Privacy, Identity & Digital Policy: A Comparative Assessment of the United States, Spain & Canada

Paper Presented at Queen's University
International Workshop on Privacy & Surveillance
November 16th & 17th, 2006

Jeffrey Roy
Associate Professor
School of Public Administration,
Faculty of Management
Dalhousie University
Email: roy@dal.ca

1) Introduction

The purpose of this paper is to examine the nexus between privacy, identity, and the digital policies and electronic governance initiatives of governments in three different national jurisdictions included in the international public opinion survey on surveillance and privacy: Spain, the US, and Canada. Undertaking a comparison of Spain and the US is useful on two fronts beyond this direct two country comparison: first, it allows for a broader comparative consideration of North American and European dimensions to privacy and identity issues; and secondly, it enables Canada to be situated within both national and continental perspectives.

The guiding premises underpinning this investigation are twofold: first that terrorist attacks in both Spain and in the US since (and including) 9-11 have bolstered public sector action aimed at stronger security measures that make use of new digital technologies in order to augment capacities for identity authentication and management; and secondly, that resulting privacy concerns, even if trumped by security, remain important political considerations in the countries in shaping government action.

These premises can be partly viewed as hypotheses to be tested and confirmed or modified by the survey data. However, somewhat general, they are also meant to serve as a platform for a more rigours, comparative examination of the two countries in order to dissect in particular the second premise above. Key questions include: i) in what ways does public opinion vary across both countries and why; ii) how are these differences (if any) tied to the respective political systems (i.e. Parliamentary versus Presidential) and what are the implications for transparency and accountability; and iii) are (and how) political models of federalism impacted by the emergence of digital governance emphasizing electronic identity interoperable public administration networks.

Building on this comparison, the Canadian case can then be presented and considered accordingly in terms of the potential lessons from each country that carry influence or relevance for the Canadian experience. Moreover, Canada-US relations and continental governance dimensions to privacy and identity may also be contrasted with Europe. This paper will thus conclude with some insight as to whether or Canada seems to be maintaining its traditional middle ground between European and American governance models, as well as the implications of Canada's positioning for identity and privacy matters specifically and democratic accountability more generally.

2) Electronic Government and Four Dimensions of Change

With respect to public sector action and democratic accountability, Identity and privacy trade-offs may be viewed trough both administrative and political lenses, both of which are intertwined with the emergence of electronic or e-government during this past decade. E-government may be defined as: 'the continuous innovation in the delivery of services, citizen participation, and governance through the transformation of external and internal relationships by the use of information technology, especially the Internet'.[i] Building on this definition it is possible to point to four significant dimensions to public sector change in a digital era: service, security, transparency and trust (Roy 2006). All of these dimensions are inter-related in some manner with the widening presence and rapidly expanding importance of a digital infrastructure encompassing information and communication technologies and online connectivity.

Service and security:

The first two of these dimensions are primarily focused on changes to the internal decision-making architecture of government, in response to pressures and opportunities associated with the Internet. Indeed, delivering services online became the hallmark of e-government during the 1990s: as more and more citizens conduct their personal and professional affairs online, these 'customers' of government look to do the same in dealing with state, whether it is paying their taxes or renewing permits and licenses of one sort or another (Andal-Ancion and al. 2003; Curtin 2003). As governments moved online it became intuitive that an online reiteration government departments and agencies would not be the most effective way of developing more transactional and interactive capacities in an efficient and effective manner (Fountain 2001; Kearns 2004). Thus, the notions of service streams were developed, clustering and organizing services in a citizen-centric manner (Coe 2004; Goldsmith and Eggers 2004).

Yet in many cases service functionality remains limited, particularly with respect to the processing of financial payments. This is a limitation due in large measure to the concerns about security (Holden 2004; Radl and Chen 2005). The ability to interact effectively with customers online requires a safe and reliable architecture, particularly for the handling of personal information – such as credit card numbers – that often underpins financial transactions (ibid.). Fostering government-wide capacities for receiving, storing and sharing secure information is a complex undertaking, and the benefits of more efficient and integrated care through networked information systems are entirely dependent on secure and inter-connected governance architectures (Joshi and al. 2002; Entwistle and Martin 2004; Patton 2005; Bellamy and al. 2005).

These first two dimensions, service and security, are primarily about how governments are reorganizing themselves internally to adapt to new opportunities and threats in the external environment. In contrast, transparency and trust speak to changes rooted less in the internal structures of government and more in the evolving democratic environment within which governments operate – as the Internet has facilitated the creation of new channels of political mobilization and interaction between citizens and their governments (Prins 2001; Coleman 2003).

Transparency and trust:

It has been said that we live in the 'age of transparency' (Tapscott and Ticoll 2003). For organizations in all sectors, openness must be embraced as routine and ongoing since secrecy invites suspicion, resulting in questions, exposure and increased costs and complexities down the line (Mitchinson and Ratner 2004). As e-government creates expectations for improved transparency, and as information is more readily available and more widely shared by public sector authorities themselves, the Internet has greatly facilitated the potential for performance reporting by both government bodies and neutral and subjective observers (Stowers 2004; Wilson and Welch 2004).

More than a mere technical apparatus for providing information, the Internet has also become an associational infrastructure, enabling knowledge and power to be more widely distributed and contested (Paquet 2004; Courchene 2005). One result is a lessening of tolerance for secrecy as individuals and new forms of associational movements mobilize around specific issues and interests (Evans 2002; Dwyer 2004). Governments themselves have not been immune or ignorant to these pressures for reform, responding increasingly with calls for more public participation and citizen engagement (Oates 2003; Oliver and Sanders 2004; Coleman and Norris 2005).

Here lies the basis of a major foundational shift under way for democratic governance. A world of information scarcity is one that bolsters bureaucratic power and organizational secrecy (Fountain 2001; Kamarck 2004). A democracy of limited information and knowledge means an uneducated citizenry deferring to the authority of the ruling elite: pressures for more openness are limited and easily repressed. In a world of digital communications and widening networks of social and political interests (both online and offline), governments face rising pressure to adapt to a much more fluid and dynamic informational environment – one that is far less conducive to secrecy (Juillet and Paquet 2002; Tapscott and Ticoll 2003). The emergence of web-blogs is a case in point.[ii]

Despite such pressures, governments may also resist change, as "the culture of secrecy is deeply engrained" (p. 82, Reid 2004; Roberts 2005). The degree to which this resistance is durable, as well as its impacts of public perceptions and ultimately the performance of government itself, is interwoven with the notion of trust. Trust is multi-faceted in terms of how governments seek, retain and deploy legitimacy in pursuing policies and action tied to the public interest (O'Hara 2004). There is evidence that trust is less deferential in nature and more forged on the basis of direct exposure and engagement – handicapping unresponsive hierarchies in both the corporate and political worlds (Cairncross 2002; Dwyer 2004; Eggers 2005).

Consequently, many proponents of e-democracy seek new opportunities for more direct and continual forms of public participation[iii]. While calls for such expanded forms of engagement predate the Internet, online connectivity is a powerful enabler given the potential to both distribute information and power more widely and facilitate a broader conversation with stakeholders and the public (Clarke 2004). Yet, any systemic introduction of more digital forms of democracy would constitute a major revolution in all aspects of the public sector apparatus, both technologically and organizationally (Pavlichev and Garson 2004). This revolution is uncertain at best given historical evidence suggesting that digital technologies will most likely be used by those in power to reinforce existing power structures or at the very least, resist efforts to alter them (Kraemer and King 2005).

3) Identity, Interoperability & Privacy

Across the four dimensions of e-government perhaps no issue has received more attention than that of privacy – tied to ongoing concerns about the handling of personal information. At a basic level, many individuals continue to shun online shopping for fear of releasing confidential details such as credit card information into a virtual gateway with a perceived host of potential unintended consequences as to how such data can be shared and used[iv].

