Security Dilemmas for Canada's New Government

Jeffrey Roy
Dalhousie University, Canada

INTRODUCTION

The context of this article stems from the growing importance of digital technologies within public sector processes and applications tied to the realms of service and security. Both currents continue to influence the public sector and both rely increasingly on digital capacities for information sharing and processing. Yet there are also tensions between them as although both are bound by a more citizen-centric focus, the interpretation and application of this focus is different in each case. Service delivery is predicated on providing information and transactions to citizens in more efficient and integrated ways. Security underpins such service capacities, but it also denotes the usage and deployment of a digital infrastructure to both identify and respond to potential threats. Tensions between service and security have been and continue to be central to managerial and governance reforms associated with digital technologies internally and online connectivity externally.

The Government of Canada is illustrative of the importance of both of these agendas. Over the past decade, Connecting Canadians gave birth to the flagship online service initiative, Government Online (GOL), which has since evolved into the emergence of a new Service Canada entity beginning in the fall of 2005 in order to better integrate and coordinate all delivery channels, including the Internet, telephone, and walk-in, staffed venues. At the same time, the post-9/11 restructuring has resulted in the creation of the Department of Public Safety and Emergency Preparedness Canada and the first overarching national security strategy. Importantly, all of these initiatives are predicated on stronger horizontality within government across previously autonomous units. Such is the challenge of interoperability—meaning the ability to communicate and coordinate action across systems designed for separate and unique purposes.

While interoperability has evolved from a primarily technical challenge to one that is recognized as organizational, the political meaning of interoperability is equally consequential though less recognized and understood. There are new pressures for different levels of government to work with one another more formally and effectively: such pressures extend transnationally, particularly continentally where Canada–U.S. relations have become a predominant framework. Central to this framework is a 'national' security effort that is nonetheless highly intertwined with the Canada–U.S. border and rising pressures for interoperability on a continental scale. Although some elements of 'border management' are explicit (such as the Smart Border Accord), the organizational restructuring and technological retooling of Canadian government is more complex, as is the spectrum of options and choices between independence and sovereignty on the one hand and bilateral (and to a lesser degree trilateral) interdependence on the other. Of particular interest in this article is the prominence of digital technologies in underpinning a culture of information sharing and surveillance both within and across the Canada–U.S. border.

In sum, the objective of this article is thus to better understand:

i. the similarities and differences between service and security in terms of organizational, technological, and political dimensions;
ii the managerial and governance reforms within the public sector driven by the events of 9/11 and the implications for information management and accountability; and
iii. the pressures for cross-border governance arrangements between Canada and the United States.

BACKGROUND: SERVICE AND SECURITY

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 their state, whether it is paying their taxes or renewing permits and licenses of one sort or another (Curtin, Sommer, & Vis-Sommer, 2003). Although the initial impetus for utilizing online channels to deliver information and services was often financial savings through improved automation and efficiency, many such forecasts proved excessively optimistic due to both investment costs and governance complexities (Fountain, 2001; Allen, Paquet, Juillet, & Roy, 2005). Service transformation efforts tied to the Internet began to evolve in the late 1990s, leading to the 1999 pledge to achieve comprehensive online service delivery by 2004:

The Government On-Line Initiative (GOL) was launched to meet this commitment. The goal of GOL is to provide Canadians with electronic access to key federal programs and services. The initiative focuses on grouping or 'clustering' online services around citizens' needs and priorities, rather than by government structures. (Coe, 2004, p. 6)

The government showcases citizen satisfaction surveys with online delivery channels[1] and the results of various surveys such as Accenture's annual rankings as evidence of progress: much of this recognition is owed to the government's main portal[2] that, in the spirit of integrated service delivery, is grouped according to clusters of services and specific client groups.[3] A key objective of GOL had been ensuring that the 130 most common federal services were online by 2005. Although by the end of 2004, nearly all of them were 'identifiable' online, most offerings remain informational, rather than transactional, and the ability to fully complete services and make payment remains more limited. Some current examples include: integrated change of address features, online tax return filing, business registrations, submission of select statements of employment, applying for government employment, and a variety of purchases for government publications.[4] Security is a foundation for such efforts:

Secure Channel is a portfolio of services that forms the foundation of the Government of Canada's Government On-line (GOL) initiative. Secure Channel's primary goals are to provide citizens and businesses with secure, private and high-speed access to all federal government's on-line services, and to provide an environment that enables and encourages departments to integrate with federated common services.[5]

By 2004, the secure channel had been deployed across all federal departments and agencies as the basis of a new government-wide network infrastructure—and it also allowed for the small but growing base of online service offerings summarized above (among other initiatives planned, the secure channel is expected to allow for the first-ever availability of the national census online in 2006). Despite a common platform, leveraging it across traditionally separate entities in order to integrate service offerings is a more complex undertaking. The main barrier is getting departments to work together in sharing information and combining authority in order to realize more 'citizen-centric' processes. The vertical structures of separate departments serving individual ministers largely translate into autonomy over interoperability: "Silos continue to reign" (Coe, 2004, p. 18). Such is the context that drove the creation of Service Canada in 2005, a new government-wide vehicle for integrated service delivery both online and via other delivery channels as well (Roy, 2006b).

CONVENIENCE, COMPLEXITY, AND ACCOUNTABILITY

With respect to service delivery, it is not uncommon to hear project champions both inside and outside of government insist that "the citizen does not care about how governments are organized internally—and how they process information and undertake decisions, their only—or perhaps primary concern is getting good service" (i.e., the end result of a service encounter). Such a viewpoint is analogous in some respects to online, citizen-centric banking where the typical customer accesses his or her entire portfolio of products and services through an integrated portal, caring little