Government is talking of relationships but still automating control systems," Duncan insisted.

An indication of the patchwork was the fact that two departments alone – Revenue Canada and Human Resources Development Canada – have signed about 500 memorandums of understanding to share their information with other departments, agencies, levels of government, and private companies.

We began with a hypothesis about such sharing, based on the fact that some departments are information seekers and others are information providers. We thought it worthwhile to explore the power dynamic and tensions in such situations. But we were reminded that many departments have enormous amounts of information and that the issues of networking, privacy and power applied internally as much as externally.

Human Resources Development Canada, for example, holds information for a plethora of programs, from employment insurance to youth programs to the social insurance number to the gun registry: "We're the one department that touches every Canadian, from cradle to grave," said Jim Martin, director general, Internal Audit Bureau, Financial and Administrative Services. He added, "The tension is not between a department providing information and a department seeking information. It is a tension within the department itself on how to handle information and privacy." And it is not clear where the balance is – even in law.

But this departmental struggle with large databases may blind us to the larger issue of relationships with the individual citizen that Reg Alcock expressed in an imaginary scenario of a couple moving from Ottawa to his beloved Winnipeg. One person is receiving unemployment benefits. On the trip to Winnipeg, the couple decides to take a two-week vacation in the United States. They want to let government know about this change in their life, but it is not easy to reach the right people. Until recently, the federal government had 118, 1-800 numbers.

Why would it not be possible, instead, to call one toll-free number and have that answered by a person who could help that couple out? "Yes, your passports are updated," that person would advise. "We now have fixed your address for all government activities. We'll straighten the EI file to recognize the two weeks out of the country."

Why can't government be that efficient? It is not just security: Banks maintain security on electronic transactions and handle personal matters by telephone. Why can't government?

As well, in the private sector significant changes in organizational structure have followed technological investment. In governments, by contrast, technology investment has only led to increased transaction intensity and, in some cases, the slicing off of government activities to new forms. We have not seen the structure within government change – flattening the vertical nature of government, decentralizing dealings with the public and centralizing policy, to mirror private-sector adaptation.

continued on p. 9

The Health Infoway

Health ministries across Canada have been working together to build a “Health Infoway,” recognizing the importance of good information and effective communications in health care. The “infoway” serves as a good example of the intergovernmental systems that will eventually have to be built in many areas.

The recent report of the Advisory Council on Health Infostructure presented thirty-nine recommendations, of which twenty-six involve collaborative efforts by the federal–provincial–territorial ministries, showing what a tangle information can be. An additional six recommendations relate to aboriginal health.

The report notes, “Most of the first time patients visiting doctors’ offices, community clinics and hospital outpatient clinics or emergency wards bring with them little or no medical history, only their subjective impression. This situation adds a potentially dangerous haphazardness to diagnostic and treatment decisions. Even if the patient brings a record from a physician or health care professional, it is incomplete and unhelpful in all too many cases.”²

The Health Infoway would link all health records, not just records of sickness. The key recommendations include a health-information roadmap; health informatics and telematics standards; a tele-health task force; electronic health records; a national health surveillance network; and harmonization of privacy legislations.

Currently, various jurisdictions and even various administrations within jurisdictions record information in different ways. For example, hospital deaths are recorded. But some hospitals do not include individuals who are dead on arrival at emergency departments while other hospitals count them.

The national health surveillance network will allow laboratories to be networked. It currently can take six months to find out about a salmonella outbreak; if labs were networked, information might be communicated in a few days.

Andrew Siman, director general, Office of Health and Information Branch, Informational Analysis and Connectivity Branch of Health Canada, stressed that the “infostructure” must be built collaboratively and through consensus, as awareness is built. Major efficiencies will likely be attained. But the main goal must be better health: “It is important to understand that better access to better information leads to better decision-making on our health.”

Imagine a child who moves with his family from Ontario to rural Alberta. When the child develops a sudden illness that requires transport for treatment to Edmonton, the doctors would be able to collaborate. Necessary information could be shared such that when the child arrived at the Edmonton hospital, the physician would have had access to medical records in both provinces and would be prepared to act.

As an example of provincial initiatives, we looked at Alberta Well-Net, a partnership between the government, major health players and a consortium of companies. Information will continue to be collected, but it will be tied together electronically on common standards.

One challenge Alberta Well-Net faces is that the project will take a long time, and people will lose faith if early successes are not available: “People will have a problem today, and they don’t want to hear it will be dealt with in five years,” said Dan Bader, Alberta’s deputy minister responsible for strategic technology issues and CEO of Alberta Well-Net.

Reg Alcock suggested that to the extent the silos in government are changing, it is simply that they are turned on their sides. In some jurisdictions, one-stop service centres have been built, but when citizens enter they are confronted with desks from a variety of departments rather than with an integrated service.

The private sector accepts change more quickly because of the profit motive and the fear of being sideswiped by competition. In government, this motivation is missing and a classic generational problem exists as well. The generation in control harbours fears about technology and is not as comfortable or as aware of technology as younger people are. Lacking good signals of success, such as profit, public servants are reluctant to let go of their information flow.

To overcome that resistance in making reforms, empowerment must flow from the top. In the United States, Vice-President Al Gore played a prime role in this effort, as did the prime minister in Australia. Successful federal–provincial projects are often a result of policy agreement between the prime minister and a premier – the bureaucracy then fine-tunes and implements the policy. A large force overcomes turf protection.