At the same time, however, significant growth rates of both Internet use and online services would suggest that while some segments of the population may continue to shy away from online channels (or face barriers associated with the digital divide), clients and citizens in all sectors will be proportionally more likely to move in such directions over time[v]. Banking online offers some support for this view: in 2003, online banking transactions in Canada rose 30.7 % to 192.1 million transactions (in comparison to 26.6 million in 1999), whereas telephone banking transactions fell by just under 5% to 87.7 million (both channels trail volumes at electronic banking machines that nonetheless fell 6.2% in 2003 to 1.131 billion transactions).[vi]

Perhaps more than fears about malicious acts, concerns about privacy and personal information weigh even heavily on government efforts to deliver services online. This characterization reflects the interaction of technical, organizational and socio-political variables shaping debates about information management and security. Moreover, government services often differ qualitatively from those of the commercial sphere, with more obligatory relationships resulting in the collection of highly sensitive information across a wide range of entities and functions that collectively comprise 'the public sector.'

There may well be sound reasoning for governments taking a more cautious and gradual approach than their private sector counterparts, much of it security-related. The political risks of security breaches in the state settings are often perceived to be far more serious than proportionally similar risks in the private sector context, a comparison most often attributed to the significantly greater holdings of personal and sensitive information held by the public sector (Joshi and al. 2002; Holden 2004). This relationship is complex and dependent to a significant degree on the level of trust accorded to the public sector by the citizenry. In jurisdictions where trust is high, technical solutions are more readily supported and the organizational changes required for more innovative and integrated forms of service are more feasible. The converse is true as well – where lower levels of confidence and trust translate into stronger vices for both organizational resistance and technical cautiousness. It is for such reasons that it is impossible to separate out service-delivery capacities of e-government with broader institutional reforms shaping the setting of democratic governance within which such processes occur[vii].

Nonetheless, even within a standardized set of social and political conditions all governments must address both the perceptions and realities of privacy within a broader spectrum of information and identity management that is at the core of both better client-centric responsiveness externally and the corresponding need for new forms of coordination internally. There are two inter-related components in doing so: putting in place an infrastructure of reliable interoperability and ensuring mechanisms for accurate identity and authentication (Lips and al. 2006).

In terms of a reliable and interoperable infrastructure internally, a fundamental requirement for more citizen-centric governance is the ability – facilitated by a secure architecture, to both store and share personal information in a virtual manner across previously separate organizational units. In theory, it becomes possible for an individual or a company to expect (or endorse) that information provided through one public sector gateway (i.e. a service renewal or transaction completion) should be readily available across the public sector for any other usages that may arise, be they related or unrelated to the initial encounter (Kearns 2004; Bellamy and al. 2005).

As information management and privacy issues continue to grow in their reliance on a digital infrastructure, three dimensions of computer security can be underscored as central: *confidentiality* - requires that information be disclosed only to authorized parties at the authorized time and in the appropriate manner*; integrity* – includes both the trustworthiness of the content, as well as the origin of the information; and *availability* refers to the ability to access and use information or resources as desired (adapted from Radl and Chen 2005). The issues of identity and authentication are central to this model. Although once again not entirely novel, they are far-reaching in their potential to reshape both the expectations of the citizenry and the performance of government in a digital era.

Governments also maintain multiple points of contact and interactive dealings with single individuals or organizations – and as such, they are increasingly keen to explore a similarly integrated approach on a holistic or even partial scale of service and transaction types. While the potential for 'value' creation is real (Kearns 2004), so too are the risks associated with an 'identity' tied to more and more information flows that, in turn, must be stored and shared (Joshi and al. 2002). In a networked world, each mechanism for identify verification leads to another possible opening for breaches that can then be used to penetrate a variety of gateways into interconnected systems:

> *As more identifiers are linked to one identity, the threat to privacy and data integrity increases, and the security of the data decreases. Absent substantial controls on how this information can be used, shared and stored, there are wildly varying management practises for the same data…Any party looking to subvert data will seek data or systems at the lowest level of protection and then use the data for authorization to subvert the security surrounding high value users (p.6, Digital Government Civic Scenario Workshop Report 2004).*

Within such openness and connectedness, identify theft is a problem that appears to be growing in some proportion to the growth of Internet usage generally[viii], making it a particularly serious issue for the evolution of online and integrated services in the public sector. The correlation between identity theft and more unintended mishaps of information mismanagement on the one hand, and expanding Internet use (and usages) on the other hand, underscores why such issues are rising in prominence.

While such issues are hardly new - as concerns about privacy have permeated discussions about electronic information systems for the past many decades (Burnham 1980; Science Council of Canada 1984; Bennett and Raab 2003), the stakes are rising, not only to the individuals involved in sharing the personal information electronically but also to the economy as a while in so far as online channels for consuming and transacting are viewed as safe and reliable (OECD 2004). In short, fostering trust is both a private imperative and a matter of public interest in the virtual world.

Striking a balance between new forms of legal protection and self-governance involves a mix of extending and enforcing new legal rules on the one hand, and a more collective effort to foster a culture of risk management through personal and corporate responsibility. Such a mix will vary across cultures and jurisdictions: for example, whereas Europeans are said to be more distrusting of the private sector with respect to managing and sharing personal information, Americans have traditionally directed their distrust toward government (whether this dichotomy holds up in a post-9-11 world is further examined below).

Evidence to date suggests that in the realm of electronic service delivery – in both industry and government, a reliance on both set of measures is necessary due, in large, part to a segmentation of any population into three distinct camps: those highly suspicious about an erosion of personal privacy in a more digital world, those who are indifferent, and in between the largest proportion of more pragmatic individuals whose views are likely to shift according to experience and circumstance (Bellamy and al. 2005). It is precisely because of the fluidity of this middle group that perceptions of risk have become so central to discussions about information management and privacy in an expanded realm of security measures since September 2001 - aimed at preventing terrorism and ensuring public safety (Coleman 2006).

The parameters of the debate have thus shifted politically, but also technologically as digital tools are viewed less as means toward convenience and efficiency (laudable aims but ones flexibly interpreted by many) and more toward matters of security (Strickland and Hunt 2005). Many governments are now pursuing bolstered forms of identity management through more technologically sophisticated devices for authentication such as national identification cards and biometrically enabled passports[ix]. The former approach, for example, has been adopted by the British government which plans to introduce such a card by 2008[x]. Australia and Hong Kong are currently implementing new national 'smart cards' that would serve as an identity link to all public and private transactions conducted electronically. Italy and Spain have adopted similar paths, to name but a few (Torrisi and Mezzanotte 2004).

Further, many jurisdictions - including Canada and the United States, are presently exploring modified passports that would make use of biometric devices to improve authentication and identity management capacities (Meyers 2003). Radio frequency identification devices (RFID) are viewed as an area of particular interest for a developing a more secure infrastructure for commercial transactions, transportation and human mobility and verification schemes (Hodges and McFarlane 2004).

Defenders of such measures point out that terrorist and criminal elements are making effective use of new technologies to conduct their own plans (i.e. the 9-11 hijackers used the Internet to communicate and jointly plan their attacks) and it is therefore both normal and desirable that governments counter in kind. Moreover, for the vast majority of citizens who are law-abiding, there may be a presumed comfort level in having nothing to hide. Yet, such sentiment – coupled with fears of terrorism, may also yield a supportive environment for widened surveillance activity on the part of public sector authorities (Whitaker 1999). Some observers worry that a willingness to relax privacy in the name of public safety ignores the wider implications of a more digital information architecture based less on individualized human behaviour and more on patterns and profiles emerging from electronic data flows:

> *A classic error is repeated endlessly in numerous contexts, and it reveals the depth of the misunderstanding that surrounds surveillance today. The claim is frequently made that if we have done nothing wrong, we have nothing to hide and thus nothing to fear…The problem is that this is not how things work, especially in the context of surveillance as social sorting, as an aspect of complex assemblage of governance practises. Against the personal claims of individual innocence, surveillance practises are profoundly social, in the sense that persons are clustered into categories, whether or potential consumer groups or potential lawbreakers. It is one's often unwitting membership of or association with certain groups that makes all the difference (p. 140, Lyon 2004).*

Prior to September 2001, such concerns were but a small and limited outgrowth of the widening interest in 'customer relationship management' and personal marketing techniques that often depend on this type of individual clustering and response. More recently such issues have garnered more interest and attention in light of the expanded security imperative now pursued by governments, nowhere truer than in the US.

