The internal governance of e-government: implications of a new sector of public management for trust and accountability

David C.G. Brown, PhD  
School of Political Studies  
University of Ottawa  
Ottawa, Canada

2012 Annual Congress of the International Institute of Administrative Sciences  
Merida, Mexico  
June 2012

Abstract

Trust and accountability are central to any system of governance. The paper asks how these issues are affected by information and communications technologies (ICTs) in public sector management. It uses the case of the Canadian federal government’s Chief Information Officer (CIO), its senior advisor on the use of ICTs in public administration.

The paper begins by discussing trust and accountability in public administration. It then looks at information and technology as a new sector of public administration, “mapped” by the CIOs responsibilities, which in turn constitute the management component of e-government. The sector’s elements have included management of information technology and of information, freedom of information, privacy, security, government communications as well as service to the public and internal services to government. A third section returns to trust and accountability in this e-government context. The paper concludes that e-government is a transitional phase in the modernization of public sector governance; many of the foundational elements endure but lasting new elements highlight both the opportunities and the risks for effective trust and accountability.

Table of contents

Abstract ............................................................................................................................................. 0  
Table of contents ............................................................................................................................ 0  
Trust and accountability in public administration ........................................................................ 3  
Information and technology: a new sector in public administration ....................................... 5  
Trust and accountability and e-government .................................................................................... 9  
Conclusions ..................................................................................................................................... 14  
References ...................................................................................................................................... 17
Introduction

The trust and accountability dimensions of e-government brings together several threads that, in the theory and practice of public administration, are new either in themselves or especially in combination. Our conceptual understanding of e-government is still evolving and there has been a relatively limited focus on its institutional aspects. At the same time, consideration of trust and in particular of accountability in the public sector is much more concrete if it is linked to an institutional context, which is infused with societal norms and values and provides the mechanisms within which accountability is played out.

This paper seeks to contribute to that concrete understanding by looking at the case of the Canadian federal government's Chief Information Officer (CIO), a senior-level, government-wide institutional response to the information and communications technologies (ICTs) that have profoundly affected both society at large and the public sector in the past generation. The CIO's responsibilities have brought together a number of management policies and relationships within and outside government that raise important questions of trust and accountability. In most cases these are not new to public administration, but their impact has been heightened by ICTs, as has the actual and potential tensions among them. The paper argues that this is a two-edged sword for public administration, but an important first step is to recognize what is happening and to begin to study it more intensively.

Technology has always been a major influence on the role and capacities of the state – in the first half of the 20th century, the telephone, automobile and various forms of office automation all had a profound effect on public administration, in parallel with similar effects on the economy and daily life. More recently, and in particular since about the late 1980s, the convergence of telecommunications, computing and broadcasting (Rowland 2006) has accelerated the social and economic effects of ICTs, an open-ended process that is continuing with the growing centrality of mobile technologies and social networking. These developments have affected all of the state’s relationships, going well beyond introducing a new communications channel to offering the possibility of reshaping both the state’s role in society (Tapscott 1997) and how it operates internally (Borins 2007a).

The term e-government has been coined to capture this new reality. There is no standard definition of e-government, which in its broadest sense encompasses all aspects of the state’s work and relationships, when these operate within an electronically-enabled environment (Brown 2005b). Much of the e-government focus is on how, in this new and continuously expanding sphere, governments formulate public policy – including with respect to new ICT-shaped public policy sectors – and how they deliver services to the public, increasingly characterized by an emphasis on the citizen as the catalyst for structuring those services (Kernaghan 2005). Another important focus of e-government is on the procurement relationship that is created with the private sector (Dunleavy et al.
The e-government literature does address institutional effects of ICTs (Anderson 1999, Fountain 2001, Charhi and Robert 2004), including their link to trust and legitimacy in the eyes of the public (Snellen 2005). Less attention has been paid, however, in either the e-government or the public administration literature more generally, to the institutional effects of ICTs on internal public sector governance and in particular to the emergence of central management agencies concerned with prescribing and overseeing policies, practices and projects across the government “enterprise” relating to the management of ICTs and the information they carry.

One such central management agency grows out of the private sector model of a Chief Information Officer (CIO), some version of which has been adopted in a number of national and sub-national governments. This development has not received much attention in the public administration literature, however, especially in a comparative context, and it is difficult to generalize about the role and responsibilities of public sector CIOs or about their relationship to the concerns represented by the term e-government. At the same time, all governments in their management regimes address a number of common functional areas of administration that are defined or heavily influenced by ICTs. Many of these, including records management, protection of personal information, freedom of information, communication with the public and the delivery of services to the public, raise questions about the relationship between public administration and the public and related issues of trust and accountability.