The Service Canada initiative has been trying to spearhead the federal government's efforts to improve service delivery. Over the years, blue pages on government services have been included in phone books, 1-800 numbers were developed, and kiosks were set up in malls so that citizens could access information.

A major barrier, of course, is knowledge. Surveys show that 25% of citizens do not know which level of government to begin with when they have a problem involving government, and 60% had problems finding the right person once they found the right government.

Service Canada is working to ease that situation, trying to figure out ways in which government could respond more logically to citizen needs. The premise is that a department in one location with proper support from another department can provide information on behalf of that other department. Technology allows such support, but, at the same time, it cannot be expected that every public servant will know everything about government. Instead, Service Canada is trying to train designated employees and equip them with appropriate technology so that they can help direct people to the right source of information.

A pilot project in New Brunswick and P.E.I. is also looking at ways in which citizens can create their own Internet portal through which they can import information on the government services. In effect, this would be the individual's contact point with government. As he or she ages, the information on the site would change, adapting to the life-cycle of government–citizen relationships. Eventually we might all have our own individual portal.

But this service would presuppose some knowledge of government. And it wouldn't necessarily deal with another annoying aspect of citizen–government relationships: the burden of filling out forms, often with having to repeat information. A small business starting up in Ontario, to take one example, can be required to fill out thirty-seven forms. What if the individual submitted all the information once and each department received only the data it needed? Or if a person moved, why couldn't he or she submit the new address once and have it distributed to all the government departments – federal, provincial and municipal – that need to know about the change?

Technology holds the promise of enabling such solutions – if we get it right. As Alcock keeps asking: “Why can’t dealing with government be simpler? Why can’t you log in anywhere or call one number to deal with government?”

The answer in part, of course, is privacy and security. Systems that cut across departments open the possibility of abuse. What we expect from a bank – each customer-service representative knowing our entire transaction history – might be frightening when applied to government. Can it be arranged while maintaining privacy safeguards? What security safeguards are needed?

Beyond service delivery, there are questions of policy formulation and performance reporting that have to be considered, since these can drive and be driven by the nature of information technology. Do we know what we are building? Do we have any idea what we are mapping out when we are accumulating information? How does the nature of information technology affect governance?

Virtually all federal and provincial governments are now engaged in performance reporting. Often, collecting the data necessary to meet these obligations requires the development of complex and expensive systems. Once these are in place, they are difficult and costly to change. How confident are we that the performance indicators around which these systems are being constructed are the ones that we will want over the medium to long term? Can we adapt quickly enough and make appropriate changes?

Information technology, both in service delivery and policy, requires a re-thinking and perhaps a re-engineering of government. At its core, information – like so many of the challenges facing government – is horizontal while government is vertical. The challenge facing governments, then, is to realign policy-making, service delivery and program evaluation along a horizontal axis.

Information technology may now be the biggest agent of change within the public sector. Creating new systems and integrating old ones is making government more horizontal. But how well will the new, emerging architecture of government fit the horizontal issues and objectives? Can we be confident that governments are not exchanging departmental “silos” for a tangled “network” of systems that leaves policy-makers, service providers and program evaluators running off in all directions?

We may never build the superhighway of perfection. But we also must avoid getting clogged in an incomprehensible maze of back roads to nowhere.

PRIVACY

To technology specialists, privacy may at times seem like a hindrance, preventing them from achieving their goals. The reality is, however, that privacy is an essential element in the quest for better information systems. As the private sector has realized with e-commerce, privacy is necessary to allow them to achieve their technological goals. Members of the public need assurance of privacy and security when they are dealing with sensitive matters – be they about money or personal information – on new technological systems.

This can, however, lead to the mindset that permeated our initial roundtable discus-

sions: privacy is effectively a commodity that can be traded off. Planners must simply figure out how much privacy Canadians are willing to sacrifice to attain better efficiency from government and then negotiate or unilaterally implement such a solution.

But through our discussion, we came to a deeper understanding of the role of privacy in the information revolution. Our understanding starts by recognizing that privacy is an unfortunate word to use in these considerations, since it connotes something selfish or hidden. However, when considering government information systems, the word privacy is actually shorthand for a more profound and fundamental issue: the degree of intrusion the state should have. As federal privacy commissioner, Bruce Phillips observed, "The people who come to roundtables like this advocating privacy are doing more than that. They are asking: To what extent should we be re-defining the nature of the state's role in the lives of the citizens to suit technology?"

He reminded us that the first role of government is to defend the state and the second is to protect the security of its citizens. Efficiency is way down on the list. Phillips also noted that simply because technology allows something to happen does not mean it should happen – and it should not be left to bureaucratic whim to decide: "You have to make the technology fit the rights and not the rights fit the technology."

Privacy is an essential democratic right. The extent of privacy rights reflects our relationship to the state and the very nature of the society in which we live. Privacy rights also contribute to the health of that society. One-window shopping is an exciting possibility, but privacy is fundamental to human beings. And the privacy rights we are struggling to re-define in an interconnected world may be as fundamental as those that were developed with such rhetorical flourish and vision 200 years ago in the French and American revolutions.

At the same time, it is worth recognizing that privacy can be a barrier to democratic participation. For government to be more effective, it needs more information. As governments try to reach out and work with community groups and other third parties and involve them in policy formulation and implementation, information will have to be shared for program effectiveness and accountability.

This is an opportune time for such discussions and decisions, since, as a society, we are at an early stage of the information technology implementation process. Solutions will be easier and more effective if they are built into the systems now. At the same time, some participants in the roundtable warned against moving too quickly and suggested freezing experimentation.

