Security, Sovereignty and Continental Interoperability: Canada's Elusive Balance

Jeffrey Roy

Social Science Computer Review 2005; 23; 463
DOI: 10.1177/0894439305278890

Security, Sovereignty and Continental Interoperability

Canada's Elusive Balance

JEFFREY ROY
University of Ottawa

In an era of digital government, citizen-centric governance is a central aim—one that is often predicated on more efficient and responsive service owed through digital connectivity. Antiterrorism efforts accentuate this focus, albeit with a very different set of aims. Governments have been quick to establish new antiterrorism and homeland security measures that create new and expanded capacities for gathering, analyzing, and sharing information. In doing so, tensions have arisen with respect to the appropriate scope of governmental action, and the proper mix of secrecy and transparency. Such tensions also extend beyond borders, as North American governance faces new and rising pressures to adapt to a post–September 11, 2001, nexus of security, technology, and democracy. This article argues that the culture of secrecy already prevalent within security authorities is being extended to continentally under the guise of interoperability without sufficient effort to ensure openness and public accountability within and between countries.

Keywords: security; governance; interoperability; digital government; sovereignty; border; terrorism; information; information systems; Canada

> Electronic information systems are live environments in the full organic sense. They alter our feelings and sensibilities, especially when they are not attended to.
>
> —Marshall McLuhan (McLuhan & Firoe, 1968, p. 9)

In an era of digital government, citizen-centric governance is a central aim—one that is often predicated on more efficient and responsive service owed, in large part, to greater digital connectivity internally (i.e., to share information in new manners), and externally (i.e., to gather information and reach out to citizens and stakeholders). Antiterrorism efforts accentuate this focus, albeit with a very different set of aims. Governments have been quick to establish new antiterrorism and homeland security measures that create new and expanded capacities for gathering, analyzing, and sharing information, within governments and across governments and other sectors, notably the private sector.

In doing so, tensions have arisen with respect to the appropriate scope of governmental action, and the proper mix of secrecy and transparency within a security apparatus operating under a unique and delicate balance between autonomy and accountability. Such tensions also extend beyond borders. In Canada, for example, not only is there a set of debates and

AUTHOR'S NOTE: This article was written while on sabbatical at the University of Victoria's School of Public Administration. I am grateful for the support provided by the School and, in particular, the research assistance of In-In Pujiyono and the constructive and helpful input of Professor Evert Lindquist.

Social Science Computer Review, Vol. 23 No. 4, Winter 2005 463-479
DOI: 10.1177/0894439305278890

concerns about public-sector action within the county that closely resembles that of the United States, there is growing awareness about technological and political interdependence on a continental scale. As a result, North American governance faces new and rising pressures to adapt to a post–September 11, 2001, nexus of security, technology, and democracy that carries implications for governance within and across national borders.

Following this introduction, the next section examines the evolving nexus between homeland security efforts and digital infrastructure, and the central themes of information management and identity. The Canadian security response to September 11, 2001, is then reviewed in the third section, drawing parallels and pressures for convergence between Canada and the United States. The fourth section of the article seeks a response to the question of whether Canadians are at risk in light of specific interdependencies between both countries: Three critical events highlight the manner by which Canadians and their authorities are increasingly intertwined with continental realities. The fifth section thus explores current and future prospects for continental relations and governance as they are shaped by tensions between political sovereignty and digital interoperability, as well as the adequacy of Canadian responses to date.

ANTITERRORISM'S DIGITAL INFRASTRUCTURE

Although there are many dimensions and meanings of *security*, we invoke the term here with respect to two, partially distinct areas. First, cybersecurity and online reliability represent important foundational platforms necessary to underpin the sustained expansion of e-commerce, e-government, and all forms of online activity. Second, homeland or domestic security strategies devised to respond to—and proactively thwart—criminal and terrorist threats are based on information management capacities and a widening digital infrastructure to plan, coordinate, and conduct action. Our focus is very much on the latter, albeit with recognition of the close ties between both dimensions.

September 11, 2001, marked a critical turning point. Prior, digital security could arguably have been presented as primarily an extension of e-commerce and e-government in terms of technologically enabled service delivery. Indeed, security remains central as companies and governments devote considerable attention to encryption, information management systems, and related elements that underpin online transactions (Holden, 2004). The overarching aim is to design technical systems and organizational channels to bolster confidence among Internet users while spoiling the intentions of would-be commercial criminals and/or thrill-seeking hackers (Clifford, 2004; Joshi, Ghafoor, & Aref, 2002; Nugent & Raisinghani, 2002). The details of such efforts often remained shielded from widespread political and consumer debate: For most observers and users of digital systems, technical intricacies remained hidden (Bryant & Colledge, 2002; Demchak, 1999). What mattered were outcomes for users such as convenience and/or cost (Hart-Teeter, 2003; Ronchi, 2003).

Since September 11, 2001, the mind-set of many governments has shifted (Barber, 2003; Brenner, 2004; Waugh, 2003). The American fixation on homeland security, for example, denotes an important new face of e-government in terms of resources and priorities (Pavlichev & Garson, 2004).[1] Governments now seek new and expanded antiterrorism measures that are premised on new or expanded capacities for coordinated information sharing, planning, and responding on a government-wide scale (Fitz-gerald, 2004; Henrich & Link, 2003; Roy, 2005b). Interoperability has become a guiding principle: Often viewed in a technical or digital manner (i.e., computers, networks, and databases being able to communicate with one another), in any organizational environment the human and managerial layers to

such connectedness are as complex (Allen, Juillet, Paquet, & Roy, 2001; Allen, Paquet, Juillet, & Roy, 2005; Fountain, 2001; Gill, 2004; Scholl, 2005). Moreover, interoperability across sectors (notably private industry) also becomes important (Dutta & McCrohan, 2002).[2]

Central to this security apparatus are information flows and identities. With respect to information, the challenge is not generating more of it but rather making sense of it (arguably creating knowledge as a result).[3] An example 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 (Sirmakessis, 2004). Cybersecurity and information management systems are crucial to not only gathering and processing information but also safeguarding it against accidental or malicious threats. Such issues are now viewed through a national security lens as the potential for threats against critical infrastructure components that include information databanks, defense operations, and energy and environmental management systems that all rely increasingly on computer systems and connectivity (Denning, 2003).