4) Comparing the United States & Spain

Since autumn of 2001, the mindset of governments in most countries – notably the US, has been dramatically reframed. The American fixation on homeland security denotes an important new face of e-government in terms of resources and priorities[xi]. The US is not alone: around the world, many governments have been quick to establish new anti-terrorism and homeland security measures that are premised on new or expanded capacities for coordinated information sharing, planning and responding on a government-wide scale (Henrich and Link 2003; Kim and Lee 2004).

A sophisticated and reliable digital infrastructure is a necessary precursor to such government-wide action – and as such, interoperability has become a guiding principle in such efforts. Moreover, in fostering a systemic view of security within a jurisdiction such as a country, interoperability across sectors (notably, the private sector) also becomes an important element (Dutta and McCrohan 2002). Strategies for cyber-security rely heavily on public – private sector cooperation (Lane and Roy 2006).[xii]

Central to such efforts are the increasingly electronic formation and management of both information flows and identities. With respect to information, the challenge is not generating more of it but rather making sense of it (thereby creating knowledge as a basis of policy and action[xiii]). An important and contentious tool in homeland security is data mining that – much like the term implies, involves digitally and virtually trolling through massive amounts of information gathered in raw form, and then analyzed for meaningful patterns or events (Chen 2002; Sirmakessis 2004). Few areas have attracted more attention from US federal authorities over the past five years (Regan 2004). Various US federal initiatives involving data-mining such as CAPPS II, MATRIX, and the Total Information Awareness program have generated controversy (all of which have been abandoned but not without similar undertakings continuing to be pursued).

For US authorities, three factors have arisen as sources of concern and debate. The first factor is the significant financial investments now flowing into security efforts - and an expanded digital infrastructure for information analysis, communications, research and development, and new screening and surveillance systems. Some industry estimates

point to homeland security spending levels in the United States to surpass $180 Billion by 2008, a figure that includes all levels of government and the private sector (and an amount that nearly equal the total annual budget of the Government of Canada).[xiv]

Such massive injections of public funds face growing questions about the extent to which managerial, accountability and oversight capacities are up to the challenge of deploying these resources in a responsible and effective fashion. Therefore, the second and quite related factor is the size and complexity of the organizational deployment. Difficulties that plague the US Department of Homeland Security are a case in point: the Department has been unable to fulfil its role in effectively consolidating and coordinating the formation and usage of terrorist watch lists from its various sub-units, a deficiency ascribed by department officials to an absence of resources and sufficiently developed infrastructure for doing so.[xv]

The third factor – undoubtedly the most politically contentious, is the appropriate scope of security objectives and means to be undertaken by democratically accountable governments. Tensions in the US between a traditional mindset of limited government and the post-9/11 jump in support for an expansion of state activity are thus central in shaping political debate, particularly through the spring and summer of 2005 as the Patriot Act underwent a Congressional review under the guise of a sunset clause in the initial legislation. While the spirit of the Act remains largely unmodified, specific provisions – notably those pertaining to wiretapping, surveillance and the so-called 'library' clause have generated scrutiny.[xvi]

A key issue in such an environment is an absence of sufficient openness on the part of public authorities (Reid 2004). US government watchers claim that during this decade the culture of secrecy has been significantly reinforced at the expense of transparency and public accountability.[xvii]Another, related dimension to such concern that secrecy is becoming the norm in security matters - due in part to covert activity, but also the extraordinary level of complexities that permeate an increasingly ubiquitous and invisible infrastructure extending across the realms of both government and commercial activities:

> *Law enforcement and intelligence services don't need to design their own surveillance systems from scratch. They only have to reach out to the companies that already track us so well, while promising better service, security, efficiency, and perhaps most of all, convenience. It takes less and less effort each year to know what each of us is about….More than ever before, the details of our lives are no longer our own. They belong to the companies that collect them and the government agencies that but or demand them in the name of keeping us safe (p. 300, O'Harrow 2005).*[xviii]

The existence and reliability of such identifiers thus become critical enablers of the functioning of the system as a whole. With respect to individual privacy, it is the efforts of the federal government to systemically interlink unique identifiers and virtual information flows that is one cause for concern. Regan's detailed analysis of the detailed provisions of the Patriot Act demonstrates the critical extensions of information gathering capacities on the part of law enforcement authorities, accompanied by a weakening of political and judicial oversight mechanisms – leading to what the author terms as a total absence of accountability. More specifically, the author formulates three fundamental implications from her analysis:

> *first, the capstone of the creation of a domestic surveillance system; second, the government's ill-conceived assemblage of unmanageable amounts of information; and third, the possibility of the creation of a national identification system in the United States (p.490, Regan 2004).*

Indeed, the latter implication is supported empirically by three simultaneous initiatives led by federal government authorities: i) within the federal government the creation of new smart cards envisioned for all federal employees, the first of which were administered in October 2006; ii) federal legislation requiring states to meet national specifications for technologically bolstered and interoperable driver's licenses; and iii) the proposed development of a national id card for Americans travelling abroad as a low cost alternative to a passport (and somewhat related new id requirements on foreigners entering the country, with the US leading international efforts to develop biometrically-enabled, electronic passports recognizable across jurisdictions).

Such developments have clearly recast the internal, administrative architecture of digital networks away from a pre-9-11 emphasis on new service models to a security fixation. Key questions are apparent in terms of transparency and trust, driven by the views of the American public. Before turning to an analysis of American survey results, we will first review the main contours of Spain's political environment in terms of e-government and the relative balance between service and security.

The Spanish Case:

In terms of both aspirations for and the adoption of e-government over the past decade, Spain occupies something of a middle ground between those countries typically thought of as technological leaders and developing nations. Clearly more wealthy and democratic than the latter group, and firmly implanted as a core member of the European Union, Spain nonetheless lags many of its Northern European cousins in Internet accessibility and usage.[xix] In 2005, 21% of Spanish households possessed a broadband Internet connection (most all concentrated in Spain's largest cities), while just 3% of Spanish enterprises received orders online for their products or services (just 8% of Spanish individuals reported an online purchase).

For such reasons, the Spanish national government (quasi-federal, with 17 autonomous regions, each with its own Parliament and control over its own system of local governments) has viewed e-government as two inter-related reform agendas – first, to improve the performance of the public sector in terms of new service delivery channels presented by the internet and new information technologies (while refurbishing the internal administration to do so); and secondly, to foster stronger socio-economic and political development throughout the country as a whole by encouraging the usage of digital infrastructure. A derivative of this latter direction is a view that e-government can be a driver of more openness and transparency in public sector governance and new opportunities for public engagement, thereby raising levels of trust accorded by the citizenry to their government.

As with most countries, it is the service dimension that has been most visible in Spanish e-government efforts – at both federal and regional levels. The current e-government strategy of the Spanish government is presented in the 2004-2007, Public Administration Technological Modernization Plan. This plan, otherwise known as Plan Conecta, is "designed to improve the quality of services provided by Spain's central administration

and to bring it closer to the citizens and businesses by using new technologies, reducing bureaucracy, simplifying procedures and eliminating unjustified delays."[xx] Spain's wealthiest and most autonomous and politically assertive of regions, Catalonia (encompassing Barcelona), is pursing similar aims through a government-wide initiative known as CAT 365 that also encompasses many local administrations.

Within this context the emergence of smart cards as a basis for electronic and more integrated services is a cornerstone of efforts to promote both digital government and a digital society more broadly. The new electronic id card (eID) envisions not only faster and more accurate (and paperless) id authentication processes, but also the usage of electronic signatures and contracts as a basis of virtual engagements between citizens and companies on the one hand and public sector authorities on the other hand.