It is also worth highlighting that just as technology can strip away rights it can also enhance them. It is possible, for example, to implement systems that automatically tell who accesses a file and which part of it, in a way that is beyond the capacity of traditional paper-based systems.

Informed consent and transparency are critical to developing a proper privacy regime for information technology systems. People must be allowed the opportunity to give consent to the collection and use of their information. They must be aware of the uses to which the information will be put. It must be easy to find out what is happening and to check one's own file.

Consent, it is worth stressing, cannot exist in monopoly situations. If a student does not consent to the use of personal information for the Canada Student Loan program by Revenue Canada, to whom else can he or she turn?

In our deliberations, privacy advocates kept asking: Can the individual opt out? If someone, for whatever reason, does not want personal information to be part of the Health Infoway, for example, can he or she refuse to participate? Is “no” an option? Governments will have to grapple with that touchy but fundamental question.

The Public Interest Advocacy Centre surveyed 2,053 Canadians about privacy in late 1994. It found that nine out of ten respondents would be at least moderately concerned if government departments and private firms, or if two private firms, shared information about them, while seven out of ten respondents would be moderately concerned if two or more government organizations shared information.

“Levels of concern are clearly higher when private firms are involved,” Frank Graves of Ekos Research Associates noted in his commentary on the results. “The difference could reflect less trust in private organizations than in government institutions. Government may be viewed as a safe, legitimate organization whose integrity requires such informational exchanges. Exchanges between government and private firms are likely to involve a commercial aspect and may therefore be more suspect in peoples’ minds than are exchanges strictly within government.”

According to the survey, Canadians assess each specific invasion of privacy in a pragmatic way. For example, circulation of health information from government agencies to insurance companies was viewed as a seriously invasive practice. On the other hand, computer-supported circulation of prescription information among pharmacists to ensure compatibility of multiple medications was only considered a moderately serious invasion of privacy: “The two instances dealt with circulation of sensitive health information, but the one which can be linked with possible negative consequences (insurance) was viewed as highly invasive while the one linked to a clear benefit (pharmaceutical prescriptions) was not viewed as so invasive,” Graves noted.

Ekos found that five interrelated elements explain privacy concerns by the public: knowledge and familiarity; transparency; control and regulation; rationale/benefit; and legitimacy/trust. Two items emerged as paramount. The first is control – does the individual give consent to, or have control over, the process? The second is the potential consequence – what is the probability of being adversely affected by the decision or action made on the basis of the information collected?

Also important were the following concerns:

- Is the information subjectively sensitive?
- Is the practice covert or open?
- Is the party that is using the information behaving in an ethical manner?
- What is the level of surveillance or external control imposed?
- How acceptable is the behaviour sought to be controlled?
- What is the probability of an individual actually experiencing the situation?
- How trustworthy or legitimate is the institution?

- How widespread is the practice?
- How important is the result or action?

Perhaps the most important finding was that direct experience actually *reduces* the probability that someone will find privacy invasion threatening. In fourteen of the fifteen scenarios tested, there was a negative relationship between prior experience of the situation and the likelihood of finding it an invasion. The exception was in the case of the government deducting child-support payments from tax refunds, where it might be expected that those experiencing the situation would feel particularly wounded.

The following generally recognized guidelines for privacy in Canada were set by the Canadian Standards Association (CSA):

1. *Accountability*: The organization is responsible for personal information under its control and should designate an individual (or individuals) who is accountable for compliance with the CSA principles.
2. *Identifying purposes*: The purposes for which information is collected must be clear before the information is collected.
3. *Consent*: The individual has to give consent to collection, use and disclosure.
4. *Limiting collection*: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization.
5. *Limited use, disclosure and retention*: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
6. *Accuracy*: The information must be kept as accurate, complete and up to date as necessary for the identified purpose.
7. *Safeguards*: Protection and security are required.
8. *Openness*: Organizations shall make readily available to individuals specific information about policies and practices in managing information.
9. *Individual access*: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. *Challenging compliance*: The ability should exist to challenge all practices.

Government information on individuals can be divided into two types: personal data, for which privacy concerns arise, and aggregate information that might be used for data-mining or program analysis, the use of which raises less concern unless the unit of analysis becomes small enough to permit identity of an individual.

Bruce Phillips noted that when people call his office with complaints they tend to be shocked at how much information sharing is already going on: “I wonder what the taxpayer would think if we said that we share tax information with 300 other agencies and institutions?” he asked.

One of the new threats to privacy is data-matching. Government can take two sets of data collected for different purposes, connect them, and troll for new revelations. This violates the CSA standards on limited use and the individual’s right to know how information will be used. But when it is initiated to detect fraud, it might be an invasion of privacy the citizenry approves of, according to the Ekos principles, since the purpose is laudable.

To Phillips, this is not enough: “If more information sharing is necessary, then informed consent is the *sine qua non*. If you can’t get the informed consent, it ought not to be done,” he insisted.

He cited two examples to illustrate the negative and positive aspects of data-handling. In the first example, an Employment Insurance (EI) official ran a data match of customs declarations by returning Canadians with lists of EI recipients. Phillips considered it a fishing expedition – a search and seizure of information – and took it to court, winning when a judge ruled the department exceeded its authority. A further Charter argument on the search and seizure issue is to be decided.

A second example was when the chief electoral officer decided the best way to establish a permanent electoral roll was to use updated addresses from tax records. Individual consent was sought through a question on the tax form, and over 80% of Canadians agreed to the information-sharing proposal.

