# Identifying Canadians at the Border: ePassports and the 9/11 Legacy

**Brenda McPhail, Christopher Parsons, Karen Louise Smith, Joseph Ferenbok, and Andrew Clement**

> Madam Speaker, I would like to refer the member to page 14 of the throne speech where it says that the government is planning to introduce a new biometric passport that will significantly improve security. . . . Before the government is able to do something like this, it will need to negotiate on a world-wide basis with the organization that deals with and approves the form of passports. If it does not, we will have a biometric passport that will not be able to be read by any country that our citizens visit. I think the government is talking about the biometric being a fingerprint, an iris scan or face recognition. I am really not sure just where it is headed with this . . . [1]
>
> On the new biometric passport, the hon. member is correct. We will need to ensure that it meets international standards. It is very important, of course, for our continuing trade with other countries. We have a lot of people crossing borders and we need to move forward on this. Hopefully, we will do it expeditiously and have those agreements in place so we have mechanisms and means to ensure free trade in our country.[2]

## Introduction

A significant transformation of identification techniques, practices, and policies, particularly as they relate to travel and border crossings, is one of the lasting and widespread surveillance legacies for Canadians as a result of 9/11. The 9/11 Commission Report identified travel documents and border controls as significant elements in terrorist plots: "for terrorists, travel documents are as important as weapons."[3] The report suggests that in the United States, "in the decade before September 11, 2001, border security—encompassing travel, entry, and immigration—was not seen as a national security

1 *House of Commons Debates*, 40th Parl, 3rd Sess, No 7 (11 March 2010) at 1320 (J. Maloway), http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=40&Ses=3&DocId=4342803.

2 Ibid. (S. Coady).

3 National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (2004), 384, http://govinfo.library.unt.edu/911/report/911Report.pdf.

*Canadian Journal of Law and Society / Revue Canadienne Droit et Société*, 2012, Volume 27, no. 3, pp. 341–361.

matter."[4] However, the report estimates that as many as 15 of the 19 hijackers were potentially vulnerable to interception by border authorities, had stricter controls and better intelligence gathering and application methods been in place. Given this report finding, addressing perceived deficiencies in traveller identification and border controls became a paramount matter of national security for the US government.

This has had a series of significant effects on Canadian citizens. The Canada/US border is often touted as the longest undefended border in the world, but since 9/11 this is increasingly viewed in certain political arenas as a source of consternation rather than pride. Until relatively recently Canadians could enter the United States using a variety of common identity documents, such as a driver's license or birth certificate. Since 9/11, however, there has been a "tightening" of border security. One such tightening effort, the US Western Hemisphere Travel Initiative (WHTI), made it mandatory since June 2009 for Canadians travelling to the United States to use a passport or other approved citizenship document at all land borders. Not only have the choices for acceptable identity documents become more constrained, but there has been increasing attention to developing and implementing technologically enhanced document formats that, it is claimed, are more physically secure, that are more difficult to forge or alter, and that facilitate the routine capture of fine-grained information about biometrically identified individuals.

The primary such document is commonly known as the ePassport. The ePassport incorporates a digitally signed, contactless, integrated circuit (IC) chip that includes (among other elements) the bearer's biographic information found in the document and the bearer's biometric image. The microchip allows for wireless exchanges of data during border crossing as well as the ability to visually or automatically authenticate the stored image to the individual presenting the document.[5] A small number of countries were considering ePassports well prior to 9/11, with the first ePassport introduced in 1998 in Malaysia.[6] The International Civil Aviation Organisation (ICAO), the UN agency responsible for the international standardization of travel documents, was also investigating how to incorporate machine-readable biometrics into passports within its Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) following a formal recommendation to do so in 1995.[7] However, after the attack on the Twin Towers, the investigation of, and movement toward, implementing standards for the inclusion of biometrics in passports gained significant momentum. In the new risk-state, the ePassport was placed on the world stage as a technical means to assuage

4 Ibid., 383–84.

5 Passport Canada, "Preparing for Change, Passport Canada Annual Report 2008–2009" (2009), 27, http://publications.gc.ca/collections/collection_2010/maeci-dfait/FR2-1-2009-eng.pdf.