This paper looks at the Canadian federal government’s CIO. Originally established in 1993, the CIO is a senior officer of the Treasury Board Secretariat, which combines the role of budget office and central agency for management practices across the government, including in the areas of financial and human resources management. The CIO is the government’s senior advisor on the management of ICTs and of information and has, under favourable circumstances, played a leading role in technology-enabled public sector reform (Brown 2005a). The position’s responsibilities have evolved over time, but at various points it has had lead responsibility within the government for a number of areas of management shaped by information and technology, which together define a management “space” that can be understood as encompassing the public administration dimension of e-government. In the nature of its responsibilities, the CIO is a key actor in the governance of e-government.

The paper begins by considering some of the relevant aspects of accountability, trust and values, which have long been central issues in public administration. It then outlines the management dimensions of information and technology as a new sector in Canadian public administration, within the established constitutional and governance framework of the Canadian state. The sector’s individual elements all carry with them values and goals that raise issues of accountability and trust, but in combination they highlight additional
challenges, especially when the individual sets of policy objectives come into conflict. These issues are discussed in the paper’s third section. The concluding section looks at some of the dynamic tensions going forward, arguing that there are both opportunities and significant risks for the legitimacy and effectiveness of public administration. While the discussion is concerned with the Canadian case alone, it is hoped that it will contribute to comparative analysis of the equivalent phenomena in other administrative systems.

**Trust and accountability in public administration**

This section summarizes the approach taken in the paper to trust and accountability as they relate to public administration in general. A later section applies this line of thinking to the public administration dimensions of e-government.

Trust and accountability raise basic questions about the nature of public administration and its relationship with society and the individual citizen. In considering these issues, a useful starting point is that all public administration functions carry with them public policy goals that are linked in some way to larger societal values. These goals are at a minimum oriented towards creating a framework for effective management of public resources. The crucial link to society is that those resources are raised through taxation and other forms of revenue collection from the public; they are allocated within the rule of law and a framework of accountability to the public, in a liberal democracy through representative legislative institutions and the courts, with the details depending on the larger constitutional system. In principle, this creates a trust relationship between the public and government, in which the public’s acceptance of the legitimacy of state actions is in return for an undertaking that citizens are treated fairly by the state and have genuine access to its institutions and decision-making. A corollary is that there are mechanisms for holding state institutions to account and that these work in a satisfactory manner.

From the perspective of the individual citizen, a fundamental aspect of trust is that the state does them no harm and that their personal interests are reasonably protected. The bedrock of these interests includes basic human rights such as security of the person and personal freedoms including those of conscience, expression and movement. Individuals provide a great deal of information about themselves, their families and their daily lives to the state, and how this information is used is another foundation for a relationship of trust between the citizen and the state – as discussed later in the paper, this is one of the central trust issues in the e-government context. In practice, trust is built up and shaped through the accumulation of interactions and experiences that individuals have with their government, touching on issues such as whether they have access to decision-makers and feel their concerns have been dealt with fairly, not to mention expeditiously.

A second level of trust-building is through the citizen’s perceptions of the state’s role in society at large. In broad terms, this has to do with the operation of state institutions, beginning with constitutionally established representative
institutions. In the latter case it is a matter of the citizen trusting both their own representatives to “do the right thing” and the representative institutions to function effectively in holding executive authority to account and ensuring that it, in turn, operates in a lawful and constitutional manner – that the state “plays by the rules.” Again there is a vital underlying reciprocity: the citizen needs to be able to trust the state, but there is also an expectation that the state trusts the citizen, at least until justifiably proven otherwise.

Trust can be viewed as being a function of a mutual sense of ownership: if the citizen and the state are understood and seen to support each other, each to have a stake in the success of the other, then trust results and – in the best form of virtuous circle – trust can also nurture the relationship. Two of the most basic ways in which citizens can express their trust in the state are through voting and paying taxes, the former being the means by which the citizen provides legitimacy and direction to representative institutions and their critical decision-making and accountability roles, the latter being the vehicle for giving the state the resources to carry out its work. A healthy state never forgets that it is acting with its citizens’ consent and through spending their money. Citizens who trust their state are more likely to pay their taxes, to collaborate with it (including through providing the information it asks them to provide) and to abide by its decisions and actions.