For public-sector security authorities expanding their digital capacities, there are three sets of factors, each comprising a partially distinct set of risks, uncertainties, and controversy. The first set is the significant financial investments now flowing into 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 US$180 billion by 2008, including all levels of government and the private sector (an amount rivalling the total annual budget of the government of Canada).[4]

Clearly, future spending is subject to numerous uncertainties, not the least of which being the occurrence and scale of any future terrorist attacks. Current spending levels have generally received little political opposition in the shadow of September 11, 2001. However such massive injections of public funds face growing questions about the extent to which managerial, accountability, and oversight capacities are sufficient for such resource injections. Therefore, the second and quite related set of factors is the size and complexity of deployment. Difficulties that plague the U.S. Department of Homeland Security are a case in point: The Department has been unable to fulfill its role in effectively consolidating and coordinating the formation and usage of terrorist watch lists from its various subunits, a deficiency ascribed by officials to an insufficiently developed infrastructure for doing so.[5]

The third set of factors—the most politically contentious—is the appropriate scope of objectives and means by democratically accountable governments. Tensions in the United States between a traditional mind-set of limited government and the post–September 11, 2001, jump in support for an expansion of state activity are thus central in shaping political debate, particularly in the spring of 2005 (when the PATRIOT Act underwent a Congressional review under the guise of a sunset clause). Although the spirit of the Act remains largely supported, specific provisions—notably those pertaining to wiretapping, surveillance, and the so-called library clause have generated scrutiny.[6]

A key issue in such an environment is concern about insufficient openness on the part of public authorities (Reid, 2004). U.S. government watchers, for instance, claim that during the past 4 years, in particular, the culture of secrecy has been reinforced at the expense of transparency and public accountability.[7] Another, related dimension to such concern that secrecy is becoming the norm in security matters—because of, in part, not only covert activity but also the extraordinary level of complexities that permeate an increasingly ubiquitous and invisible infrastructure:

> 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. . . . More than ever before, the details of our lives are no longer our own. (O'Harrow, 2004, p. 300)[8]

Such concerns about surveillance tie information and identity (De Rosa, 2003). To learn anything specific about an individual or group of individuals, there must be reliable identifiers—critical enablers of digital systems (Heymann, 2001/2002). An example is the deployment of biometric tools on passports and other forms of identification.[9] It is important to note, biometric devices not only allow for national authorities to screen incoming visitors but also enable authorities to monitor the movements of their own citizens abroad, provided there is interoperability on a transnational scale (Su et al., 2005).[10] This pressure for more coordinated across borders underscores a key challenge to traditional notions of national sovereignty and power and drives more distributed governance patterns (Bennett & Raab, 2003; Giddens, 2002; Hayden, 2005; Ougaard & Higgott, 2002; Paquet, 1997). A paradox of antiterrorism is the reassertion of national authority in an environment, nonetheless, dependent on transnational governance. Security, mobility, and commerce thus become coevolving agendas in cross-border relations—particularly with neighboring countries (Ferguson & Jones, 2002; Jorgensen & Rosamond, 2002; Salter, 2004).

THE CANADIAN RESPONSE

For Canadians, the tragic impacts of September 11, 2001, were felt first and foremost in terms of the loss of human life—indirectly via American neighbors and more directly through the loss of 24 Canadian citizens. In other ways, responses to the initial attacks also underscored the closeness of the two neighboring countries.[11]

In the days that followed, an additional and hugely significant collateral threat to Canada took shape, albeit one economically oriented. The threat was underscored by two occurrences: First, stories circulating in the American media that at least some of the hijackers entered the United States by way of the Canadian-U.S. border (a theory that would prove unfounded); and second, the seemingly endless line of trucks extending back some 36 kilometers from the Windsor-Detroit border crossing (joining Ontario and Michigan). The first point threatened to expose Canada as a weak link in U.S. security, whereas the second image underscored the economic catastrophe that could result from being cast in this manner.[12]

Accordingly, it is difficult to overstate the sensitivity of Canadian authorities to American views and actions. According to Meyers (2003), the United States forged ahead with the securitization of its borders and "dragged" Canada along with it. In the aftermath of September 11, 2001, plans that had already been under way were fast tracked to create a "smart border" accord of some 30 points to reinforce security while facilitating mobility, a balance facilitated, in large part, through technological innovation, bilateral interoperability, and biometric potential.[13] The government of Canada reinforced this focus with a major financial commitment to border security in late 2001.[14]

Within the country, the legislative centerpiece of Canada's response to September 11, 2001, case with Bill C-36, the country's first official Anti-Terrorism Act, thereby defining terrorism legislatively for the first time and expanding the powers and means of federal authorities to combat such activities.[15] Underwriting this expansion is also an enhanced degree of secrecy in many aspects of law enforcement and legal proceedings, the focus of which has been the subject of much debate in a manner like debates surrounding the U.S. PATRIOT Act (Allman & Barrette, 2004). Complementing this legal extension is wider rec-

ognition of the importance of digital security to underpin organizational interoperability, ensure the resilience and integrity of government information holdings, and also address the risks and realities associated with the transnational scope of terrorist activity (Brown, 2003; Preyer & Bos, 2002). In short, digital security would serve as central tenant in the war on terror (Hart-Teeter, 2004).

As in the United States, however, the technical and organizational capacities of the Canadian government for doing so were quickly shown to be suspect—and greatly in need of overhaul (Kernaghan & Gunraj, 2004; Roy, 2005b). For instance, with respect to information technology (IT) security generally across government, there is evidence of long-time neglect. In a 2002 audit of government IT security, the Auditor General of Canada (2004) reported that little baseline information existed in the state of IT security across government. A follow-up audit in 2004 (Auditor General of Canada, 2005) described progress as "unsatisfactory."[16]

Along with these technical difficulties are challenges to better coordination across government. The Auditor General again concluded that horizontal efforts have fallen short: "gaps and deficiencies point to a requirement to strengthen the management framework of issues that cross agency boundaries, such as information systems, watch lists, and personnel screening" (Auditor General of Canada, 2004, p. 39). In one effort to create an Integrated National Security Assessment Centre in 2003 to "use intelligence from many sources to produce timely analyses and assessment of threats to Canada," the difficulties of establishing a collaborative mechanism overrode the importance of its role (Auditor General of Canada, 2004, p. 39). In a separate study, the Senate Standing Committee of National Security and Defence (2004) reported similar findings—quoting one assessment of what is required—namely, "an unprecedented level of cooperation inside and outside of government" (p. 14).[17]

A holistic response to such problems came in 2004 via Canada's first-ever National Security Policy that featured a more integrated framework: antiterrorism, policing, border control, and cybersecurity are the purview of a single Minister.[18] The U.S. Department of Homeland Security served as inspiration for Canada's Department of Public Safety and Emergency Preparedness Canada (PSEPC):

> (PSEPC) was created to secure the safety of Canadians while maintaining the benefits of an open society. It integrates under one minister the core activities of the previous Department of the Solicitor General, the Office of Critical Infrastructure Protection and Emergency Preparedness, and the National Crime Prevention Center. (n.p.)[19]

Cybersecurity and informational strategies have been greatly bolstered: Indicative of new approaches is the Advance Passenger Information/Passenger Name Record (API/PNR) program is designed "to protect Canadians by helping to identify high-risk, would-be travellers":

> The Canada Border Services Agency (CBSA) is authorized to collect and retain information on travellers and to keep it for customs purposes under section 107.1 of the Customs Act. API is basic data that identifies a traveller and is collected at the time of check-in. (Government of Canada, 2004, n.p.)