Phillips believes that this shows permission can be gained in other instances if the privacy issue is properly addressed at the program-design level. But if consent cannot be gained, he argued privacy rights cannot be set aside. Another guideline the roundtable heard is that any departure from informed consent should follow the principle of Section 1 of the Charter of Rights: the purposes would have to be justified and reasonably accepted by Canadians.

Currently, individual departments do not have to consult the privacy commissioner before undertaking a project, and if they do consult the office they need not follow the advice. Phillips argued a better information-sharing review process is needed, either by fortifying his office or providing another element of review. He is not convinced that the privacy commissioner should be able to stop a department wanting to share information, but neither should the minister be able to proceed unilaterally. Perhaps some third agent should adjudicate.

Representatives of various departments we heard from stressed that they struggle with privacy and security issues and that they try to strike a proper note. The Health Infoway report, for example, repeatedly highlights the importance of protecting privacy. Privacy commissioners are being consulted on the building of the infoway, and a harmo-

nization accord on privacy is being negotiated between the federal government and the provinces.

The architects of that new system believe it can be more secure than the current process, with access restricted to those with a need to know. The advisory committee recommended that informed consent – clearly defined – should be the basis for sharing information. Alberta’s Dan Bader insisted that technology could build safeguards that are better than those in the current paper system. He finds it ironic that the public is comfortable seeing paper-based systems in a physician’s office and equates electronic records with the horror scenarios of movies.

At the same time, we were reminded that government has a legitimate interest in health data that might encroach on privacy rights: “Do I have the right to know [that] men over the age of fifty aren’t taking prostate tests or that a person visited the doctor 365 times last year?” asked Andrew Siman of Health Canada.

A comprehensive review of the federal Privacy Act was conducted in 1987 by the House of Commons justice committee and led to the report *Open and Shut*. Many useful reforms were suggested, but no significant action was taken.

Government departments today do not have to tell citizens that government holds information on them. “Shouldn’t we have a more liberated attitude than that?” asked Bruce Phillips. Investigative bodies can refuse to give information about what they have on an individual, without any injury being shown to the investigative process. On the whole, departments have been restrained in the use of these clauses. But in recent years, he maintained, departments have been taking advantage of loopholes when it is convenient.

In an era of ever-larger and sophisticated databases, it would appear to be time to review and re-invigorate privacy legislation at the federal level. Pippa Lawson, counsel to the Public Interest Advocacy Centre, pointed to Bill C-54: “Here we are putting in place strong legislation for the private sector, and the public sector is back in the Dark Ages.”

EQUITY AND E-COMMERCE

Governments are responsible not only for overseeing their own information technology but also for overseeing its expansion throughout society.

The roundtable recognized, but did not spend time probing, the federal government’s role in encouraging Canadians to use the emerging e-commerce economy. The roundtable also did not struggle with the important issues of international regulation of information that are now even more pressing with the growth of the Internet. These topics were beyond our time and scope.

We did spend some time on the issue of equity, which struck a chord. “My eighteen-month-old grandson is playing on a computer, and two minutes from my home are 1,000 kids who do not have access and then will have to compete with my grandson when they get to kindergarten,” said Marlene Catterall. “One eighteen-month-old child is as equally valuable as another eighteen-month-old child and should have equal access to the tools of life-long learning.”

Equity in government services is a fundamental principle. Systems should not create inequities in accessing public services. If a government service has to be through a computer, what kinds of inequities are we creating? How do we determine who has easy access and who does not – and how do we fix the problem?

Governments should also look at the potential of information technology for improving equity. How can we arrange technology so that we are working towards a more equitable society? Can information technology allow us to determine who wins with government policies, checking the benefits for men, women and children? Human Resources Development Canada looked at the gender impact of employment insurance changes, but budgets do not appear to receive any such analysis, even though modern technology makes that investigation easier.

The federal government's e-commerce strategy received a boost with Bill C-54, which was introduced on 1 October 1998. The bill attempts to build trust in the digital marketplace by securing privacy rights and to clarify marketplace rules by providing a legal framework.

Before C-54, Quebec was the only jurisdiction with privacy legislation covering the private sector. Part 1 of the legislation, on privacy, protects personal information that is collected, used or disclosed by organizations in the course of commercial activities. Parts 2 to 5, on electronic documents, recognize electronic signatures and provide for the use of electronic means by which to communicate or record information or transactions. The bill also amends the Canada Evidence Act, the Statutory Instruments Act, and the Statute Revision Act.

The bill attempts to create a climate of trust and confidence in the digital marketplace by providing a right of privacy for personal information gathered in the course of commercial activities. It builds on the CSA code – essentially putting the ten principles into law – and provides for recourse and redress mechanisms, through the federal privacy commissioner and the federal court. It would also allow Canada to adhere to the European rules on data protection.

The bill does not apply to information that is used, collected or disclosed for journalistic, artistic or literary purposes (although information gathered for the marketing purposes of the news media is not exempt). Information that is used, collected or disclosed for personal or domestic purposes is also exempted.

Specific exemptions from the consent requirements are for

- health or life-threatening situations;
- debt collection and fraud investigations;
- compliance with subpoenas, warrants or court orders;
- law enforcement, administration of an act, national security;
- statistical or scholarly study;
- conservation of archival or historical records; and
- as required by law.

The privacy commissioner can investigate complaints, call witnesses, compel evidence,

and visit business premises. The commissioner has the power to mediate disputes, audit compliance, and make findings public. Another major role of the commissioner is to undertake public education and awareness of the privacy rules: “The effectiveness of the complaints procedure will depend on the effectiveness of the privacy commissioner in making organizations aware of the requirements of the legislation,” stressed Michelle d’Auray, executive director of the Electronic Commerce Task Force.