Following initial and ongoing pilot initiatives in various Spanish communities, the current objective is to enable country-wide usage of these new cards by the end of 2008 (though a more gradual, and flexible timetable is envisioned for when all citizens will be in possession of one, recognition of reality in light of the aforementioned figures on varying Internet access and usage across the country). While these new cards will be embedded with a microchip to facilitate secure online transactions and real-time access to photos and digitalized hand-written signatures, there are no immediate plans for the incorporation of biometric devices (despite ongoing discussions at the European level).

It bears noting that despite the service improvement connotation to such cards, the lead public sector authority in development and implementation has been the national police, acting within the Ministry of Internal Affairs. No stranger to domestic terrorist activities (primarily rooted in the Basques region), Spain was itself jarred by international terrorism in 2004 when the Madrid subway bombings killed 191 people and wounded nearly 2000 more. Some observers contend that the political fallout from the event (that happened on the eve of a national election) greatly shaped the outcome – bringing a new government to power.[xxi] Nonetheless, while the new government would quickly take distance from the US (announcing a military withdrawal from Iraq), security and terrorism remain key priorities of the federal government, in a manner that with respect to id mechanisms and balancing of security and privacy may not differ greatly from efforts of the US federal government (a point to be more explored more fully below from the public perspective upon review of the survey data).

With respect to political oversight mechanisms and actors pertaining to security and privacy matters, however, Spain is closer to the Canadian Parliamentary model than that of the divided executive of the US Presidential system. With a majority in Parliament, the Spanish Prime Minister and his Cabinet are in full control of the resource and decision-making apparatus of the executive branch – answerable to opposition parties also represented in Parliament. Furthermore, in recognition of the importance of privacy as a public issue, and in a manner not unlike Parliamentary jurisdictions elsewhere in Europe (as well as Canada, Australia and New Zealand), an independent privacy authority also acts as a watchdog (answering directly to Parliament as opposed to the executive).

In Spain, this individual is the Director of the Spanish Data Protection Agency, and he is an instrumental figure in matters of information management and the introduction of the new eID strategy. While little research exists as to the efficacy of this function in the Spanish context (that this author could find), there has been some recent debate and criticism as to the invoking of such responsibility in a single individual, with some political

stakeholders proposing a broader commission of members to augment accountability through a wider range of viewpoints and deliberation. It seems that in contrast to the Privacy Commissioners of Westminster countries in the Anglo-Saxon world (where such a Commissioner is understood, for better and for worse, a theme returned to below, to likely be a critic of the government), there has been some concern about whether or not this individual in Spain is sufficiently independent (alternatively, historically rooted Spanish unease with an excessive concentration of power may also be a factor[xxii]).

In contrast to North America, Spain's governance and policies are also intertwined with the continental architecture of the European Union – with its own President, Council (Heads of Member States), Commission (bureaucracy), Courts, and Parliament. In addition to the judicial and political oversight of these latter bodies, a European Data Protection Supervisor (EDPS) serves as an independent officer reviewing all European institutions (in a manner akin to the Spanish and Westminster models), while each individual institution also appoints a data protection officer that works in concert with the central European office (at present the Assistant EDPS is from Spain).

Similarities & differences:

Before comparing Spain and the US in terms of public attitudes, this institutional contrast between the United States and the EU (as well as most member states and Parliamentary jurisdictions including Canada) is worth underscoring. In the US, the absence of an independent privacy authority (criticized by some) is offset in some manner by Congressional oversight – whereas in Parliamentary jurisdictions, the absence of sufficient political oversight (as with other domains such as financial management and spending) has led to the appointment of new and specific bodies to compensate. By contrast, the European model is arguably a more complex hybrid.

Prior to 9-11 it was common to assert that privacy differed greatly across Europe and the United States in terms of both public sentiment and legal regimes. The somewhat generalist claim (that despite shifts to be discussed remains relevant today) had been that in terms of the possession and management of personal information, European distrust was primarily directed at the private sector whereas in the US, Americans were most overtly suspicious of government. Accordingly, stricter European privacy laws covering corporate behaviour have been a particular point of distinction and often contention between both continents (Prins 2001; Archick 2006).

Such overtones would seem to be reflected in the results from the international privacy survey, where Spaniards are more distrusting of the private sector on most matters than is the case in North America (Canadian and American results are quite similar). It is notable for instance that of the three countries, Spain is the only one where more than one half of the population rejects the notion of their government sharing personal information with the private sector. Similarly, just over 70% of Spanish respondents support (with over 40% strongly agreeing with) the notion of a government-sponsored national ID card, while fewer than one half of Americans concur. A similar result is apparent in the implicit Spanish support for the creation of a national database to underpin id card expressed as a high degree of confidence in 'having a say' in how such information is handled: nearly 80% of Spaniards feel they would have at least some say, with one half of this portion characterizing it as a 'complete say' (by contrast less then 20% of Americans and Canadians feel that would have a complete say, with overall just over one half of respondents in both countries expressing at least some say).

This general predisposition toward a greater level of confidence in such an undertaking helps to explain why identity management and interoperable mechanisms as a basis of more integrated service delivery have been somewhat less politically sensitive in many European jurisdictions. The added layer of terrorism and security merely reinforced this comfort level with more assertive state strategies. Such is the case for Spain – seemingly intent on the one hand in deploying new technologies, and notably a smart card, to improve service and transcend traditional bureaucratic processes, while on the other hand embracing the need for stricter security measures in the aftermath of Spain's own internationally-rooted terrorist attacks in 2004.

The United States, by contrast, has embarked upon a path of identity and interoperability led by the federal government in a manner that would have been unthinkable prior to 2001, even with the advent of e-government and its service emphasis. Indeed, the US would appear to be undergoing two simultaneously shifts in terms of the public mood pertaining to privacy and information flows across the public and private sectors: most dramatically in being generally supportive of federal government initiatives tied to security, but also more subtly in widening unease about company breaches and growing calls for stricter legislative and regulatory enforcement of misconduct (Holmes 2005).

In terms of governmental action, the survey results suggest, however, that the US President does not garner unqualified support for security initiatives such as a national id card – with nearly one-third of Americans strongly disagreeing (and another 15% also disagreeing). Aside from Congressional oversight and alternative proposals in areas such as border controls and a new id card for international travel (and potentially a Congress partially or fully controlled by Democrats following the November 2006 elections), US States are also powerful stakeholders, as is a critical media and an underlying current of suspicion toward government that has long been a defining characteristic of the American political culture.

Some activist groups such as Privacy International have in fact pointed to these American contrasts in making the case that the European Union (and one can suppose by extension many of its member countries) may actually be surpassing the US in eroding personal freedoms and privacy. In a detailed, comparative examination of policy and process in both the EU and US, the author concludes that:

> *Both the US and Europe have implemented far reaching powers in the name of combating terrorism. In many areas they have implemented similar policies. They have both used strategies to lessen debate, either through appending ills to spending measures (e.g. Real ID Act in the US) or approving a policy at a closed-door international forum despite the protestations of Parliaments (e.g. Passenger data, biometric passports, and communications data traffic retention at the EU).*
>
> *If there is one remarkable difference between the two it is that when the US goes too far on a policy and controversy arises, eventually public discussion and the democratic process tends to restrain the powers of the Government. There is no similar policy deliberation in Europe (p.41.)*
>
> *…Consistent surveys of the American people show that the vast majority are concerned with the use of personal data by both industry and government, despite the simplistic explanation that is usually proffered that Americans fear only their Government and not abuse by the markets.*

> *In Europe there seems to be a complacency on the protection of personal data. There are no equivalent surveys of public opinion except for when a terrorism law is being discussed. There is little public discussion on privacy (p.44, Hosein 2005).*

Partly derived from the preceding discussion, a case can be made that such a viewpoint may be a somewhat extreme characterization of both continents. In the US, for example, it is not clear that the 'vast' majority are concerned about industry (but concern is growing and increasingly shared across both sectors). Moreover, it was the efforts of European governments and European Parliamentarians that has prodded the EU in challenging the US on several fronts – including secret CIA prisons and the transfer of air passenger information between European and American authorities. Finally, on the matter of RFID usage, the EU has shown itself to be consultative and prepared to draft new laws to reassure public opinion that seems uneasy with the potential usages of this new technological instrument (although in line with the European market-state dichotomy of trust and suspicion, the unease would seem more directed at industry than governments[xxiii]).