While the Canadian government pointed to September 11, 2001, as reason enough for such measures, four important concerns have been presented by critics: (a) infringement on the privacy rights of Canadians, (b) the secrecy surrounding government operations managing such initiatives (and by extension the related information sources), (c) the potential for

"function creep" where information gathered by one part of government for one purpose (in this case antiterrorism) invariably finds its way into other processes tied to other purposes, and (d) the possibility for errors or mishaps because of mismanagement of information and identities in particular.

The interplay of these four sets of concerns has shaped much of the debate. For example, although the first point is partially mitigated by a variety of legislative safeguards addressing privacy concerns—and the independent Privacy Commissioner (reporting to Parliament rather than the Government)—these same Commissioners are often among the most active critics of government action, underscoring problems associated with secrecy, function creep, and identity management (Loukidelis, 2004).[20] The potential for error and mismanagement within the security apparatus is also a prevalent theme of the most recent Auditor General findings (Auditor General of Canada 2005a, 2005b).

U.S. HOMELAND SECURITY: ARE CANADIANS AT RISK?

While concerns have, therefore, arisen within Canada pertaining to the expanded realm of government security actions, equally prominent have been a number of critical events involving American authorities. Three such events are examined here, each of which underscores the growing transnational dimensions of security, politically and digitally: They are the deportation of a Canadian citizen deported from the United States to Syria, concerns about the Privacy Act enabling U.S. authorities to gain access to personal information of Canadians, and shifting documentation requirements for cross-border travel.

Maher Arar is a Syrian-born Canadian citizen who came to Canada in 1987, subsequently earning a master's degree and finding employment as a telecommunications engineer for an Ottawa-based company. In September 2002, returning from a trip to Tunisia on a stop-over in New York, he was detained by U.S. security officials, questioned, and eventually deported from the United States to Jordan and then to Syria where he would be interrogated, imprisoned, and tortured for more than 1 year. On his return to Canada in late 2003, his crusade to shed light on what he alleged to be a groundless campaign against him has resulted in the formation by the Canadian government of an independent public inquiry (or Commission of Inquiry) to examine this affair.[21]

The inquiry has been set up to review the appropriateness of the actions of Canadian officials in the case—and provide recommendations on a new oversight mechanism for the security related actions of the Royal Canadian Mounted Police (RCMP; the federal police service with certain responsibilities pertaining to domestic security). Although the Commission's final report is not expected until late 2005, a substantial amount of work has been undertaken since its formation in February 2004. In regards to the scope of this article, two major and interrelated points stand out from the first year of the Commission's activities: first, the inherent secrecy of national security matters, and second, the inability of the Commission to shed light on the role of American authorities despite their centrality to the case.

The first point has been the focal point of ongoing legal battles between various stakeholders in the camp of Mr. Arar and the government of Canada. On repeated occasions, significant portions of government submissions and testimony have been censored for "national security reasons." Moreover, the government overruled decisions by the judge leading the inquiry—who argued for the release of information to the public (in some cases the government chose to black out portions of the judge's rulings pertaining to the information in question). After prolonged legal disagreements (delaying the proceedings of the inquiry), the main parties came to an agreement in late March 2005 that would seem to significantly relent to the government view by temporarily agreeing to no longer seek public

release of the details in question.[22] Similarly, in the spring of 2005 government lawyers argued that RCMP officers should not be compelled to testify (because of national security provisions), and at least one notable stakeholder involved in the process went so far to suggest that the Inquiry's findings may never be fully released because of the government's "culture of secrecy" strengthened under the guise of security.[23]

The second point reveals the separation between domestic oversight mechanisms and transnational action. It has been widely presumed that the United States deported Mr. Arar based on information provided by Canadian authorities. Indeed, much of the media coverage surrounding this case focused on this possibility—generating a considerable amount of political and public interest about the nature of the bilateral action. U.S. involvement has largely been excluded from the direct purview of the Arar Commission however. Jurisdiction cannot be extended; and although invited to partake in the Inquiry, the United States politely declined.

Ultimately the inquiry may shed some light on the American role as a by-product of investigating the actions of Canadian officials (and the possibility that they cooperated in some manner with their U.S. counterparts). However, it is only because of the sensational nature of this particular case that any such probing is taking place, despite the increasingly regularized practices of information sharing between authorities in both countries (Barry, 2004). The secrecy of such practices—and the more general absence of political oversight on security matters—is an important theme of domestic and continental governance that will be returned to more fully below.

It is, of course, relevant and important that the Arar case unfolded in the aftermath of September 11, 2001. Indeed, the second bilateral episode pertains directly to the U.S. PATRIOT Act and its potential extension into Canada. The issue stems from the outsourcing activities of many governments in Canada (and elsewhere) resulting in functions previously undertaken within the confines of public-sector organizations shifting to external specialists delivering that function via a contractual partnership. Outsourcing typically denotes the transfer of technical and organizational resources (often including personnel) to this external provider and in the realm of digital technologies and constant pressures for modernizing and improving decision making and service delivery capacities, this type of collaborative activity has become engrained into the fabric of organizational life.

In Canada, perhaps no government has been more aggressive of late in pursuing this path than the Province of British Columbia. During the past several years, it has entered into a number of new outsourcing initiatives aimed largely at upgrading the digital infrastructure of the provincial government. Many components of the information management architecture within the province rely increasingly on the direct involvement of the corporate sector. In many cases, companies invariably handle personal data pertaining to citizens of BC.[24]

In 2004, the provincially appointed Privacy Commissioner of BC publicly declared that such information could be at risk of being directly sought by American authorities because of provisions of the PATRIOT Act. The concern stems from the fact that many companies involved in outsourcing activities in the province are, in fact, Canadian subsidiaries of U.S. corporations. Thus, these companies could be obliged in some instances to share their information holdings with U.S. authorities if called on to do so (because of the invocation of the PATRIOT Act for a security-related matter). Despite efforts by government officials at all levels in Canada to downplay the significance of an issue receiving considerable media coverage, it was subsequently revealed that internal efforts on the part of officials in the federal government confirmed the legitimacy of case made by the BC Privacy Commissioner (and as a result, led to a review of federal contracting provisions).