Final recourse is to the Federal Court of Canada, which can use broad powers to order organizations to comply with the legislation. It can also order an organization to publish notice of any action taken to correct its practices and award damages, including punitive damages. The privacy commissioner, on the other hand, can issue a report on complaints but cannot issue an order.

For the first three years after passage, the law will apply only to federal works, undertakings, and businesses – federal broadcasting, telecommunications, banks and interprovincial transportation – under the federal umbrella. The law also applies to interprovincial and international trade in personal information – the selling of any personal information by a company across provincial or international borders. After three years, it will apply to all commercial activities by the private sector, including companies under provincial or territorial jurisdiction, unless exempted because a similar provincial law covers them, as in the case of Quebec. It also applies then to all transborder flows, including intra-firm transfers.

But the law does not apply to areas under specific provincial jurisdiction (provincial government, municipalities, universities, schools or hospitals); employee records in the provincially regulated private sector; non-commercial activities (charities, non-profit organizations, and professions such as law or medicine); and any government institution to which the Privacy Act already applies.

The bill will bring uniformity of privacy regulations. Members of the Canadian Marketing Association, for example, were abiding by the CSA code, but competitors outside the association were not.

In developing the law, d’Auray noted that several important lessons were learned:

1. Government administration and effectiveness depends on voluntary transmission of vast amounts of personal information from the private sector. Citizens are not always aware of such transfers, and consent is not always sought or obtained. It is given voluntarily to provide support of the administration of programs.
2. A citizen’s option to disclose information to government is rapidly decreasing. Technology makes data matching, access and tracking easier. At the same time, in other ways, it can also allow greater citizen control over information.
3. Public–private partnerships in information are essential to efficient and effective service delivery. As an example, the government receives employment tapes from companies and searches for individuals committing employment-insurance fraud. Banks transfer to Revenue Canada reports on interest on accounts. A game warden searching

for a poacher can approach an outfitter and obtain information. As well, a lot of health information is being transferred. While transparency in public-private information partnership is critical to citizen acceptance, there is not much citizen awareness of these transfers. And certainly there is little individual consent.

Moreover, there are concerns raised by the growth of government out-sourcing, as well as by the privatization and the creation of independent agencies. What privacy rules apply when government information or employee records are transferred outside of formal government structures? The federal Treasury Board now asks that departments try to maintain existing standards, but this is not a regulation, just an advisory.

In addition, as government cuts back, it might point people to the private sector for assistance. The Health Infoway, for example, might provide a link to an association that provides detailed information on a malady, but this association may have a policy of selling the names or e-mail addresses of site visitors to a pharmaceutical company.

Bill C-54 received general support from the roundtable, although there were concerns about some of the exemptions being too loose. But the feeling, again, was that a gap exists between the current marketplace for information and what citizens actually realize is happening: "Just because information is being collected does not mean it is acceptable to the public," said Pippa Lawson. Again, a public debate to highlight the progress and problems ahead seems worthwhile.

CONCLUSIONS

The roundtable covered a lot of territory in its four sessions and shared ideas and information, hunches and hopes. The intention was to gather informed people, stake out the territory, and assess what major issues would have to be addressed by government. Three issues stand out:

1. Government must accept that information technology is a leadership issue. That notion must be accepted – and implemented – by leaders at all levels of the government hierarchy.
2. Government must formally address the implications of information technology for its own structures, both in service delivery and policy formulation. While the kind of sweeping changes seen in the private sector might not be appropriate for government, it would seem that government has yet to capitalize fully on the possibilities. At the heart of this is the issue of moving data across traditional boundaries. This needs further study on a priority basis. Such study should be undertaken in a manner that reflects the horizontal nature of the issue. For example, rather than giving one House committee responsibility, a better mechanism may be the creation of a parliamentary task force that has representation from a number of committees, as well as from all parties.

3. Privacy is central to the information technology challenges faced by government. It should be noted that privacy does not mean the simple enhancement of security of information; rather, it is a metaphor for the relationship between citizens and government. The Privacy Act has to be reassessed in an era of rapid technological change and heightened ability to share information. Parliamentarians were particularly insistent that this issue not be left to bureaucrats to decide. They want to be brought into discussions at an early stage.

The rocket ship that is modern technology has left the launch pad. This is a time of vulnerability but also of opportunity. The better we plan our direction, the more successful will be the flight and the less the chance of mishaps along the way.

NOTES

- 1 Thomas M. Siebel and Pat House, *Cyber Rules: Strategies for Excelling at E-Business* (New York: Currency/Doubleday, 1999), p. 2.
- 2 Canada, Advisory Council on Health Infostructure, *Canada Health Infoway. Path to Better Health. Final Report* (Ottawa: Public Works and Government Services, 1999), p. 4.

Harvey Schachter is a Kingston freelance writer specializing in business and public policy issues.

AFTERWORD

A NOTE ON THE CROSSING BOUNDARIES PROJECT

Reg Alcock
Donald G. Lenihan

The Crossing Boundaries project united senior representatives from seven federal departments, members of Parliament, and informed advocates and commentators from academia and other independent organizations to examine initiatives that use information technology to make government more effective and efficient.