Trust is reinforced by accountability, which like trust is about a relationship, in this case between those who have authority and confer it on another and the recipient of that authority (Aucoin and Jarvis 2005). Ultimately, accountability is about how authority is used, including whether the recipient has respected its limits, on the one hand, but also its objectives. Accountability is most often thought of as a process of holding someone to account – both the recipient of authority (for how they have acted) but potentially also the grantor of authority, for how well they have framed the authority, monitored its use and acted on the results. Often, accountability in practice becomes a matter of allocating blame and extracting consequences when something has gone wrong; it is a field riddled with ambiguity. The most clear cut cases are when the wrongdoing is (or is alleged to be) of a criminal nature and can be addressed in the courts; generally, however, in public administration the events and debates in question are administrative, growing out of internal management policies and procedures, and accountability mechanisms are wholly or in part to be found in the political process and the court of public opinion. These processes have a significant impact on public trust in public institutions.

Accountability relationships exist both between the public sector and society and within the public sector, i.e., within public administration. Public administration is built around a number of functional disciplines, each of which has its own internal institutions, rules and procedures. Each state has its mechanisms for providing internal direction and guidance to its administration, and there is variation in the degree to which common approaches are required or at least desired. It can be assumed, however, that all states draw on the same range of functional disciplines in order to create their internal management.
environment. Each of these disciplines carries a number of objectives and values that may be explicitly or implicitly prescribed, whether by political and senior civil service authorities, as a reflection of societal values or arising from professional protocols. These in turn provide the reference points for making accountability judgments and the benchmarks for establishing trust.

Historically the two major functional sectors, or sub-disciplines, of public administration have been the management of people and of money – in Canadian terminology comptrollership (financial management) and human resources management. With some important exceptions, notably in the field of human resources management,¹ both functions are governed in the Canadian federal government by a range of policies and procedures that are set and overseen by Treasury Board, a committee of Cabinet ministers. Based on an array of legislation, these policies establish a common framework for management across the public service in areas that are considered to be important to the government as a whole while leaving discretionary room to line Ministers and their senior officials to tailor their management environment to the nature of their programs and services.

These (and indeed all) functional areas can be described in terms of a range of values that infuse the formal policies but that also are an essential part of their implementation, accountability and credibility, providing the basis for trust in their application and effectiveness. Financial management, for example, has historically been concerned with values of prudence and probity, economy, efficiency and (more recently) effectiveness. In the same way, human resources management can be assessed against these tests but also those of professionalism, political neutrality, merit and integrity as well as by the absence of political patronage and of bureaucratic cronyism. An underlying test in both areas is honesty and absence of corruption. As discussed later in this paper, the management practices that are linked to e-government can be described in similar terms.

Information and technology: a new sector in public administration

The Canadian federal government’s CIO is both its senior advisor on the management of information and of ICTs and the leader of related professional communities of practice in the public service. Although inspired by private sector CIO models, the position’s authority within the Canadian public service has been described as weak (Borins and Wolff 2000), based on the fact that it does not control several key levers of central administrative authority, including the allocation of IT budgets to government departments, purchasing of IT goods and services, or supervision of the CIOs that have been appointed in each of the government’s ministries and agencies. At the same time, the TBS CIO operates within a government-wide internal governance model established in the 1960s.

¹ Treasury Board is responsible for labour relations within the public service and sets government-wide management policies in most areas of human resources management. Separate legislation establishes a merit-based system of appointment to public service jobs and an independent Public Service Commission to oversee it.
Based on advice from an external advisory commission on government organization (Canada Glassco 1962-3), the Canadian public service is structured around three interlocking organizational models: line departments (i.e., ministries), which deliver programs and services to the public; central agencies, which advise Cabinet and Treasury Board on policies and decisions relating to the management of the government as an “entity” (52); and common service organizations, which provide selected services to government, working within Treasury Board and other government management policies that apply both to them and to departments.

Under this model, oversight of public service management functions has been given to Treasury Board and its supporting Secretariat (TBS), of which the CIO is one of the senior officials. TBS also advises the government on the overall expenditure budget and the operating and capital budgets of individual departments, including monitoring major capital projects. The CIO’s role is based on advising Treasury Board ministers on the areas of management for which it is responsible and on leading and monitoring implementation of related Treasury-Board approved policies and procedures across the public service. A key part of this role is providing leadership to the functional specialists in departments and common service organizations who are operating within the same Treasury Board policies. Within TBS, the CIO is also a technical advisor to and collaborator with the budget office and with policy centres in related areas of management. The absence of line authority in these areas, then, is compensated by considerable influence and leverage, backed by collective ministerial authority and direction.