Although legal experts dispute the reach of the PATRIOT Act to play such a role in facilitating information gathering in Canada, the significance of any such "threat" can be mitigated by two complementary vehicles—bolstered legislative and contracting provisions,[25] and a protocol of goodwill to make use of formal bilateral channels for securing such information if and when required (Courtois, 2005). Yet controversies such as the Arar affair may limit the extent to which the Canadian public is prepared to embrace this second avenue of bilateral cooperation as sufficiently reassuring against a highly controversial piece of U.S. legislation generating much scrutiny in both countries.[26]

Despite such bilateral flares, neither the Arar case nor concerns about the PATRIOT Act's reach have quelled cross-border traffic and the desire of companies and citizens from Canada to enter the United States. Along with economic flows of goods and services, nearly two million Canadians visited the State of Florida alone in 2004. This inflow of tourism is estimated to generate more than $1.5 billion in direct tourism spending (Florida's largest inbound source of tourism as well as the highest levels of foreign direct investment).[27] With respect to travel documentation, requirements have typically been minimal, including various government-issued identification cards such as birth certificates or driver's license.

The first barrier erected in the post–September 11, 2001, environment to this relative free flow of individuals affected Canadian-landed immigrants. Beginning in March 2003, landed immigrants in Canada from many countries faced new visa restrictions.[28] In April 2005, the U.S. government announced that by the end of 2007, Canadians entering the United States will require a passport or a likeminded form of "secure identifier."[29] Although the transition period is regarded as a cushion to soften the blow of this important change (in 2002, only one fourth of all Canadians held a valid passport), impacts will be widely felt. It is ironic to note, this latter policy change was announced just weeks after the release of a trilateral North American study (under the auspices of the U.S.-based Council on Foreign Relations) calling for the formation of continental security perimeter and a set of more politically focused institutions to forge the sort of North American "community" that might one day facilitate widened mobility through standardized identification measures, shared policies, and interoperable systems. In sum, heightened tensions between sovereignty and interoperability present themselves.

CONTINENTAL INTEROPERABILITY AND GOVERNANCE QUANDARIES

Security concerns now predominantly shape relations between Canada and the United States (as well as those between United States and Mexico).[30] Moreover, the pursuit of this common security agenda is increasingly informational and digital, and a level of interoperability between authorities must be achieved to facilitate a collective sense of confidence in one another, and a basis for joint action. Yet, as the examples from the previous section underscore, such a path is not without difficulty. From the Canadian perspective, historical concerns about U.S. dependency (and dominance) remain a major political issue, and as a result, *interoperability* is a term often interchanged with *integration* in political debate. Some observers argue that in accordance with this focus the post-September 11, 2001, context is viewed as more about bilateral commerce than domestic safety (Kruger, Mulder, & Korenic, 2004).

For some, wider collaboration therefore requires a continental "community" that embraces many shared interests while respecting national differences and independence (Pastor, 2001, 2004). Pastor's efforts underpin the trilateral vision endorsed by prominent representatives of Canada, the United States, and Mexico and released by the Council of For-

eign Relations (at a time chosen, in part, to coincide with the North American Leaders Summit in Waco, Texas, in March 2005). The trilateral initiative is bold—albeit incrementally so—in proposing to complement more integrative security measures with a new political dialogue and shared economic investment aimed at the collective prosperity of all parts of the continent.[31] Such a vision is predicated, in part, on an optimistic interpretation of public opinion data that suggests sufficient support in all three countries to underpin a more unified continental ethos to complement national affiliations.

Without referring to this blueprint itself, the leaders drew from it in pledging to create a trilateral framework, the Security and Prosperity Partnership for North America. Such a commitment is consistent with the trilateral aspirations of the Mexican president who has been the most aggressive in calling for the pursuit of stronger governance ties in a manner akin to the model of Europe. The significance of the participation of Canada's prime minister in this joint pledge was notably tempered by recent commercial tensions between the two countries (in particular, lumber and beef), and the decision announced just days before the Summit that Canada would not partake in the U.S.-led initiative for ballistic missile defense. Moreover, trilateral relations involving Mexico are far less visible in Canada than bilateral coverage: Mexico and Canada are in some respects separated by a similar fixation with the United States from their own vantage point. While some Canadians may be open to the notion of a Mexican ally in trilateral negotiations—thereby blunting U.S. power to some degree—others take the view that such a third party can only dilute progress that could otherwise be made on a bilateral basis.[32]

Yet nowhere is the absence of a stronger basis for continentalism more apparent than in the United States: Terrorism concerns and homeland security efforts joining an expanded and often contentious U.S. focus around the world limit the room for more politically integrative approaches to North American governance. Moreover, for many elected representatives in federal and state legislatures, differences between southern and northern bilateral agendas merit incremental and distinct responses more than committing to a trilateral community. In short, there is little indication that September 11, 2001, will play a similarly catalytic role toward continental integration as World War II did in kick starting the construction of a more integrationist and unified European agenda. As all proponents of strengthened North American governance acknowledge, comparisons with the European Union (EU) must be sensitive to the unique time durations of each continent (and the near half century since the Treaty of Rome vs. the formation of North American Free Trade Agreement [NAFTA] in 1992), the EU's ever-expanding membership that now stands at 25 (vs. three North American countries), and the United States' unique presence not only continentally but globally as well.

Yet recent evolutions in EU governance and security may be further revealing in two respects. First, early indicators suggest that the e-government project in Europe has done more to assert national-level authority and visibility than any corresponding European dimension (EGovernment Observatory 2002; Roy, 2005a). Second, the recent elevation of security and safety issues within the EU political agenda has exposed the absence of sufficient continental capacities for interoperability and collaboration across member states (Grabbe, 2005; Henderson, 2005; Smith, 2004). The inherent secrecy of this sector—nationally and at the level of the EU—may very well impede stronger European efforts as public mistrust limits the willingness of countries to relinquish resources and responsibilities to this upper governance tier (Shearman & Sussex, 2004). In North America—in the absence of political institutions—it is reasonable to presume that such secrecy would be compounded.

One can expect the United States and Canada to continue down a cooperative path—with the U.S. model of homeland security continuing to serve as an important reference point for Canadian-U.S. relations. For the Canadian government, such a path risks relying on deception or, at best, something less than full candor in publicly asserting independence while privately pursuing interdependence with U.S. authorities wherever practically possible.[33]Moreover, this incremental approach to continental interoperability aligns itself rather well with the already secretive nature of domestic security within each country. The danger of such a path lies in the expanded realm of secrecy across many aspects of public-sector operations pertaining to security that will grow to include a wider set of trans-border provisions; however, the resulting governance apparatus will become insular and unaccountable, provoking either dangerous overextensions of authority or unintended consequences from mismanagement or error.[34]

The Canadian government is not without some understanding of these pressures, particularly, widening calls for more openness and accountability in security matters. Accordingly, a new joint Parliamentary Committee is being established to—for the first time in Canadian history—provide a mechanism of direct political review over the security community.[35] In addition, the government has created a new body, a Cross-Cultural Roundtable, and an external advisory board on national security.