As the developers of the project we occupied a special vantage point. Our views evolved over the course of a year-long series of conversations that took place before, between and after the roundtables. The impetus for the project grew out of our joint interest in how the adoption of information technology was affecting the structure and operation of government. We knew from earlier research that the ability to share data more widely in large organizations was a key enabler of structural change, and we wanted to understand the issues involved in sharing data in government. We knew that privacy would be a particularly important issue, given the nature of government information, and we wanted to explore more thoroughly the issues involved.

We felt that this examination would be best conducted through dialogue among the various professional groups involved. Because many issues raised by the topic cut across public administration, politics and the third and private sectors, we are convinced that an interdisciplinary dialogue is in everyone's interest.

A number of themes and issues were examined. The project report does an admirable job of surveying this terrain, sketching the presentations, summarizing some of the analyses and communicating the tone and direction of the discussion. But, as we all realized, neither the roundtable sessions nor the report could go much beyond scratching the surface. The topic and issues it raises are vast.

By way of afterword to the report, then, we thought it appropriate to stand back from the specific content of the sessions and engage in some broader speculation. We asked ourselves whether there was any "big lesson" that emerged or, perhaps, whether a bigger picture had begun to take shape as the project progressed. Is there, we wondered, anything to learn about the state of government or governance about which we were unaware, or not clear, before?

Shortly after the sessions were completed, the two of us met individually with the seven ministers whose departments sponsored the project. Our goal was to give them a short report on what had transpired and see how they reacted to our thoughts on it.

In preparation for these meetings, we tried to work out what we thought were some of the larger implications of key presentations, discussions, debates and issues. At the same time, we tried to distill and consolidate our own thinking. This afterword provides an overview of some of the ideas that we presented to and discussed with the ministers.

In brief, our view is that the Government of Canada is in transition from one model to another. How far along it is, is a subject of controversy. What seems to us clear is that this transition can be more or less smooth, more or less well managed and more or less successful. On the one hand, we are convinced that the result – the government of the future – will almost certainly be more efficient. On the other hand, we are less certain that it will be more accountable, open, transparent and respectful of individual privacy. The guarantees here are far less certain. Information technology has enormous power to create change. But change might as easily be in one direction as in another.

If Canadians are to ensure that the huge changes now begun will ultimately strengthen their commitment to democratic values, ongoing reflection, debate and vigilance are needed – from all sides. Information technology lands us on a vast new continent that has only just been discovered. Its forests and mountains remain unexplored.

In laying the foundation for an ongoing dialogue among politicians, the public service and informed commentators and advocates, we regard the Crossing Boundaries project as a small but important contribution to what will certainly be a massive and prolonged effort: the task of imaging the future. As such, it is our hope that the work begun is not lost. This afterword, therefore, concludes with a modest proposal to build on this foundation.

FOUR DRIVERS OF CHANGE IN THE 1990s

Over the last decade, Canadian governments at all three levels have undergone major change. What brought on the changes? Where are we now? What is the same, and what is different? What does the future look like? What can or should we do to prepare for it? Change in this decade has been driven by four main factors.

First, in the 1990s, governments underwent major restructuring in order to come to terms with their *deficits*. This was the single-biggest driver of change in the public sector.

Second, the new communications and information technology is integrating governments and businesses around the world. Today, huge sums of capital flash around the globe at a keystroke. A collapse in confidence in Asia's financial sector can send North American commodity prices into a tailspin. And a single product, such as an automobile that has been assembled in Canada and sold in the U.S., may also have an engine built in Korea, an interior manufactured in Indonesia, electronic components from Japan and a frame built with Swedish steel. *Interdependence* is increasingly a fact of life. Private and public interests, responsibilities and actions are linked in complex ways. Managing the connections is a central preoccupation of contemporary governance and administration. This encourages and requires a more holistic view.

Third, the delivery of government services is undergoing major change. New approaches rest on the concept of *citizen-centred service*. In this view, services are to be designed and delivered around citizens rather than around the bureaucracy. Single-window service delivery is an example. The idea that government should be integrated around the citizen rather than expecting the citizen to fit into government, with its labyrinth of departments and programs, also encourages and requires a more holistic view.

Finally, there seems to have been a *change in the political culture*. Citizens are making new demands on government. They want greater accountability, responsiveness and transparency in the processes of government; greater collaboration among governments; and a more consultative approach to policy development, program design and service delivery.

How have these drivers of change affected government?

RESPONDING TO CHANGE: THE NEW TOOLS AND PRACTICES

One obvious change is that governments have become smaller. Less well known but more far-reaching changes concern *the way* in which they operate. A range of new tools and practices has been adopted. Generally speaking, these do not fit well into the traditional, hierarchical, “command-and-control” model of government, where the organization is divided into sections, each with a specific task, and management happens from the top down. The conventional metaphor for this approach is the pyramid.

By contrast, the new tools favour a *partnership model*, where governments actively engage one another, private- and third-sector organizations, citizens and communities in new kinds of consultative and power-sharing arrangements. The metaphor of choice here is the *network*, with its myriad nodes and connections and relative absence of top and bottom. The following three features of the partnership model are now standard practice in contemporary approaches to public-sector management.

The Focus on Results

Over the last decade, new, “results-based” management practices have been introduced in most Canadian governments. This changes the way governments plan, implement, report and evaluate. In short, it affects every level of government activity. This is supposed to lead to more coordinated, effective, transparent and accountable government. If there is a central idea here it is that government has been too focused on “process” (*how* it does things) and not focused enough on “outcomes” (the *results* of what it does). The new commitment to manage for, measure and report on results is intended to correct this.