Yet there seems little question that this perspective of Privacy international is also not without credence in underscoring the post-9-11 convergence of public opinion and public policy across both continents, particularly as codified by executive branches in each respective governance model (pluralized in the case of Europe if one includes both national and pan-European authorities). By the same token, if Regan's analysis (above) is correct, many American checks and balances have been eroded by the still dramatic shifts in public opinion since 9-11 and corresponding efforts on the part of the Bush administration to vigorously pursue anti-terrorism through a Presidential-based concentration of power. The American case is probably schizophrenic, elusive of any final verdict on such matters – but an interesting and important notion is the view that the extent to which government initiatives that may threaten privacy are contested publicly and politically is a healthy sign of dissent and a positive variable in shaping government action and helping to ensure transparency and accountability.

As a European member state (predisposed toward high degrees of government intervention), strongly influenced by terrorism for both domestic and international reasons, and with a Parliamentary model not known for its formal checks and balances politically, Spain would seem to run the risk of being overly deferential to the trustworthiness of their government in terms of both political motives and administrative competencies. Such a characterization is partially tempered by Spain's increasingly entrenched democratic culture and the added layer of (at times questioned) European oversight (itself influenced by Northern European countries that are strong proponents of open and transparent government[xxiv]), but it is one that should be safeguarded both for its potential consequences in that country as well as its relevance to the Canadian case.

Where Spain and the US would seem to converge, by contrast, is in the growing activism and visibility of central (i.e. federal) governments in leading the charge on pursuing the nexus between e-government, service and security (that is at the heart of privacy matters). While the international survey on privacy did not examine inter-governmental dynamics, a related investigation of the nexus between e-government and federalism (that included Spain) confirmed the centralizing tendencies of national efforts, calling into question the relevance and sustainability of traditional models of political federalism (Gasco and Roy 2006).

This theme, enjoining the Canadian case examined below, is quite relevant indirectly for matters of privacy and security – in shaping the patterns of administrative organization and democratic engagement that are central determinants in government priorities, actions and outcomes.

5) Canadian Complacency

Canadian governance and politics have often been characterized as reflecting a middle ground between the traditions of a larger and more activist state found in much of Europe and the market-leaning, anti-monopolistic culture, both economically and politically, found in the US. The most obvious example of this middle ground is the political structures found in Canada – consisting of a hybrid between Westminster, Parliamentary democracy and English and French historical influences, and more contemporary constitutional additions such as the Charter of Rights that has been viewed as more American in its emphasis on individuality protections and judicial intervention and oversight.

On matters of privacy and personal information flows across the private and public sectors, an argument can be made that this middle ground would seemingly be serving Canadians reasonably well. As with other Parliamentary jurisdictions, Privacy Commissioners in this country (federally and provincially) have been influential stakeholders in challenging governments. A case in point is the controversy that erupted in BC when the Privacy Commissioner found that outsourcing arrangements involving American firms and BC government organizations (especially those in the realm of health care) may have been placing at risk the personal information of BC citizens due to provisions of the Patriot Act (Roy 2005b).

In this case it was the Privacy Commissioner that became the catalyst for media attention and legal inquiry, resulting in corrective Government action that has largely quelled the controversy. Similarly, on a variety of other matters that have engulfed the US federal administration in controversy (including allegedly illegal wiretapping, information sharing between telecommunications companies and governments) the Canadian polity has been relatively peaceful and silent. Finally, recent RCMP efforts in the spring of 2006 to foil what appeared to be advanced planning and preparation by a terrorist ring based in Toronto reassures Canadians that the post-9-11 realities require strong domestic vigilance (with the overriding importance of security trumping privacy concerns in the eyes of many).

Conversely, the case can be made that there is a level of complacency in Canada that resembles that of Europe – particularly with respect to government. Such complacency has been challenged in recent months by echoes of US debates involving telecommunications companies (and their transferring of customer records to US authorities) when it has been revealed that similar practises are ongoing in this country (Geist 2005). Yet, despite the fact that new legislation will likely soon go before Parliament (based on already introduced proposals by the then-Liberal government that died with the calling of the most recent federal election) that greatly augments government wiretapping and surveillance capacities (while also placing new requirements on companies to partake in such processes by providing the relevant information to do so), little public outcry has ensued.

Any such complacency may well have been jarred by findings of the Arar Commission that – quite in addition to documenting the injustice inflicted upon one Canadian citizen, exposed mismanagement and a worrying absence of oversight and accountability both within and over Canada's federal police service (that also leads domestic anti-terrorism efforts). Yet, here again little public outcry has ensued (surely a condition in explaining why the RCMP Commissioner remains).

This complacency would seem to be supported by findings from the international privacy survey, with Canadians on par with American and Spaniards in feeling that they have some, a lot or complete say in what happens to their personal information. Moreover, Canadians are the most optimistic in feeling that their domestic laws are working well (with over 60% feeling they are somewhat (50.7) or very effective (12.9) with respect to government information holdings and just over 50% for private industry). Similarly harmonized results are evident in terms of the willingness of Canadians to allow governments to share their personal information (either unconditionally, when wrongdoing is suspected, or with public consent – presumably for service convenience): Canadians are the lowest of three in flatly preferring that no such sharing occur (with just 15.8% reporting this option).

The middle ground perspective (of Canada relative to Europe and the US) seems to find additional resonance with respect to proposals for a national ID card – a de facto reality in Spain that may explain the over 40% of Spaniards strongly agreeing with this notion. By contrast over one third of Americans strongly disagree – with Canadians in the middle of both camps (more supportive than Americans but less opposed). Opinion is similarly divided on the workability and efficacy of a national database, with only the Spaniards showing a majority confident that such a system is likely to be successful.

It is important here to underscore that in North America at present, it is the US federal government that despite its more polarized citizenry is intent on pursuing new national id mechanisms (that as Regan argues are surely likely to be interlinked within a broader surveillance framework), whereas the current Canadian government has been trepid in its intentions (largely reacting to US proposals that would impact border crossings while expressing cautious support but no tangible plans in terms of a new form of national identifier). Perhaps the Canadian government's uncertainty reflects the lukewarm support of Canadians (less opposed than Americans but less supportive than Europeans, including the British[xxv]), and the largely reactive nature of Canadian security policy (and by extension security/privacy trade-offs resulting from such policies) since 9-11 within a North American context.

The other explanation, one extending beyond the findings of the international survey, lies in Canadian federalism – and the fragmented nature of identification management in this country. While security is primarily a federal jurisdiction, life events and the resulting critical documentation (i.e. birth certificates) are provincial as are driver's licenses and health care (where identity management is fundamental to the realization of electronic health reforms). In a country reacting to the US and less directly scarred by terrorist attacks than the US, it may be that the federal government in this country is somewhat less bolstered to unilaterally infringe upon other levels of government by imposing new rules and mechanisms. This point is especially true of a political context in which the government of the day is more decentralist than its predecessors, committed to resolving the fiscal disequilibrium between federal and provincial governments. Yet, by the same

token inherent tensions remain between the federalist traditions of jurisdictional boundaries and the contemporary pressures for more interoperable and seamless governance (Jaeger 2002; Roy 2006).

6) Conclusions

A plausible case can be made from the preceding analysis that in term of the erosion of privacy and the overall efficacy of information management within a jurisdiction as a whole, Canadians should be more worried about complacency than Europeans (despite the contradictory logic in such a claim since a public is unlikely to be worried about matters for which it is complacent).

The US political system and its inherent checks and balances are important variables in shaping governmental action – especially at the federal level. While Spain's Parliamentary model features a more concentrated set of authority structures, there is a strong dosage of European realism aimed at challenging American perspectives and regulating information flows and privacy both pan-regionally and domestically (with an important degree of cross-fertilization across both levels). Still, it should also be noted here from the discussion in this paper that there is room for concern in terms of Spanish complacency – in light of inherently supportive European tendencies toward government action generally and a growing degree of convergence between European and American measures (as well as inter-continental collaboration[xxvi]).