The CIO’s responsibilities have varied considerably over the years, not surprisingly as there was little precedent for many of the functions involved or for the ways in which they have been combined. Although further evolution is likely, the situation has stabilized in recent years, reflecting a greater understanding of what is involved in the management of information and technology and a resulting institutional maturity. In this evolution, there have been some constants in the range of CIO functional interests as well as some moving parts. There has also been an outer perimeter of management functions for which the CIO has never been responsible but which are clearly closely related and are the responsibility of the government CIO in at least some other jurisdictions (Borins 2007b). Together, these responsibilities define a map or space that can increasingly be thought of as the public administration dimension of e-government. This space is characterized not only by a set of management functions but also by the relationships that they entail, many of them – unusually for public administration – with groups outside the public sector.  

---

2 The reference is to a study of the Corporate CIO of the Province of Ontario – Canada’s largest provincial government – which has a “strong” CIO in the terms set out by the Borins and Wolf study.

3 It should be noted, however, that the CIO has no role in setting public policy with respect to ICT-based industrial development and infrastructure in the wider economy. This is the responsibility of the Department of Industry.
At the heart of this administrative space is the interlocking relationship between the management of ICTs – of technology – and of their information content. These are linked by a policy framework (Canada TBS 2007b) that articulates eight guiding principles: information as a valuable asset, IT as an enabler, stewardship of information and IT, a whole-of-government approach, respect for individual privacy, effective security of information, transparency in support of access to information and accountability, and institutional bilingualism in English and French. Within this framework, a policy on the management of information technology (IT) calls for IT management to be linked to business planning in departments and encourages sharing within and among departments of IT infrastructure and resources. This policy also provides the framework for the management of telecommunications and computing common services to government and for the development of IT applications in support of other areas of government administration, notably financial and human resources. In addition, it provides the basis for an active CIO involvement in the approval and monitoring of major IT projects across government, including ensuring that they have risk-based management frameworks in place.

A second core CIO policy calls for a life-cycle approach to information management, linking the collection, use and reuse, dissemination, protection, preservation and long term disposition of information. This provides the basis for government recordkeeping practices but also creates a broader framework and unifying thread for several other information-oriented policies, which are linked to various stages of the information life-cycle. Among these, perhaps the most influential has been the Access to Information (ATI – i.e., freedom of information) policy which implements legislation passed in 1983. Its provision that government records requested by the public should be made available within 30 days forced a major re-thinking of information management practices, and the ATI Act remains an important underpinning of government transparency and accountability. Its companion, the Privacy act, and the associated Treasury Board policy, which are based on the OECD privacy code, provide for a right of access by individuals to their own information, complemented by protections against unwarranted secondary use and access by third parties. In both ATI and privacy an independent commissioner has been established, on the model of an ombudsman, to receive and investigate complaints about government non-compliance, with powers to report to the responsible minister and also to Parliament.

The CIO is responsible for two other information and technology-related policies. One relates to the ethical use of the Internet and internal electronic networks by government employees. The other, which in fact goes beyond the realm of e-government narrowly defined, is the policy on government security, which covers the gamut from identity management through information protection, security screening of current and prospective employees, physical security of government premises and assets, IT security (itself a vast topic), continuity of government business in emergency situations, and security issues arising from government contracting and outsourcing. A common element of
much of this policy is protection of information in the many dimensions in which it comes into play in public administration.

Several other policies build out from this core, some of which are currently part of the CIO’s responsibilities, others of which have been in the past. The most important of the latter is the government communications policy, supported by a policy on the Federal Identity Program, the government’s corporate identity and branding regime. Although initially under the CIO’s jurisdiction, the communications policy has for the past decade been separately administered, reflecting its political sensitivity. This policy builds on the dissemination aspect of the information life-cycle, however, and intersects the other information policies in numerous ways. Based on a principle of “informing and serving Canadians,” including measures to ensure broad access to public information, the policy covers a wide range of communications functions, among them public opinion research, citizen consultation and engagement, media relations, advertising, publishing, copyright and licensing, and new media. Earlier versions of the policy were cast in terms of the government’s duty to inform the public so that citizens could exercise their rights and obligations, and that sentiment remains embedded in the policy’s provisions.

A more recent policy, but one that in many ways has grown out of the others is with respect to service to the public. A major concern is to ensure integration of the various “channels” of service delivery, ensuring that electronic services are effectively combined with those provided through telephone, kiosks, postal mail and in-person channels, reflecting the multiple ways in which citizens typically obtain their services from government (Marson and Heintzman 2009). An underlying premise is that service delivery has a critical role in enhancing citizen confidence and trust in government (Heintzman and Marson 2005). The service policy has had a volatile organizational history, having been part of the CIO’s original mandate, twice separated organizationally to give it higher profile, but now back within the CIO’s fold. The policy is infused with the concepts of citizen-centred service which emerged even before the wide spread of ICTs (and in that sense of e-government) but which came into even greater prominence under their influence. In Canada, a highly decentralized federal state, one of the consequences of citizen-centered logic in the electronic environment has been greater collaboration between the federal and provincial governments in providing services to common client groups in the public (Brown 2007).