Managing Horizontally

In the old model, government departments tended to act in isolation, turning themselves into a series of unconnected “stovepipes.” As things become more interdependent, issues increasingly cut across several departments and jurisdictions. In response, governments are developing new, “horizontal” approaches to planning, managing and delivering programs. For example, traditional health policy tended to be reactive, focusing on the curing of illness. Now it focuses on promoting well-being, a more inclusive concept that not only looks at “health determinants,” such as education levels, exercise, diet and the environ-

ment, but that also encourages citizens to take greater responsibility for managing their own health. On the service-delivery level, single-window service is an attempt to overcome the stovepipes by getting different departments and levels of government to coordinate and integrate related services.

Partnerships

A third feature of the new, emerging model of government is the focus on partnerships. These can be intergovernmental, interdepartmental, public-private or public-third sector. Traditionally, partnerships between government and the private or third sectors have been much like contracting-out arrangements. Government itemizes the tasks it wants performed and pays the partner for performing them. Now a new and less structured approach to partnerships is emerging. In this one, parties aim more at working together. This can range from a simple co-location of offices to efforts to co-manage policy areas, programs and resources. The key idea here is that at least some of the planning and decision-making of government is shared with the partner. We can call these *collaborative partnerships*.

FINDING THE FULCRUM OF CHANGE: CROSSING BOUNDARIES

Change is unavoidable; but there are at least two ways to deal with it. We can allow it to happen and then react to it; or we can be proactive and try to manage it. If we opt for the latter, we must move away from the old “command-and-control” model of government, with its rigid structures and top-down approach to management. We need a model that is flexible, horizontal and able to coordinate diverse actors and interests.

The new tools and practices move government in that direction. But they are not enough. If, like a lever, they can be used to move heavy loads, they still require a fulcrum – a point where change comes to a focus – on which they can rest. Is there such a point?

There is no single point in government where all change is concentrated, but there are some parts of the system where the impact of change is most clearly felt. Perhaps the single-most important one is the departmental, jurisdictional and sectoral *boundaries* that separate a government’s activities from other parts of itself, from other governments, and from the private and third sectors. These are the walls that support the traditional command-and-control model. Current drivers of change tend to knock them down.

Still, if greater interdependence between walled-in areas cannot and should not be prevented, neither should existing boundaries be allowed to collapse just because pressure for change builds. The system’s boundaries define the limits and authority of any part of government. When we say that someone is accountable, for example, we set limits to this by identifying the boundaries within which he or she exercises authority. Boundaries also determine how decisions can be implemented. For example, government usually acts through one of its parts, such as an appropriately mandated agency or department. Both are crucial to ensuring the accountability and transparency of government.

“Managed change” aims at balancing interdependence and separateness. The new tools can facilitate greater integration of some things while keeping others apart. More specifically, departments, governments, organizations and sectors are experimenting with collaborative partnerships that allow for

- *joint planning and decision making* that use teams of individuals from a number of organizations to plan and make decisions;
- *integrated service delivery*, which ranges from electronic kiosks to partnerships as a way of bringing government(s) together around citizens;
- *common practices and standards*, where agreed upon by governments, help coordinate and integrate activity across boundaries; and
- *joint reporting and evaluation*, which help governments arrive at similar conclusions that, in turn, help them coordinate new planning and initiatives.

New practices like these change the way government works. They force a re-thinking of the command-and-control model of government by re-defining how, when, where and why boundaries are permeable, eliminable, elastic, diffuse or firm. If leaders want to manage change effectively, they must learn to use these tools to manage boundaries differently.

INFORMATION, INFORMATION TECHNOLOGY AND THE PARTNERSHIP MODEL OF GOVERNMENT

A few key points follow from these reflections.

First, the new partnership practices all make effective government far more dependent on a flow of information across boundaries that is current, of high quality, easily accessible and effectively communicated.

Second, because this kind of information is so important to the new model, realizing it will require a major change in the infrastructure government uses to do business. Traditional, hierarchical, departmental structures must be supplemented – if not replaced – by horizontal information networks and systems.

Finally, because information systems are horizontal, they will penetrate boundaries of all sorts in the existing system. So, on one hand, information is a key resource of the model of government needed to manage change. On the other, the flow of information itself tends to dissolve the boundaries within the system. The partnership model thus creates a state of dynamic tension in which boundaries are maintained but are shifting and diffuse. They are more like electrical fields than the solid walls of the traditional command-and-control model.

As these observations suggest, a key challenge facing government at the turn of the millennium lies in how information is gathered, managed, communicated and shared. And that, in turn, depends upon how the boundaries within the system are managed. Decisions about what information systems to use, how, when, where and why thus have both management and governance implications. In brief, as a management question, these decisions

are concerned with how to make government more efficient and more effective. In general, this will move government in the direction of the partnership model. On the other hand, changes to our existing model of government must respect its fundamental values, ensuring that government remains open, accountable, transparent and accessible and that individual privacy is protected.

NEXT STEPS: BUILDING ON THE FOUNDATIONS

The Crossing Boundaries project began a discussion among decision-makers, advocates and opinion leaders about how boundaries are to be conceived, structured and managed as government positions itself in cyberspace. Issues and opportunities abound.

For example, we heard that the use of information technology in government could give the term *citizen engagement* a whole new meaning. These days, it usually refers to how citizens might become engaged in decision-making on policy issues, ranging from capital punishment to zoning bylaws. Possible means for engagement include citizen juries, deliberative polling, referendums and town-hall meetings. When information technology is mentioned in this context, it is generally treated as a way of widening such involvement.