What remains suspect, however, is the extent to which this new political forum can challenge the traditional culture of secrecy surrounding security operations. Although the new Parliamentary Committee is meant to transcend overt partisanship in Canada (with representation from all political parties in Parliament), members will be sworn to secrecy under existing legislative rules severely limiting the public release of information (in many cases, rules have been strengthened under recent antiterrorism legislation). Accordingly, it is unclear the extent to which this new body will serve as a vehicle for expanding public awareness and involvement in security matters—and thus a basis for strengthened accountability. New tensions may also arise in devising workable relationships and a division of duties between the new Parliamentary Committee and other review bodies in place, particularly as all of these actors adjust and adapt to the ongoing and potential changes to the security apparatus.[36]

With respect to continental security, the Arar Commission demonstrated the separateness of Canadian-U.S. authorities and their respective systems of review and oversight[37]—and there is little reason to expect a new Parliamentary structure to have more success in engaging American stakeholders in such a political review mechanism. The deputy prime minister overseeing this new Committee has already stated categorically that information from third parties (including other countries) will only be shared with Parliamentarians with the consent of the providing party (an unlikely prospect in the case of foreign governments and national security matters).

The risks for Canada in this type of setting are many. First, in bilateral (and now trilateral) discussions, the negotiating power of Canadian authorities is likely to be weakened by the backdrop of a public viewed as inherently unaware, suspicious, or even hostile to most options entailing closer and more overt forms of collaborative action. Second, the citizenry, in turn, is likely to become cynical as evidence emerges (most often through errors or contentious incidents exposed in an after-the-fact manner) that demonstrates the pursuit of such collaboration though more backhanded channels. Third, in such an environment, the growing digital component to security efforts will unfold in a largely insular and hidden fashion. In the context of North American relations, this latter point is central: The consequence is that rather than engage in an open dialogue (that would, in turn, help facilitate a basis of public learning to guide future decisions), simplified political debates and the more complex realities of governing face a widening gap.

Illustrative of such risks is the recent foreign policy statement in Canada (released in late April 2005). At one time billed as an important rethinking of Canada's role in the world (and within it, the continent), the initiative became tightly managed by the government of the day, sensitive to its minority status in Parliament and ongoing bilateral sensitivities with the United States. Accordingly, the statement reinforces the familiar rhetoric of close bilateral collaboration with a safeguarding of distinct national interests and outlooks. Although there is acknowledgment of plans to "strengthen coordination of cross-border law enforcement and counterterrorism programs," there is little discussion of either the political or digital mechanisms that are envisioned for doing so. Moreover, the lack of public consultation and the absence of any formal political discussion on its release (along with ongoing coverage of a widening corruption scandal) ensure a minimal impact—reinforcing present contours of secrecy (and by extension for many, indifference) and suspicion (on the part of those already hostile to closer continental ties) shaping continental security matters.

CONCLUSION

The evolution of Canadian security policy during the past few years reveals three major lessons for Canadian democratic governance and Canada's participation in continental governance relations. First, the U.S. reaction to September 11, 2001, has been the predominant factor shaping Canadian policy and governmental structure. Second, the inherently secretive nature of security policy and the national security apparatus is gradually and incrementally being extended to the continental realm. Third, the governing style and structures of Westminster Parliamentary government may well be particularly conducive to reinforcing this second point, limiting the public discourse on current domestic matters and prospective continental choices.

The fact that there is little indication of more formalized continental governance in the short term nonetheless provides some time for reflection. As a result, there may be a short-term opportunity for the new National Security Committee of Parliamentarians to think outside the box with respect to its role in not only reviewing existing national security arrangements but also preparing—in concert with the public at large—the groundwork for future reforms. There are many high-level and important issues that will crowd the work of this new body, issues rooted in fundamental concepts such as freedom, rights, terrorism, and domestic and international law. At the same time, the Committee would be well advised to tackle two themes explicitly and innovatively: the continental dimension to "national security" and the growing prominence of digital technology within and between governments.

In terms of an explicit continental focus, the Committee should seek to forge new and direct political ties between elected officials in Canada, the United States, and Mexico. Although any such mechanism would undoubtedly begin with a limited, consultative role, at the very least the formation of a publicly recognized and regularized vehicle for political dialogue would begin to lay the groundwork to better integrate continental interdependence and trilateral political review. The sketching of a modest agenda for trilateral action and institutional building offered by Pastor (2004), provides—if nothing more—an open and useful starting point for political dialogue and an exchange of views.

With respect to digital technologies, the main challenge is twofold. First, the new National Security Committee must be equipped with the resources and the will to foster expertise in the intricacies of technological and political interoperability and its impacts on a changing organizational security apparatus domestically and continentally (and undoubtedly globally to some degree as well). Not only is this investment crucial to shaping the continental dimension to its work in an appropriate manner, it is also equally central to under-

standing and contributing to national security domestically. Specifically, the Committee should seek to find ways to build on the commitment of the deputy prime minister to lessen the overall culture of secrecy shrouding law enforcement and security activity (despite the discouraging signs emerging from the Arar Inquiry).

This focus is particularly relevant to the emerging governance complexities of domestic and continental security that carry enormous implications for managerial governance and accountability in a restructured public service. The Committee can, for example, provide a tangibly visible and political dimension to the issue of managerial horizontality that permeates national security and information technology efforts in practice but is all but ignored in public (replaced instead, in the former case by an overtly simplistic assigning authority to a single minister for the entire portfolio of agencies, departments, and cross-governmental processes).[38]

The lessening of secrecy also invited an exploration of the potential for greater public involvement in national security matters, via their elected (and in some cases appointed) representatives and in new and more direct fashions. Through traditional public consultations, new intergovernmental partnerships, and online channels of deliberation, the National Security Committee could undertake to serve as a catalyst for a broad and more open dialogue on national security arrangements and their consequences for existing domestic institutions and a complementary and shifting continental agenda—the importance of which is not about to abate any time soon.

NOTES

1. The U.S. federal government had adopted an e-government agenda largely based on improved service delivery prior to September 2001. However, service transformation projects managed by Office of Management and Budget (OMB) have had trouble securing even modest funding levels for pilot initiatives during the past 3 years: In contrast the president's proposed 2006 budget calls for $41.1 billion for the Department of Homeland Security, within information and communications technology (ICT) investments feature prominently (for budgetary details, see `www.dhs.gov`).

2. Prior to September 11, 2001, the federal government focus on cybersecurity was indirect and fragmented. In February 2003, the president tabled the country's first-ever "national strategy to secure cyberspace," elevating the issue with White House–level involvement.

3. 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 defense, intelligence, and homeland security (Desouza & Vanapalli, 2005). While acknowledging to the distinction and its relevance, this article does not pursue it, referring exclusively to information as all forms of processed and unprocessed data inside and outside of governments.

4. This estimate was reported by *GlobalSecurity.org*, an American observatory and research group devoted to security, defense, and intelligence matters.