Another tier of management policies provides the outer perimeter of the information and technology administrative space. Notable among them is a set of policies under the rubric of management of assets and acquired services, which govern government purchasing of goods and services, including technology and IT-related consulting and personal service contracts. In practice, all technology hardware and most software applications, including many that are designed specifically for government, are supplied by private sector vendors, often based on advice provided by private sector consultants. While the CIO is not directly responsible for purchasing these goods and services on behalf of the federal
government, the CIO has a leading role in the government's relationship with the private sector, both as an overseer and as an interlocutor.

This administrative space is still emerging, not least because it must continue to respond to new technologies. At the same time its broad dimensions and relationships are increasingly stable, and it is becoming possible to look at it as a whole and to identify some of its internal dynamics. A characteristic of the space is the extent to which it incorporates areas of public administration that are externally oriented, tied to the state's relationships with the citizen and other economic and social actors. As discussed in the next section, these touch on numerous aspects of trust and accountability.

**Trust and accountability and e-government**

The “map” of management functions that are coalescing under the broad rubric of an e-government administrative space identifies a set of policy goals and values that provide a framework for looking at related issues of trust and accountability. This institutional environment is still maturing. If the government CIO provides a focal point, the position is not yet 20 years old in the Canadian public service, and its counterparts in most other governments are even more recent. The outer boundaries of the space are still taking shape, as are its internal dynamics and external relationships. Even allowing for this fluidity, however, there is no question that e-government defined in these terms is linked to some of the most important contemporary issues of trust and accountability.

Using the Canadian example, the e-government administrative space is most easily understood as being made up of seven functional areas of management, embodied in Treasury Board (i.e., government-wide) management policies adopted and refined over several decades by a succession of governments from different parties. In that sense they carry a broad level of political support, itself an important foundation for building public trust. These functional areas are: the management of technology and of information, access to information, protection of personal information (privacy), government security, government communications, and service to the public. In most cases these building blocks are not new; indeed, all but the service to the public policy pre-date the establishment of the CIO, and even that policy has earlier antecedents. The successive waves of ICT-based technologies in the past two decades have added features to these policies, however, and have brought profound changes in the administrative environment in which they operate as well as in how they relate to each other and to actors outside government. Cumulatively they have added an altogether new dimension to public administration.

While it can be argued that government is ultimately defined by what it knows and what it does with that knowledge, it is the change in the technological medium that has shaped the e-government environment. ICT hardware, software and infrastructure at their most basic are tangible assets, entailing significant financial costs and an injection of specialized skills into government; in turn this creates an expectation that the major investment involved will be managed cost-
effectively at every stage from needs identification and design through acquisition, operation, updating and eventual replacement.

Major technology projects are publicly visible and create risks for a number of reasons. In addition to basic expectations of good asset management, they are vulnerable to rapid technological change, to the extent that design solutions adopted at the beginning of a multi-year project are often found to be obsolescent by its completion. A related issue is that government needs to ensure that its technology platform is broadly compatible with the capabilities of society at large – that it is up to date with the more advanced individual and corporate users while not leaving behind the less and non-technologically oriented elements in society. Put another way, government – which in Canada and typically in most countries is the largest single institution and technological environment in the country – needs to be innovative in its adoption of technology, playing the role of a model actor on the information highway (Canada IHAC 1995 & 1997), while guarding against the high risks of technology project failure.

With significant amounts of public money at stake, the risks are also political. A large part of IT spending is on the acquisition of goods and services from the private sector, which is itself a highly diverse environment, ranging from large multinational firms to self-employed individual contractors. The ability to manage the private sector relationship is one of the critical factors in e-government success (Dunleavy et al. 2006), putting pressure on government to act both competently and transparently. Cumulatively, therefore, the introduction of IT as a major asset and cost of public administration by itself introduces and brings to the fore a number of issues and relationships that have a direct bearing on public trust in public administration and its political masters.