Information technology could make it possible for citizens to be more than button-pushing, passive consumers of information from government. Citizens could design and manage their own interactive, electronic portfolios. Each citizen could have a porthole on government that selectively integrates personal and generic information from a number of areas, such as health, income security programs, employment counselling, financial management, travel, citizenship and vital statistics. Such a system would be a giant step in the direction of a more personal relationship between government and citizens in which needs, entitlements and preferences are responded to in a timely, regular and individualized way. But are citizens ready, willing and able to manage a customized relationship with government?

Another issue concerns managers who have to make important decisions about selecting or designing a large new information system. Most have little expertise in the area. But new reporting requirements, the need to upgrade service delivery or to ensure that planning and policy development reflect the horizontal interests of government often require the development and purchase of such systems. The issues surrounding such a decision can be manifold and very complex, ranging from cost concerns to worries about the system's long-term viability or its impact on the practices of governance. Responding to this challenge requires a broader, more open discussion of the issues. Perhaps that would lead to the development of a more sophisticated management framework for making choices.

All seven of the sponsoring departments in the Crossing Boundaries project have major IT initiatives under way that revolve around information-sharing or the creation of new horizontal information systems. Although considerable attention has been paid to issues around privacy, comparatively little has been given to the larger question: What is the impact on the structure of government? Indeed, this discussion has hardly gotten off the ground. The experience of these departments should be more thoroughly mined.

Stronger links between the political and administrative arms of government, as well as other governments, the third and private sectors will be required. The learning that should take place is multifaceted and requires expertise from all sides. Accordingly, we propose to build on the foundation of the first project by developing a second one. This project could take the form of a special committee or task force composed of parliamentarians and senior public officials, along with representation from other appropriate organizations. The committee or task force could meet regularly, perhaps twice a month, for approximately a year. This would provide adequate time to examine and discuss a range of initiatives in the sponsoring departments and develop a detailed report. The goal would be to mine these initiatives for the lessons they may hold about the changing structure of government and how information technology can be used to ensure that the government of the future remains open, transparent, accountable, responsive and respectful of individual privacy.

Reg Alcock is a member of Parliament for Winnipeg-South. Donald G. Lenihan is director of research at IPAC.

The New Directions Series

The Institute of Public Administration of Canada (IPAC) has, for many years, sponsored issue-oriented working groups of public servants and academics to find practical solutions to emerging issues. The Institute assembles groups of experts working on public-sector reform and public policy to discuss, compare, analyse, document and advance the understanding of critical issues and themes. While these reports are published in the language in which they were written, the executive summary is provided in the other official language.

The projects continue to explore a wide range of issues. In its continuing commitment to exploration and exchange, IPAC launched this series. Publications in this collection highlight critical findings and analysis from our action-oriented research activities. Besides advancing the understanding of current best practices, this work also serves to advance the understanding of what these initiatives mean with respect to the broader concerns of public-sector reform. These reports are available free of charge to IPAC members. Orders can be placed by contacting the IPAC national office in Toronto (www.ipaciapc.ca).

La Collection Nouvelles Directions

Depuis plusieurs années, l'Institut d'administration publique du Canada (IAPC) commandite des groupes de travail axé sur les grandes questions en administration publique. Composés de praticiens et de théoriciens, ces groupes d'experts se réunissent pour apporter des solutions pratiques aux nouveaux enjeux qui confrontent les administrateurs publics. Spécialisés dans les secteurs de la réforme administrative et des politiques, ils discutent, comparent, analysent les problèmes et questions critiques qui sont soulevés et documentent leurs observations, faisant ainsi avancer la compréhension dans ces domaines. Des rapports découlant de ces études sont publiés dans la langue dans laquelle ils sont soumis. Un sommaire exécutif est présenté dans l'autre langue officielle.

Nombreuses questions d'actualité sont continuellement étudiées dans le cadre d'activités de recherche. L'IAPC a donc lancé cette collection afin de poursuivre son engagement d'explorer et d'échanger. Les publications qui paraissent dans *Nouvelles Directions* mettent en relief des conclusions et analyses importantes qui sont tirées de notre recherche active. Tout en faisant avancer la compréhension des meilleures pratiques en vigueur, ces études permettent de mieux saisir leur importance en ce qui a trait aux préoccupations plus générales concernant la réforme du secteur public. Ces rapports sont offerts gratuitement aux membres de l'IAPC. Pour obtenir des exemplaires, prière de communiquer avec le bureau national de l'IAPC à Toronto (www.ipaciapc.ca).

Other Reports in the Series/ Déjà parus dans la collection

1. *Management and Performance Measurement in the Jewellery Industry: A Golden Opportunity?* By Ann Rauhala.
2. *Performance Management: Linking Results to Public Debate.* By John English and Evert Lindquist.
3. *From Controlling to Collaborating: When Governments Want to be Partners.* By Jim Armstrong and Donald G. Lenihan.
4. *Improved Reporting to Parliament.* By Jim Thomas.
5. *Crossing Boundaries: Privacy, Policy, and Information Technology.* By Harvey Schachter.
6. *Collaborative Government: Is There a Canadian Way?* Edited by Susan Delacourt and Donald G. Lenihan.
7. *Business Planning in Canadian Public Administration.* Edited by Luc Bernier and Evan H. Potter.
8. *Making Government the Best Place to Work: Building Commitment.* By Monica Belcourt and Simon Taggar.
9. *To Better Serve Canadians: How Technology is Changing the Relationship Between Members of Parliament and Public Servants.* By Jonathan Malloy.
10. *Service North of 60.* By Frances Abele and Katherine Graham.