5. Main findings of an August 2004 report by the Office of the Inspector General (White House, 2004).

6. 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." (Ifill, G. & Strossman, N., 2005, n.p.)

7. In 1999, for example, 126,809,769 pages of government information were declassified. By 2004, this number has dropped to 28,413,690 (*Secrecy Report Card*, 2005).

8. 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 1 hour, contestants gathered information on nearly 25 million people (of potential use for fraudulent activities). In its corporate response, Google said that their service is a reflection of the Web. Google said that although they aggregate and organization the information published on the Web, they do not control the information itself nor control access to it. Indeed, there is no evidence suggesting that either company is somehow directly at fault.

9. The United Kingdom has recently adopted a plan to introduce a new, mandatory identification card, along with biometrically enabled passports. Indeed, pilots are already under way in Scotland, and during the next several years the plan will be complemented by the creation of a National Identification Registry.

10. The International Civil Aviation Organization (`www.icao.int`) is the leading intergovernmental organization examining biometric standards for travel documentation.

11. In the hours following the terrorist attacks, the small town of Gander, Newfoundland (with a population of roughly 11,000), welcomed some 6,000 unexpected travelers from diverted aircrafts—mostly Americans (2 years later, many Americans would return to participate in an organized gathering of goodwill to mark the occasion). One week later, nearly 100,000 Canadians gathered on Parliament Hill in Ottawa (along with the American Ambassador to Canada) to pay homage to the human loss of September 11, 2001.

12. Estimates peg bilateral commercial exchanges across the border in excess of $2 billion per day, with approximately 200 million border crossings each year.

13. From Gerhart and Torok-Apro (2005): The Smart Border agreement generally speaks to the secure flow of people, the secure flow of goods, secure infrastructure, and coordination and information sharing in the pursuit of these objectives.

14. Specifically, in the 2001 federal budget, the government allocated $7.7 billion in new funds during 5 years on a range of initiatives and reforms centered on public security and safety and antiterrorism. One public opinion poll conducted in April 2004 showed rising support among Canadians for higher spending on antiterrorism (55% of those surveyed) and military defense (54%) (Fife, 2004).

15. Bill C-36 adds a definition of *terrorist activity* to the criminal code. The definition will cover an action that is "taken or threatened for political, religious or ideological purposes and threatens the public or national security by killing, seriously harming or endangering a person, causing substantial property damage that is likely to seriously harm people, or in interfering with or disruption an essential service, facility or system" (Government of Canada). The new Bill gives police the power to detain a suspected terrorist for 72 hours without charge, compel Canadians to testify during an investigation, and intercept a wider range of private conversations for a longer period of time. The Bill affects other legislation such as the Income Tax Act. Organizations supporting terrorist groups that claim to be charities can now be stripped of their charitable status. The Bill also allows the government to store the DNA of suspected terrorists, to compile lists of terrorists and their organizations, and to freeze and take away their assets.

16. The focus of this audit included five key areas: cooperation and information-sharing among lead organizations on IT security, development and implementation of IT security standards to support policy, effectiveness of the Government Security Policy and existing security measures, contingency planning, and risk management (Auditor General of Canada, 2004).

17. Indeed, the Senate Committee report went further in underscoring the absence of an intergovernmental architecture for cooperation and the resulting dearth of resources and capacities on the front line (i.e., local level governments and emergency service providers).

18. Information on the various players and initiatives is available at `www.safecanada.ca`. Within the realm of cybersecurity, one new initiative created in February 2005 is the Canadian Cyber-Incident Response Centre (`http://www.ocipep.gc.ca/ccirc/index_e.asp`).

19. The minister is also responsible for a portfolio of six agencies: Canada Border Services Agency, Canada Firearms Centre, Canadian Security Intelligence Service, Correctional Service of Canada, National Parole Board and the Royal Canadian Mounted Policy.

20. The Privacy Commissioner of BC has voiced his concern against surveillance and data-mining efforts, underlining "function creep" as a serious threat (Loukidelis, 2004). He also underscored problems of secrecy and complexity that impede public accountability and the raise the prospect of unintended consequences.

21. Arar's deportation and torture in Syria are not disputed. However, the reasons for this deportation remain unclear because of national security laws limiting the divulging of government documents in public. Arar's camp claims that the basis for his ordeal was groundless—perhaps involving misinformation gathered within public authorities in Canada and then shared with U.S. officials. The Canadian government appointed the Commission of Inquiry to independently examine the actions of Canadian officials and authorities.

22. Specifically, by agreeing to the government's wishes, the government, in turn, withdrew its legal challenge from the Federal Court of Canada to keep the information in question secret (the information pertains to testimony of

various government officials made on camera: The Commission maintained its view that the information should be released and emphasized that it would seek public disclosure at a time and in a manner that would not interfere with the Inquiry proceedings. Details of the agreement, along with all proceedings of the Inquiry may be viewed at www.ararcommission.ca).

23. This comment was made by a former federal cabinet minister, Ron Atkey, acting as amicus curiae (friend of the court) in the inquiry process (reported in the *Globe and Mail* newspaper on May 3, 2005).

24. The issue was triggered by the proposal of the British Columbia (BC) government to contract out the administration of BC's public health insurance program. In the summer of 2003, the BC Ministry of Health put out a request for proposals seeking a private partner to take over the administration of the BC Medical Services Plan (MSP) and Pharmacare. The Province selected Maximus, a private American company with a Canadian subsidiary. The BC Government Employees' Union (BCGEU) then mounted a court challenge to this contracting out. The challenge is a judicial review based on two grounds: (a) an argument that the contracting out contravenes the "public administration" requirement of the Canada Health Act and (b) that the contracting out violates the BC Freedom of Information and Protection of Privacy Act (FOIPPA). The second of these grounds served as the entryway for the BC Privacy Commissioner to examine the case.

25. In October 2004, the BC provincial government formally amended privacy legislation to introduce safeguards such transfers (including stiff financial penalties for violations).

26. Along with domestic media coverage, many Canadian viewers regularly watch cable news channels and public television programming from American broadcasters.

27. The figures are results of a study undertaken by InfoAmericas, a market intelligence, research, and consultancy firm and reported by the Government of Canada (Department of Foreign Affairs, 2005).

28. Countries exempt from this new policy include Australia, Brunei, Ireland, New Zealand, Singapore, and the United Kingdom (and its territories).

29. There appeared to be some confusion over the precise specifications of the new policy, as "passport" was not specified (and the president acknowledged the potential for some flexibility in other options provided security considerations are met). It is important to note, in Canada no other options present themselves, although there are widening discussions of an exploratory nature across both countries about a new form of continental identification interoperable within both countries (although one presumes a Canadian passport would be a likely prerequisite for qualification). Accordingly, the Passport Office in Canada is under growing strain to keep up with demand and balance service and security agendas (Auditor General of Canada, 2005).