The management of information presents a parallel set of issues, bringing into sharp focus both the possibilities and the risks inherent in the technologically-conditioned environment in which public administration now operates. Information represents a major and, in the world of ICTs, a rapidly growing asset of government. Databases and electronic networks, whether wired or mobile, offer the potential to link together records and information that have previously been isolated, permitting the combination and recombination of data in ways that could not have been anticipated by their original authors. This offers the prospect of knowledge-based government (Bontis 2007, Tapscott 1997), which by virtue of its role in society has the most extensive and in many areas the most reliable information base in the country. At its best, the result is better evidence for public policy, fairer treatment of citizens and other social actors, and more transparent use of public funds, creating expectations for management of

---

4 The Canadian government does not have hard numbers on its spending on IT. A study in 2005 estimated that about 10% of the operating budget was spent on hardware and software acquisition, staff costs for IT-oriented personnel in the public service, and various kinds of IT contract services (Brown 2007). The study has not been repeated but it is generally considered that IT spending continues to be in this order of magnitude.

5 See for example, the work of the International Records Management Trust (IRMT), which identifies good records management as the basis for providing reliable evidence in the ICT context and through that for
this public resource in the same spirit of prudence, transparency, efficiency and effectiveness that applies to the government’s financial resources. This is a highly ambitious goal in practice, however, not least because it builds on good record-keeping and archival practice – a field that was neglected more often than not even in the pre-ICT era and has faced major challenges in the transition to electronic records (Brown 2012).

The previous section of this paper briefly sketched the range of information-based management functions that are linked through the information life cycle. Each of these has a basis in public policy and creates expectations that play an important part in shaping public attitudes towards government and ultimately in the public’s trust, collectively and individually, in e-government. The functions are individually important, but cumulatively powerful. Some of the elements have already been alluded to, but a brief review highlights their e-government-related characteristics. In the Canadian ordering of the e-government administrative universe, four functional areas are oriented towards the public in general and the citizen as an organizing concept, although all of them are ultimately concerned with regulating internal administrative procedures and relationships. A fifth is more internally focused but affects external relationships in a number of ways.

An abiding theme of e-government is the importance of service to the public, using ICTs to focus on the citizen’s requirements and interests in organizing and delivering services and to improve the quality and cost-effectiveness of those services. Arguably the single most powerful technological innovation has been the empowerment of the citizen through self-service mechanisms – the concept is not new, but the ability to conduct transactions from the citizen’s home or from any other location of the citizen’s choice, without the intervention of government officials, has enormous long-term implications. Like so much else about e-government, these are still unfolding, but they potentially include changing the power balance between the citizen and the state – giving the citizen more control over their daily lives – while also lessening the costs and scale of the state, although not its reach.

Fostering trust between the citizen and government can be thought of as a broad objective of e-government (and the state of that trust as a measure of its success), but there are also practical benefits, including broadening the accessibility and take-up of government services, as well as improving compliance in areas such as tax collection. In Canada, the service to the public policy in fact builds on several others, with systematic efforts to improve service to the public dating back to the 1960s. A landmark was the passage in 1969 of the Official Languages Act, which established the federal government as institutionally bilingual, with English and French having equal status in internal administration as well as in service to the public. The latter is manifested in the right of citizens to be served in the language of their choosing, a forerunner of trust and accountability (IRMT 2012). The IRMT is focused on public sector records management in developing countries, but its analysis is no less applicable to OECD countries, which have been forced by ICTs to go back to first principles in their own approach to records management.
citizen-centred service. A second foundation piece was the Access to Information Act 1983, which again gave the citizen the initiative in seeking the release of government documents, without relying on government decisions to release information and records.

At the same time, encouraging proactive disclosure was a major theme of the government communications policy when it was launched in 1988, an approach that is continued in recent open government initiatives (Canada TBS 2012). More generally, the communications policy places on government an obligation to keep the public informed, both so that citizens can exercise their rights and obligations but also so that they have a sufficient basis for holding the government to account. A vital corollary to the general approach to communications is extensive efforts to ensure that Parliament and the public have full information about the budget and how taxes are spent. An informed public is better able to make use of government services and to do what is asked of it by government and national legislation. It is also better able to participate in the public policy process, another dimension of e-government. Electronic access to government websites, databases and virtual space offer the possibility not only of better access to information on which decision-making is based but also access to the decision-making process itself. The technology even allows for participation in decision-making through on-line voting. With increasingly well-educated and computer-literate publics, the pressures to move in the direction of something like electronic democracy is likely to grow, with implications for representative institutions that are only beginning to be thought through (Roy 2008).

The other side of the coin to making information available to the public is protection of what the government knows. This too has many dimensions. Much of the information that government holds is obtained from the public, whether individual citizens, corporations or other social and economic actors. A foundation for this information gathering is the census, but it takes many other forms, including public opinion research and information obtained in the course of applications for government programs and services, through its regulatory activities, and through the multiplicity of other interactions that government has with the public in all its forms. Sometimes this information is provided voluntarily, often it is not. Ordinarily it is provided for a particular purpose, although it can also be provided for multiple purposes – in Canada, for example, an income tax return also constitutes an application for a number of social policy-oriented tax expenditures such as child care benefits.