What is difficult to explain is why echoes of US-based controversies in Canada as well as domestic episodes such as the Arar affair have failed to generate more public awareness and political scrutiny and dialogue. Although Privacy Commissioners deserve credit for drawing attention to key issues and mobilizing awareness, their inherently adversarial role as a watchdog of government limits their voice as a stakeholder in pro-actively formulating policy and administrative change. What is most disconcerting about security and privacy matters at present is the complete absence of political oversight on the part of elected officials. Since 9-11 and the subsequent creation of the federal Department of Public Safety and Security (fashioned after the American Department of Homeland Security), proposals to create a new Parliamentary Committee to oversee the federal government's security apparatus have continuously languished. The second and final report by Justice O'Connor, the Head of the Arar Commission, is to address the question of public-political oversight of the RCMP, though it remains to be seen the degree to which any such recommendations will yield reform.

One conclusion resulting from the analysis and argumentation of this paper is that the current Canadian complacency is contributing to a form of political paralysis with respect to the refurbishment (and especially the technological refurbishment) of the federal government's security and service apparatuses – that are interwoven with matters of information management and privacy. While the obvious exception to this claim was in the days and weeks following 9-11 when anti-terrorism legislation was formed and adopted at breakneck speed, since that time there has been little proactive effort on the part of successive federal governments to foster public dialogue. The aforementioned absence of action with respect to a national id mechanism is a case in point. So too are compounding difficulties plaguing the federal government's efforts to deliver services online, with problems pertaining to online identity management a central issue.

This conclusion is intimately tied to the transparency and trust variables of the e-government equation – and the consequences for identity and privacy. On the one hand, the implied notion of deferential trust toward government that characterizes much of Europe as well as Canada is increasingly challenged by current events (with identity theft, privacy breaches and cyber-insecurities growing in scope and regularity) and a broader societal shift in terms of information sharing, openness and education that is personified by the Internet itself. On the other hand, however, across both Europe and North America, national governments since 9-11 have done much to reinforce and increase the scope of secrecy both explicitly (in terms of security matters) and implicitly in terms of online, customer centric processes that downplay the citizenship aspects of governance in favour of real-time service simplicity, efficiency and interoperability.

This widening imposition of a syndrome of executive branch secrecy is perhaps the greatest threat to democratic accountability generally and personal privacy specifically. The risk lies in technocracy – driven by the virtualization of service and security apparatuses with a lessening of traditional political oversight and a failure to create new mechanisms of public engagement and review. Such conditions may support complacency in the short term, but at some point systemic breaches (of the sort that entrapped Mr. Arar) coupled with compounding questions about both competency and trustworthiness will take their toll. At such time, privacy and identity will be catalysts for a much needed and more holistic rethinking of the organizational and institutional architectures that are required for this new century.

A derivative matter (admittedly one not directly supported by the survey evidence invoked in this paper but nonetheless related) is the potential for an erosion of federalism in federalist jurisdictions (such as the three examined here) in favour of larger, more administratively and technologically centralized administrations at the national level. The growing assertiveness of federal-national governments on matters of service and security threaten to erode the proximity-based arguments in favour of more localized and decentralized forums for public engagement (Gibbons 2004; Roy 2006). While any precise findings about the Spanish case are beyond the scope of this paper, it seems clear that federal government actions in the US are further augmenting the visibility, spending and political relevance of Washington, DC (presumably at the expense of state capitols and local governments). Such is one ironic aspect of the unfolding legacy of President Bush who came to power in 2000 (importantly prior to 9-11) on a Republican-inspired agenda of less government generally and less federal government (reduced in scope and more respective of state jurisdiction) specifically.

In Canada, the US-inspired expansion of the secure state federally – that has built upon federal government efforts to lead in the realm of online service delivery, coupled with the Conservative's hopes for a more devolved and less acrimonious form of federalism (especially in Quebec) do not make for an easy mix. Yet, it must be underlined that the risks of technocracy are greatest at the national (and transnational) level, while the most responsive and innovative forms of governance tend to be nurtured through proximity and participation (Evans 2002; Woodward 2003; Roy 2006). This disconnect is perhaps the greatest challenge to progressive and open governance renewal in a digital age.

REFERENCES

Allen, B.A., Paquet, G., Juillet, L. Roy, J., (2005). E-Government as Collaborative Governance: Structural, Accountability and Cultural Reform. Khosrow-Pour, M., Ed. *Practising E-Government: A Global Perspective* (Ideas Group Publishing) 1-15.

Andal-Ancion, A., Cartwright, P., and Yip, G.S. (2003) The Digital Transformation of Traditional Business. *MIT Sloan Management Review*, Summer 2003.

Archick, K. (2006) *US-EU Cooperation Against Terrorism* (Washington: Library of Congress, Congressional Research Service).

Batini, C., Cappadozzi, E., Mecella, M. and Talamo, M. (2002). "Cooperative Architectures," McIver, W.J. and Elmagarmid, A. K. (Eds.) *Advances in Digital Government – Technology, Human Factors and Policy*. Boston: Kluwer Academic Publishers.

Bellamy, C., Perri, 6, and Raab, C. (2005) Joined Up Government and Privacy in the United Kingdom: Managing Tensions Between Data Protection and Social Policy. Part II. *Public Administration* 83 (2) 395-415.

Bennett, C.J. and Raab, C. (2003). *The Governance of Privacy*. Burlington: Ashgate.

Borins, S. (2004) A Holistic View of Public Sector Information Technology. *Journal of E-Government* 1 (2) 3-29

Burnham, D. (1980) *The Rise of the Computer State* (New York: Random House).

Cairncross, F. (2002) *The Company of the Future*. Cambridge: Harvard Business School Press.

Charih, M. and Robert, J. (2004) *Government Online in the Federal Government of Canada: the Organizational Issues*. International Review of Administrative Sciences 70(2) 373-384.

Clarke, R. (2004) The Internet and democracy. Halligan, J. and Moore, T. (2004) eds. *Future Challenges for e-Government* (Canberra: Government of Australia).

Coe, A. (2004) *Government Online in Canada: Innovation and Accountability in 21st Century Government* (Cambridge: Kennedy School of Government Graduate Research Paper).

Coleman, S. (2003) The Future of the Internet and Democracy Beyond Metaphors, Towards Policy. OECD, *Promise and Problems of E-Democracy: Challenges on Online Citizen Engagement*. Paris: E-Government Project.

Coleman, S. (2006) E-mail, terrorism and the right to privacy. *Ethics and Information Technology* 8: 17-27.

Coleman, S. and Norris, D. (2005) A New Agenda for E-Democracy. *International Journal of Electronic Government Research*, 1(3) 69-82.

Courchene, T.J. (2005) "E-the-people": reflections on citizen power in the information age. *Policy Options* 26 (3) 43-50.

Curtin, G., Sommer, M.H., Vis-Sommer, V. eds. (2003) The World of E-Government. New York: Haworth Press.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45 (1) 67-87.

Dwyer, P. (2004) The rise of transparency networks: a new dynamic for inclusive government. Halligan, J. and Moore, T. (2004) eds. *Future Challenges for e-Government* (Canberra: Government of Australia).

Eggers, W. (2005) *Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock and Enhance Democracy*. New York: Rowman and Littlefield Publishers.

Entwistle, T. and Martin, S. (2005) From Competition to Collaboration in Public Service Delivery: A New Agenda for Research. *Public Administration* (83) 1 pp.233-242).

Evans, K. G. (2002) Virtual Dialogue and Democratic Community. *The Transformative Power of Dialogue* (12) 157-177.

Fountain, J. E. (2001). *Building the Virtual State: Information Technology and Institutional Change*. Washington, D.C.: Brookings Institution Press.

Gasco, M., Roy, J. (2006) E-Government and Multi-Level Governance: A Comparative Examination of Catalonia, Spain and Ontario, Canada. *International Journal of E-Government Research* 2 (4) 57-75.

Geist, M. (2005) The Three Stages of Canadian Privacy Law. http://www.michaelgeist.ca/resc/html_bkup/april112005.html).