30. In 2000, many Mexicans—led by President Fox—hailed the arrival of President Bush as a major turning point: The American president would break with the tradition of making Canada his first official foreign visit, opting for Mexico instead.

31. Canadian representative, John Manley, was formerly deputy prime minister and finance minister and the person who negotiated the Smart Border Accord with then-U.S. Secretary Tom Ridge in the aftermath of September 11, 2001. The trilateral commission made six key recommendations covering—new institutions, a unified border action plan, a common external tariff, an economic stimulus focus for Mexico, a continental energy and national resource strategy, and deepened educational ties.

32. This view was put forth by former Canadian Ambassador to the United States, Allan Gotleib, in his critique of the North American partnership (April 13, 2005, the *Globe and Mail*). He questioned the new initiative's seriousness in light of numerous generalities and shortcomings, notably an absence of central authority in each country assigned with responsibility for moving forward and the refusal of the three leaders to regularize their annual meeting (as a basis for monitoring performance and updating actions).

33. In his first week as Canada's new Ambassador in Washington, Frank McKenna caused a political firestorm in Ottawa by stating that Canada was already a part of ballistic missile defense by virtue of joint North American defense structures (a view categorically denied by the government as during the same week Prime Minister Martin would announce Canada's decision to not partake in the system). Other examples reviewed early—notably the formation of joint border security units—also underscore this point.

34. Within Canada, the auditor general brought to light this danger in her 2005 audit of national security, lamenting her lack of authority over information pertaining to new passenger screening systems installed in airports (the results of the testing of this new equipment were withheld under national security laws protecting such information as sensitive).

35. The mandate of the National Security Committee of Parliamentarians (as proposed in March 2005, subject to legislative adoption) would be to review the security and intelligence apparatus of departments and agencies engaged in security and intelligence activities to fulfill their responsibilities. The Committee would submit reports to the prime minister who, in turn, would table them in Parliament (the prerogative to censor or modify these reports is unclear).

36. Along with the Parliamentary Committee are three existing review bodies: the Security Intelligence Review Committee (an independent body reporting to Parliament on the Canadian Security Intelligence Service), the Communications Security Establishment (CSE) Commissioner (reviewing the CSE), and the Commission for Public Complaints against the RCMP. The latter office, in particular, has been criticized for lacking authority—as it operates within the RCMP (much of the criticism has come from the commissioner herself), and this position is subject to review by the Arar Commission.

37. American Congressional Committees have oversight duties over federal law enforcement and intelligence services (i.e., authority to investigate action, subpoena witnesses, set budgets and structures etc., albeit often in a shared manner with many bodies). Conversely, in Canada, the only political "oversight" is the Minister responsible (who, in turn, must also remain at arm's length from direct involvement) and such, the new Parliamentary Committee is explicitly a "review" mechanism. Such distinctions reflect differences between Canada and U.S. government structures (parliamentary vs. presidential and congressional) in terms of balancing political accountability with the independence of law enforcement officials.

38. The only security-related agency not under the purview of this minister is the Communications Security Establishment (CSE), the national cryptologic agency (providing two key services: foreign signals intelligence in support of defense and foreign policy, and the protection of electronic information and communication). The minister of national defence is accountable to the Cabinet and to Parliament for all of CSE's activities. The minister also provides direction to CSE concerning the performance of its functions. The Minister of National Defence is supported by two deputy ministers. The national security advisor is accountable for CSE's policy and operations. The deputy minister of national defence is accountable for administrative matters pertaining to CSE.

REFERENCES

Ifill, G. (Host), & Strossman, N. (Guest). (2005, April 5). Renewing the PATRIOT Act. *The News Hour.* Available at www.pbs.org/newshour/bb/terrorism/jan-june05/patriot_4-5.html

Allen, B., Juillet, L., Paquet, G., & Roy, J. (2001). E-government in Canada: People, partnerships and prospects. *Government Information Quarterly, 30*(1), 36-47.

Allen, B. A., Paquet, G., Juillet, L., & Roy, J. (2005). E-government and private-public partnerships: Relational challenges and strategic directions. In M. Khosrow-Pour (Ed.), *Practising e-government: A global perspective* (pp. 364-382). Hershey, PA: Ideas Group Publishing.

Allman, W., & Barrette, D. (2004). *Opening submission of the International Civil Liberties Monitoring Group*. Ottawa: Government of Canada.

Auditor General of Canada. (2004). *National security in Canada: The 2001 Anti-Terrorism Initiative*. Ottawa: Government of Canada. Available at www.oag-bvg.gc.ca

Auditor General of Canada. (2005a). *National security in Canada: The 2001 Anti-Terrorism Initiative*. Ottawa: Government of Canada. Available at www.oag-bvg.gc.ca

Auditor General of Canada. (2005b). *Passport services*. Ottawa: Government of Canada. Available at www.oag-bvg.gc.ca

Barber, B. (2003). *Fear's empire: War, terrorism and democracy.* New York: Norton.

Barry, D. (2004). *Managing Canada: US relations in the post-9/11 era—Do we need a big idea?* [Policy Paper on the Americas V XIV (11)]. Washington, DC: Center for Strategic and International Studies.

Bennett, C. J., & Raab, C. (2003). *The governance of privacy.* Burlington, VT: Ashgate.

Brenner, S. W. (2004). U. S. cybercrime laws: Defining offenses. *Information Systems Frontiers*, *6*(2), 115-132.

Brown, M. (Ed.). (2003). *Grave new world: Security challenges in the 21st century.* Washington, DC: Georgetown University Press.

Bryant, A., & Colledge, B. (2002). Trust in electronic commerce business relationships. *Journal of Electronic Commerce Research*, *3*(2), 32-39.

Clifford, M. (2004). *Identifying and exploring security essentials*. Upper Saddle River, NJ: Pearson Prentice Hall.

Courtois, B. (2005, February 11). *The US Patriot Act and the privacy of Canadians*. Speech: Privacy and Security - Synergies in an e-Society Conference, Victoria, Canada. Available at www.itac.ca

Demchak, C. C. (1999). "New security" in cyberspace: Emerging intersection between military and civilian contingencies. *Journal of Contingencies and Crisis Management*, *7*(4), 181-198.

Denning, D. (2003). Information technology and security. In M. Brown (Ed.), *Grave new world: Security challenges in the 21st century* (pp. 47-61). Washington, DC: Georgetown University Press.

Department of Foreign Affairs. (2005). *Travel fact sheets*. Ottawa: Government of Canada. Available at www.dfait-maeci.gc.ca

De Rosa, M. (2003). Privacy in the age of terror. *Washington Quarterly*, *26*(3), 27-41.

Desouza, K., & Vanapalli, G. (2005). Securing knowledge in organizations: lessons from the defense and intelligence sectors. *International Journal of Information Management*, *25*(1), 85-98.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67-87.