A fundamental concern that goes to the heart of the trust relationship between citizen and state is that personal information is lawfully collected and that it is indeed used for the stated purpose. Corollary concerns are that it is only

---

6 In Canada this includes detailed Reports on Priorities and Plans for each department and agency as part of the Parliamentary appropriations process, follow-up Departmental Performance Reports after a fiscal year has been concluded, financing of research staff in the Parliamentary Library, and (an initiative of the current government) the establishment of a Parliamentary Budget Officer to analyze and comment on Parliament’s behalf on government spending and fiscal analysis.
trust and accountability and the internal governance of e-government

retained and shared for authorized purposes and that it is adequately protected against unauthorized access from either inside or outside government. What is at stake, however, is the completeness and quality of the information provided – citizens who do not trust their governments are less likely to comply with its information requests and will be less concerned with the accuracy of what they do tell government. This is a major e-government challenge when much of the business case for technology investments is their information-sharing and data-mining capabilities. The challenge is not to kill the goose that lays the golden eggs.

An even more difficult set of issues arises under the rubric of government security, which historically has been about information security. Networked computing and telecommunications have added a new set of issues with respect to the protection of hardware and infrastructure, but ultimately IT security too is about the information that it houses. There are many legitimate reasons for protecting information, beginning with the need to maintain the integrity of the government’s information holdings – if only so that they can be properly used, including in support of the system of accountability – and, from a citizen perspective, to protect personal information and other information provided with an expectation of confidentiality. These are central concerns of e-government-oriented public administration and are given a senior focal point within the public service in the government CIO. However, even these uses have required the introduction of additional checks and balances, notably the Information and Privacy Commissioners acting in support of Parliamentary accountability, in the first instance to ensure that the rights of individual citizens and information requesters are respected but also to monitor the government’s practices in the management of information generally and the collection of personal information in particular.

A major dilemma arises, however, from the potential for abuse that arises from the same networked ICT-enabled environment that facilitates the beneficial aspects of e-government. Information about citizens and the public more broadly is used in more than a service-to-the-public or regulatory context, notably in the realm of policing and national security. Although part of public administration, and playing specific roles in the internal management of government – for instance providing protection against hacking into government e-mail and data bases or conducting security clearances of prospective employees – the police and security agencies are in effect program-delivery organizations, primarily oriented towards the larger society and economy.

By definition information-based, police and security agencies depend on their ability to amass as much information as possible related to their cases, to identify patterns and make linkages, and in general to cut across the information boundaries and protections that exist in other areas of the public service. Police and security agencies of course have a vital and legitimate role to play in protecting the state and supporting democratic institutions, but on the margins they also carry the twin risks of becoming laws unto themselves, on the one hand, and tools of the political interests of the government of the day, on the
other, based on their extensive information gathering and analysis capabilities. A similar danger is of a government using public administration’s information holdings to further its partisan interests, whether in efforts to punish its critics or to reward its supporters. Again, networked databases increase the possibilities of abuse and the pressures on public trust.

Accountability in the context of e-government also has several dimensions. The constitutionally-based principles and mechanisms of public sector accountability are not changed by ICTs and e-government, and the CIO operates within the Canadian public service’s accountability model for management policies and practices that has been in place for nearly half a century. But some significant new elements have been introduced. The establishment of the CIO and the consolidation of a set of e-government management policies into an identifiable administrative space constitute a significant change to the larger administrative map, reshaping the map itself and changing the priorities within it. That is to say, the substance of what managers and staff in government, as well as the government as a whole, are accountable for has been affected. In addition, the way in which accountability is exercised has been affected. For example, the Canadian government has in recent years made a practice of requiring government departments and senior managers to post on government websites information in a number of areas of spending, in the name of greater transparency and accountability. These include: travel and hospitality expenses, contracts over $10,000 (a level at which managers have considerable discretion), and reports of contacts with registered lobbyists (Canada TBS 2012).

The greatest change, however, and the greatest challenge, has been in the media and political environment in which accountability is exercised. The 24-hour news cycle, combined with the Canadian version of the Westminster model, which includes a daily parliamentary question period in which any Member of Parliament can ask a question on any topic without notice to any Minister, has created an environment in which all executive actions are potentially subject to close Parliamentary scrutiny, but also where any action can quickly be escalated into public controversy. The greater availability of information through electronic channels is being parallelled by attempts at greater control of its release and of access to the media by public servants. The debate is just beginning in Canada about whether this is healthy or how its effects can be mitigated.