Gibbons, R. (2004) "Federalism and the Challenge of Electronic Portals" in Oliver, L. and Sanders, L., Eds. (2004) *E-Government Reconsidered: Renewal of Governance for the Knowledge Age*. Regina: Canadian Plains Research Center.

Goldsmith, S. and Eggers, W.D. (2004) *Governing by Networks – the New Shape of the Public Sector* (Washington: Brookings Institution Press).

Henrich, V. C. and Link, A. N. (2003) Deploying Homeland Security Technology. *Journal of Technology Transfer.* 28. 363-368.

Heymann, P. B. (2001/02) Dealing with Terrorism: An Overview*. International Security*: 26(3). 24-38.

Hodges, S. and McFarlane, D. (2004) RFID: The Concept and the Impact. *The Security Economy.* Paris: Organization for Economic Cooperation and Development.

Holden, S. (2004). *Understanding Electronic Signatures: The Keys to e-Government*. Washington, DC: IBM Center for the Business of Government.

Holmes, A. (2005) Riding the California Privacy Wave. CIO Magazine (Jan 15th: http://www.cio.com/archive/011505/california.html).

Hosein, G. (2005) *Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the US and Europe*. Privacy International (www.privacyinternational.org).

Jaeger, P.T. (2002) Constitutional principles and E-Government: an opinion about possible effects of Federalism and the separation of powers on E-Government policies. *Government Information Quarterly* 19 (2002) 357-368.

Joshi, J. B. D., Ghafoor, A. and Aref, W. G. (2002). Security and Privacy Challenges of A Digital Government. In McIver, W. J. and Elmagarmid, A. K. (Eds.) *Advances in Digital Government – Technology, Human Factors and Policy*. Boston: Kluwer Academic Publishers.

Juillet, L. and Paquet, G. (2002) The Neurotic State. How *Ottawa Spends 2002-2003: The Security After-Math and National Priorities.* Don Mills: Oxford University Press 69-87.

Kamarck, E.C. (2004) Applying 21st-Century Government to the Challenge of Homeland Security. Kamensky, J.M. and Burlin, T. (Eds.) *Collaboration – Using Networks and Partnerships*. IBM Center for The Business of Government: Rowman and Littlefield Publishers Inc.

Kearns, I. (2004) Public Value and Electronic Service Delivery: The UK Experience. Oliver, L. and Sanders, L., Eds. (2004) *E-Government Reconsidered: Renewal of Governance for the Knowledge Age*. Regina: Canadian Plains Research Center.

Kim, S. and Lee, H. (2004) Organizational Factors Affecting Knowledge Sharing Capabilities in E-government: An Empirical Study. Wimmer, M.A. ed. *KMGov 2004, LNAI 3035* (International Federation for International Processing) 281-293.

Kramer, K. and King, J.L. (2005) Information Technology and Administrative Reform: Will E-Government Be Different? *International Journal of Electronic Government Research*, 2 (1) 1-20.

Lane, G. and Roy, J. (2006) Security and Stability on the Electronic Highway: A Collaborative Challenge for Industry and Government. *Optimum Online* 36 (2) 45-54.

Lips, M., Taylor, J., and Organ, J. (2006) Electronic Government: New Forms of Authentication, Citizenship and Governance. Oxford Internet Institute (working paper).

Lyon, D. (2004) Surveillance Technologies: Trends and Social Implications. *The Security Economy.* Paris: Organization for Economic Cooperation and Development.

Meyers, D.W. (2003) Does 'Smarter' Lead to Safer? An Assessment of the US Border Accords with Mexico and Canada*. International Migration* 41 (1) 5-44.

Mitchinson, T. and Ratner, M. (2004) Promoting Transparency through the Electronic Dissemination of Information. Oliver, L. and Sanders, L., Eds. (2004) *E-Government Reconsidered: Renewal of Governance for the Knowledge Age*. Regina: Canadian Plains Research Center.

Oates, B.J. (2003) The Potential Contribution of ICT's To The Political Process. *Electronic Journal of E-Government* 1(1).

OECD (2004) *The Security Economy.* Paris: Organization for Economic Cooperation and Development.

O'Hara, K. (2004) *Trust – From Socrates to Spin* (Cambridge: Icon Books).

O'Harrow, R. (2004) *No Place to Hide*. New York: Free Press.

Oliver, L. and Sanders, L., Eds. (2004) *E-Government Reconsidered: Renewal of Governance for the Knowledge Age*. Regina: Canadian Plains Research Center.

Paquet, G. (2004) There is more to governance than public candelabras: E-governance and Canada's public service. In Oliver, L. and Sanders, L., Eds. (2004) *E-Government Reconsidered: Renewal of Governance for the Knowledge Age*. Regina: Canadian Plains Research Center.

Patton, S. (2005) Sharing Data, Saving Lives*. CIO Magazine* (March 01st, www.cio.com).

Prins, J.E.J., ed. (2001) *Designing E-Government: On the Crossroads of Technological Innovation and Institutional Change* (Hague: Kluwer Law International)

Radl, A. and Chen, Y. (2005) Computer Security in Electronic Government: A State-Local Education Information System. *International Journal of E-Government Research* 1(1).

Reed, B. (2004) Accountability in a shared services world. Halligan, J. and Moore, T. (2004) eds. *Future Challenges for e-Government* (Canberra: Government of Australia).

Reid, J. (2004). Holding Governments Accountable by Strengthening Access to Information Laws and Information Management Practices. In Oliver, L. and Sanders, L., Eds. (2004) *E-Government Reconsidered: Renewal of Governance for the Knowledge Age*. Regina: Canadian Plains Research Center.

Roberts, A.S. (2005) Spin Control and Freedom of Information: Lessons from the United Kingdom and Canada. *Public Administration.* 83 (1) 1-23.

Roy, J. (2005). Services, Security, Transparency and Trust: Government Online or Governance Renewal in Canada? *International Journal of E-Government Research*, 1(1) 48-58.

Roy, J. (2005b) Security, Sovereignty and Continental Interoperability: An Elusive Balance for Canada? *Computers and Social Science Review* 22 (2) 1-17.

Roy, J., 2006, *E-Government in Canada: Transformation for the Digital Age*. Ottawa: University of Ottawa Press.

Scholl, H. (2005). Motives, Strategic Approach, Objectives and Focal Points in E-Government-Induced Change. *International Journal of E-Government Research,* 1(1) 59-78.

Science Council of Canada (1984) *A Workshop on Information Technologies and Personal Privacy in Canada* (Ottawa).

Stowers, G.N.L. (2004) *Measuring The Performance of E-Government*. Washington: IBM Center for The Business of Government.

Strickland, L.S. and Hunt, L. (2005) Technology, privacy and homeland security: New tools, new threats, new public perception. *Journal of American Society for Information Science and Technology* (Special Issue on Intelligence and Security Informatics) 56 (3) 220-235.

Tapscott, D. and Ticoll, D. (2003) *The Naked Corporation – How the Age of Transparency Will Revolutionize Business*. Toronto: Viking Canada.

Torrisi, A. and Mezzanotte, L. (2004) Security Products: Inside the Italian Electronic Identity Card. In OECD (2004) *The Security Economy.* Paris: Organization for Economic Cooperation and Development.

Whitaker, R. (1999) *The End of Privacy. How Total Surveillance is Becoming a Reality*. New York: New Press.

Wilson, W. and Welch, E. (2004) Does E-Government Promote Accountability? A Comparative Analysis of Website Openness and Government Accountability. *Governance: An International Journal of Policy, Administration and Institutions* 17 (2) 275-297.

Woodward, V. (2003) Participation the community work way. International *Journal of Healthcare Technology and Management* 5 (1/2) 3-19.

[i] Among others this definition was deployed by the Government of Mexico in recent years, though its' precise origins are unknown. The author adopted it as the basis for a recent article that developed the framework of the four dimensions discussed in this section (Roy 2005a).