EGovernment Observatory (2002). *Survey on egovernment services to enterprises*. Brussels, Belgium: European Commission Enterprise Directorate General.

Ferguson, Y. H., & Jones, R. B. J. (Eds.). (2002). *Political space: Frontiers of change and governance in a globalizing world*. Albany: State University of New York Press.

Fitzgerald, A. M. (2004). *Addressing the security-development nexus: Implications for joined-up government*. Montreal, Canada: Institute for Research on Public Policy.

Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change*. Washington, DC: Brookings Institution Press.

Gerhart, B., & Torok-Apro, R. (2005). *The Canadian passport system: Assessing the interface between technology, security and mobility*. Graduate research paper, University of Victoria, School of Public Administration, Victoria, Canada.

Giddens, A. (2002). *Runaway world: How globalization is reshaping our lives*. London: Profile Books.

Gill, P. (2004). Securing the globe: Intelligence and the post-9-11 shift from "liddism" to "drainism." *Intelligence and National Security*, *19*(3), 467-489.

Government of Canada. (2004). *Advance Passenger Information/Passenger Name Record - Fact sheet)*. Ottawa: Author. Available at `www.cbsa.asfc.gc.ca/newsroom/factsheets/2004/0124pssengere.html`

Grabbe, H. (2005). Conclusion: The politics of freedom, security and justice in the enlarging EU. In K. Henderson (Ed.), *The area of freedom, security and justice in the enlarged Europe* (pp. 161-167). New York: Palgrave Macmillan.

Hart-Teeter. (2003). *The new e-government equation: Ease, engagement, privacy and protection*. Washington, DC: Council for Excellence in Government.

Hart-Teeter. (2004). *From the home front to the front lines: America speaks out about homeland security*. Washington, DC: Council for Excellence in Government.

Hayden, P. (2005). *Cosmopolitan global politics*. Burlington, VT: Ashgate.

Henderson, K. (2005). *The area of freedom, security and justice in the enlarged Europe*. New York: Palgrave Macmillan.

Henrich, V. C., & Link, A. N. (2003). Deploying homeland security technology. *Journal of Technology Transfer*, *28*, 363-368.

Heymann, P. B. (2001/2002). Dealing with terrorism: An overview. *International Security*, *26*(3), 24-38.

Holden, S. (2004). *Understanding electronic signatures: The keys to e-government*. Washington, DC: IBM Center for the Business of Government.

Jorgensen, K. E., & Rosamond, B. (2002). Europe: Regional laboratory for a global polity. In M. Ougaard & R. Higgott (Eds.), *Towards a global polity* (pp. 145-165). London: Routledge.

Joshi, J. B. D., Ghafoor, A., & Aref, W. G. (2002). Security and privacy challenges of a digital government. In W. J. McIver & A. K. Elmagarmid (Eds.), *Advances in digital government: Technology, human factors and policy* (pp. 42-56). Boston: Kluwer Academic.

Kernaghan, K., & Gunraj, J. (2004). Integrating information technology into public administration: Concepts and practical considerations. *Canadian Public Administration*, *47*(4), 525-546.

Kruger, E., Mulder, M., & Korenic, B. (2004, Fall). Canada after 11 September: Measures and "preferred" immigrants. *Mediterranean Quarterly*, 72-87.

Loukidelis, D. (2004). *Identity, privacy, security: Can technology really reconcile them?* [An address by B.C.'s Privacy Commissioner]. Victoria, Canada: Office of the Privacy Commissioner. Available at `www.oipc.bc.ca`

McLuhan, M., & Firoe, Q. (1968). *War and peace in the global village*. New York: McGraw-Hill.

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.

Nugent, J. H., & Raisinghani, M. S. (2002). The information technology and telecommunications security imperative: Important issues and drivers. *Journal of Electronic Commerce Research*, *3*(1), 1-14.

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

Ougaard, M., & Higgott, R. (Eds.). (2002). *Towards a global polity*. London: Routledge.

Paquet, G. (1997). States, communities and markets: The distributed governance scenario. In T. J. Courchene (Ed.), *The nation-state in a global information era: Policy challenges: The Bell Canada Papers in economics and public policy* (pp. 25-46). Kingston, Canada: John Deutsch Institute for the Study of Economic Policy.

Pastor, R. (2001). *Toward A North American community.* Washington, DC: Institute for International Economics.
Pastor, R. (2004, January/February). *North America's second decade*. *Foreign Affairs*. Available at www.foreignaffairs.org
Pavlichev, A., & Garson, G. D. (Eds.). (2004). *Digital government: Principles and best practises*. Hershey, PA: Idea Group Publishing.
Preyer, G., & Bos, M. (Eds.). (2002). *Borderlines in a globalized world*. Dordrecht, The Netherlands: Kluwer Academic.
Reid, J. (2004). Holding governments accountable by strengthening access to information laws and information management practices. In L. Oliver & L. Sanders (Eds.), *E-government reconsidered: Renewal of governance for the knowledge age* (pp. 79-88). Regina: Canadian Plains Research Center.
Ronchi, S. (2003). *The Internet and the customer-supplier relationship*. Aldershot, UK: Ashgate.
Roy, J. (2005a). E-governance and international relations: A consideration of newly emerging capacities in a multi-level world. *Journal of Electronic Commerce*, *6*(1), 44-55.
Roy, J. (2005b). Services, security, transparency and trust: Government online or governance renewal in Canada? *International Journal of E-Government Research*, *1*(1), 48-58.
Salter, M. (2004) Passports, mobility and security: How smart can the border be? *International Studies Perspective*, *5*, 71-91.
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.
Secrecy report card: An update. (2005, April 5). Available at openthegovernment.org
Sirmakessis, S. (2004). *Text mining and its applications.* Heidelberg, Germany: Springer.
Shearman, P., & Sussex, M. (2004). *European security After 9-11*. Aldershot, UK: Ashgate.
Smith, M. (2004). *Europe's foreign and security policy: The institutionalization of cooperation*. Cambridge, UK: Cambridge University Press.
Standing Senate Committee on National Security and Defence. (2004). *National emergencies: Canada's fragile front lines*. Ottawa: Parliament of Canada.
Su, S., Fortes, J., Kasad, T. R., Patil, M., Matsunaga, A., Tsugawa, M., et al. (2005). Transnational information sharing, event notification, rule enforcement and process coordination. *Journal of E-Government Research*, *1*(2), 1-26.
Waugh, W. L. (2003). Terrorism, homeland security and the national emergency management framework. *Public Organization Review*, *3*, 373-385.
White House. (2004). *National strategy to secure cyberspace* (OIG-04-31). Available at www.globalsecurity.org/security/library/policy/national/cyberspace_strategy2003.pdf

Jeffrey Roy is associate professor of the School of Management at the University of Ottawa. He may be contacted at roy@management.uottawa.ca