Conclusions

E-government is perhaps best understood as an analytical construct that is a sub-set of the study of governance. In the short to medium term, the powerful forces created by ICTs have created a kind of parallel universe where the roles and dynamics of government are carried out in ways that are observably different from earlier norms, many of which are still prominent. In the longer term, e-government will inevitably integrate with older, historically derived institutions, relationships and norms, themselves shaped by earlier technologies and innovations. In that sense the use of the term and the focus on it is transitional, helping to absorb a new dimension to an already complex environment.
This is not to argue that a concern with e-government is unjustified. While the basic features of the state and of public administration remain and will likely endure, the speed and extent of the introduction of ICTs into all aspects of daily life, going well beyond the public sector, and their continued velocity make it essential to try to understand their nature and implications. This is even more important because the effects are felt in different ways and to differing extents in different segments of the population and as between different economic and social actors. This unevenness will no doubt persist, although it can be expected that over time the great majority of the country will acquire ready access to electronic networks and the skills to use them; this may take a generation or more, however, just as there was a long transition in a country like Canada for telephone use to become the norm and its implications for public administration to be worked through. While this lag needs to be taken into account in societally-oriented public policy, it will, however, be much shorter within the public sector. The Canadian government, for one, can already assume universal access in public service workplaces to electronic information and communications technologies and electronically-enabled office procedures, and in that sense the line between e- and non-e-government is becoming increasingly obscure.

If the technological environment of government has undergone profound change in the two decades since the CIO was established, the culture and institutional assumptions, including those relating to trust and accountability are still catching up. This is the real importance of studying the phenomena that go under the heading of e-government. In a liberal democracy, much about the state and public administration remains the same: the foundation of rule of law and constitutionality, the central role of representative legislative institutions, principles and broad practices of democratically responsive administrative institutions and much more will remain integral features of the new dispensation. At the same time ICTs have brought important features that are new, of newfound importance or in new combinations that are here to stay.

A partial list in no particular order includes the widespread availability of self-service mechanisms in the delivery of services to the public (as well as of services to employees); the extensive linking of information in databases and through government networks, with wide possibilities for data aggregation and knowledge creation; the digital permanence of a broad range of information, including much that in the past was considered ephemeral; the ability to link groups of people and sources of information simultaneously, using various formats and communications channels; the shift of the centre of gravity in the relationship between the state and the citizen from the perspective and needs of the state to those of the citizen (although with important caveats); the greater prominence of private sector and other non-governmental actors in providing services both to government and even on government’s behalf to the citizen; the ability to obtain policy input from the public in “real” time and through a variety of channels; and the possibility of some form of direct democracy through the availability of on-line voting technologies.
Interestingly, in the Canadian federal government, most of the administrative policies that are being used to address this changed environment were already in place before the introduction of the Internet and the establishment of the CIO – both of which occurred in the early 1990s and which for the purposes of this discussion provide a starting point for the e-government era. Some changes have been made to the policies in response to ICTs, but even more important has been the changed institutional environment in which they are applied by bringing them under the direct or indirect leadership of the CIO. This has had the effect of giving greater prominence to the goals, values and relationships that they embody, both individually and in combination. The latter is particularly important in the context of a discussion of trust because there are basic tensions among the different policy areas that can be managed but not eliminated. In particular they bring to the fore tensions between access, dissemination and participation on the one hand and protection and restraint on the other. How these tensions are managed by government and how they are perceived to be managed by the public in general and the media and politicians in particular will have an important bearing on the trust equation in the future.

It is therefore vital to have effective oversight and accountability mechanisms in these areas to guard against abuse. These ultimately depend on the extent and capacities of democratic institutions, however, notably representative institutions and the courts. These institutions continue to operate much as they have in pre-e-government times, and their credibility has a major bearing on all aspects of the public’s trust in government. This is equally the case in the context of e-government, where established institutional assumptions remain but the context has changed and in many ways the public’s standard of judgment has as well. In the final analysis, human psychology has not changed, but the environment in which it applies has undergone considerable change and will continue to do so under the influence of ICTs. Maintaining the public’s trust and exercising democratic accountability will be all the more challenge for public institutions, and this will not always be easy to achieve. At the same time these issues will need to be successfully addressed if government is to fully absorb and act upon the potential that ICTs offer.
Trust and accountability and the internal governance of e-government

References

Articles in journals:


Books and Monographs:


Marson, Brian and Ralph Heintzman. 2009. Research to Results: A Decade of Results-Based Service Improvement in Canada. Toronto: Institution of Public Administration of Canada.


Contributions to books:


Trust and accountability and the internal governance of e-government


**Government and NGO documents:**