[ii] New blogs are continually being created: one recent survey suggests that perhaps as many as 8 million Americans have one, catering to the more than 30 million online readers in the US alone. In essence, a blog is an online platform for publishing, communicating and discussing that allows 'bloggers' to have their say on any given issue or theme deemed worthy of attention. More recently, 'vloggers' have been added to this virtual spectrum, bringing a video dimension that may offer content ranging from a corporate focus (Microsoft operates a vlog for software designers – attracting 900,000 viewers a month according to BusinessWeek) to the provocative and absurd.

[iii] An exception to this claim could be online voting – which involves an e-government application that does little to alter the representational parameters of electoral processes. Accordingly, however, the vast majority of e-democratic visions put forth go far beyond such incremental change.

[iv] While technical risks are real, perceptions also matter as many proponents of online channels have observed that security risks are also immersed in many daily credit card transactions – such as the giving of a credit card to a server in a restaurant, or telephone purchase orders etc. This mix of technological capacities and social adaptation and acceptance form the context within which multi-channel service strategies must exist for different groups of customers and citizens.

[v] Although marginal, as discussed in the previous section the threats for individuals and individual organizations can nonetheless prove to be real and consequential.

[vi] http://www.cba.ca/en/content/stats/040622-delivery%20channels%202003-leaj.pdf

[vii] Of relevance to security related matters is the bolstered public support for stronger governmental action and the relatively higher levels of trust accorded by the citizenry to law enforcement authorities versus other governmental actors. For instance, a 2003 Statistics Canada survey of 25,000 individuals revealed an 82.1% confidence level (either 'a great deal' or 'quite a lot' in police, in comparison to other groups such as banks (68.1%), major corporations (45.8%) and Parliament (42.8%): Globe and Mail Newspaper, July 07th, 2004. Such themes are returned to and explored more fully in chapter four.

[viii] In the United States, identity theft is reported to be the fastest growing crime in the country, having already harmed nearly 60 million Americans (ibid.). The Better Business Bureau of Canada estimates an annual cost of $2.5 billion to Canadian consumers and the total annual cost to the Canadian economy has been estimated at $5 billion.

[ix] Because biometrics can be used in such a variety of applications, it is very difficult to establish an all-encompassing definition. The most suitable definition of biometrics is: "The automated use of physiology or behavioural characteristics to determine or verify identity" (source – www.biometricgroup.com).

[x] The British Government has introduced legislation to establish a new agency by 2008 that would issue both passports and a national identification card, with the cards being compulsory for all citizens by 2013. The card would feature a biometric chip with an identifier unique for each individual, and its purpose is to facilitate better and more integrated access to government services for citizens, while also enabling authorities to counter identity theft, fraud and domestic security threats. Many European countries already use similar cards and there is general interest and a growing commitment to biometrically enabled forms of identification for both passports and domestic mechanisms in many countries around the world, including the United States and Canada.

[xi] The US federal government had adopted an e-government agenda axed largely on improved service delivery prior to September 2001. However, service transformation projects managed by OMB have had trouble securing even modest funding levels for pilot initiatives over the past several years, whereas the President's proposed 2006 budget calls for $41.1 Billion for the Department of Homeland Security, within which the usage and deployment of information and communication technologies (ICT) features prominently (for budgetary details, see www.dhs.gov).

[xii] Prior to 9/11, the federal government focus on cyber-security was indirect and fragmented across various e-government and e-commerce initiatives. In February 2003, the President tabled the country's first ever 'national strategy to secure cyberspace', elevating the issue within the executive branch in both the White House and the Department of Homeland Security.
[xiii] Indeed, many scholars distinguish between information and knowledge management, underscoring the latter when organizations refine and make use of information to facilitate learning and the pursuit of specific objectives. Accordingly, knowledge management is a useful prism to examine and understand many aspects of defence, intelligence and homeland security (Desouza and Vanapalli 2005). While acknowledging to the distinction and its relevance, this article will not pursue it, referring exclusively to information as all forms of data inside and outside of governments.
[xiv] This estimate was reported by 'GlobalSecurity.org', an American observatory and research group devoted to security, defense and intelligence matters.
[xv] Main findings of an August 2004 Report by the Office of the Inspector General (OIG-04-31). The report underscores the challenges of deploying information technologies in a uniquely large and fluid organizational context (similar concerns have been raised by the Canadian Auditor General with respect to Canadian authorities: see section three). It also noteworthy here that mismanagement and weak comptrollership are charges made regularly by critics of the Pentagon (both inside and outside of Congress), the point being that it is hardly unusual to witness large bureaucracies facing operational difficulties with such huge amounts of dollars (and DHS faces the additional pressures of an accelerated and politically charged formation period).
[xvi] One of the most prominent critics of the Patriot Act has been the American Civil Liberties Union who nonetheless saw fit to restrict their concerns in this manner: "The Patriot Act is a 350-page law that contains about 160 provisions. The ACLU and our ideologically diverse allies inside and outside Congress have zeroed in on fewer than a dozen that we think went too far too fast, that have not been shown to have either been necessary or effective in countering terrorism…Section 213 it turns out, the so-called sneak-and-peek provision, according to the Justice Department itself, has mostly been used for non-terrorism investigations. Section 215, the so-called library records and other tangible records provision, where people are so concerned about having their library records searched secretly without their knowledge, we're told hasn't even been necessary, that libraries are voluntarily turning over information to the government or turning them without... under different authority." (Nadine Strossen, quoted from PBS's The News Hour: http://www.pbs.org/newshour/bb/terrorism/jan-june05/patriot_4-5.html).
[xvii] In 1999, for example, 126,809,769 pages of government information were declassified. By 2004, this number has dropped to 28,413,690. Source – Secrecy Report Card – An Update, April 2005, www.openthegovernment.org).
[xviii] The Globe and Mail Newspaper in Canada reported in March 2005 that at a recent technology convention in Seattle, security experts held a contest inviting hackers to manipulate the search engines, Google and Yahoo, to find confidential information on citizens and organizations. They did just that: using Google for about one hour, contestants gathered information on nearly 25 million people (of potential use for fraudulent activities). In their corporate responses, Google said that their service is "a reflection of the Web. Although we aggregate and organization information published on the Web, we do not control the information itself nor do we control access to it." Yahoo responded in a similar manner: "we continually optimize our Web search to provide users with a comprehensive and relevant experience by indexing content that is part of the public domain." Indeed, there is no evidence suggesting that either company is somehow directly at fault, but the nature of the incident as well as the corporate responses will, for many, reinforce the suspicions O'Harrow and others.
[xix] p.3, eGovernment in Spain, June 2005 (http://ec.europa.eu/idabc/servlets/Doc?id=21024).
[xx] p.15, ibid.
[xxi] Campaigning for re-election (with a new leader), the Conservatives initially blamed Basques separatists. When it became evident that Al- Qeada it proved a huge problem for the Government (and a boost for the opposition that had been behind in polls but would subsequently win the election) in light of Spain's support for the US-led Iraq war.

[xxii] General Franco ruled Spain until his death in 1975. A military coup was launched and failed in 1981.
[xxiii] 'Only 15% of the 2,190 organizations and individuals who contributed to a survey the EU ran during the consultation exercise thought that industry would do a good job of (self-) regulating how firms used RFID tags.' (Source: BBC Online news, 10/27/2006).
[xxiv] Finland's turn at the rotating Presidency of the EU in 2006 features pledges to instil greater openness in European institutions, transparency being an engrained aspect of the Scandinavian political culture.
[xxv] Britain is proceeding with its plans for a new national identification card. Despite delays tied to administrative competencies and some public resistance, public opinion has remained supportive: Labour heir-apparent Gordon Brown has spoken in more hawkish tones than Prime Minister Bair on the service and security imperatives of strong id management. Similarly, Australia is pursuing plans for a new national smart card – voluntary at the outset, but viewed as a crucial enabler to dealing with the public service in the years to come.
[xxvi] In October 2006 US and EU authorities signed a new deal for the sharing of airline passenger information, as the previous one had been struck down by European courts. Since 9-11 more generally, "the EU has made improving law enforcement cooperation with the US a top priority" (p.2, Archick 2006).