6 Passport Canada, "ePassport Background" (2011), http://www.ppt.gc.ca/eppt/context.aspx?lang=eng.

7 J.M. Stanton, "ICAO and the Biometric RFID Passport: History and Analysis," in *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, ed. C. J. Bennett and D. Lyon (New York: Routledge, 2008), 77–93.

risks and threats. Canada has been involved in the ePassport discourse since before 2003, when Canadian representatives to ICAO helped develop the technical standards for ePassports. Despite Canada's length of interest in ePassports, domestic implementation has been slow; although their adoption was announced by the Passport Office in 2004[8] and again in the 2008 and 2010 Speeches from the Throne, implementation is currently expected to occur in July 2013. However, as the exchange that opens this article demonstrates, as recently as 2010 elected Parliamentarians seemed unaware of Canada's involvement in the past decade's work on ICAO standards. Similarly, Canadian citizens have had relatively little opportunity to learn about the nature of, or potential consequences associated with ePassports. Save for a brief spate of articles in mainstream Canadian media subsequent to the 2004 and 2010 Throne speeches,[9] and more recently when the potential cost of the ePassport caught the media's attention,[10] very little information about ePassports has been actively disseminated to the general public.

While ePassports were undergoing a protracted process of development and implementation in Canada, a series of trade and security bills and agreements were being negotiated and ratified within and between the United States and Canada. These bills and agreements enshrine biometric identification of travellers as a necessary norm. So, for example, in the "Beyond the Border" agreement that was first discussed in 2011, a central point under the heading "Addressing threats early" is a series of commitments related to verifying travellers' identities and developing technical standards to facilitate sharing information, including biometrics, in real time.[11] For the most part these agreements are not legislative but head of state to head of state, and therefore outside of parliamentary review, leaving Canadians to learn, after the fact, of the provisions they contain, and perpetuating the informational asymmetry between citizens and government.

What is the significance of the ePassport for identifying Canadians? Passports function "both practically and symbolically" to ascribe identity and nationality to individuals and are most often used at borders where such information is deeply consequential.[12] This article begins by exploring

---

8 J. Bronskill, "Canada to Introduce Biometric Passport," *CNews*, July 22, 2004, http://www.rense.com/general54/biomet.htm.

9 See, e.g., Bronskill, "Canada to Introduce Biometric Passport"; V. Pilieci, "E-passports Do Little to Stop Terrorists: Expert. Canada to Roll Out New Documents Next Year," *Winnipeg Free Press*, April 4, 2010, http://www.winnipegfreepress.com/canada/e-passports-do-little-to-stop-terrorists-expert-89863777.html.

10 See, e.g., K. Harris, "Fee Hike Questions, Concerns Persist as ePassport Set to Roll in 2012," *iPolitics* (October 24, 2011), http://www.ipolitics.ca/2011/10/24/fee-hike-questions-concerns-persist-as-epassport-set-to-roll-in-2012/; CBC News, "New e-passport Price Tag Could Be Hefty," *CBC News* (September 19, 2011), http://www.cbc.ca/news/canada/story/2011/09/19/passports-cost.html.

11 Stephen Harper, "Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness" (February 4, 2011), http://www.pm.gc.ca/eng/media.asp?id=3938.

12 P. Baudoin, "Review of *The Passport: The History of Man's Most Travelled Document*, by M. Lloyd," *American Archivist* 68, 2 (2005), http://www.archivists.org/periodicals/aa_v68/review-baudoin-aa68_2.asp

the nature of borders and the significance of border crossing as it relates to identification. Next, it examines the ongoing development of the Canadian ePassport and related trade and security agreements; it concludes by proposing practical methods rooted in design and advocacy to raise public awareness about the ePassport specifically, and identification documents and policies more generally. Such awareness can enhance discourse concerning the nature of technology, borders, and identification as it pertains to notions of privacy, dignity, and appropriate modes of policy making. The ePassport is only one manifestation of an increasing reliance on technological mediation in identity transactions, but it is a significant one, linked as it is to individuals' citizenship and mobility rights. We trace its development process in Canada as a means to highlight two trends in identification policy. First, we argue that there is increased asymmetry between governments and citizens; as citizens must reveal more and more information, the processes by which governments choose, develop, and implement new identification technologies are increasingly opaque and secretive. Second, we suggest that this is in part due to the prevailing "identity myth" that positions identification as key to security and safety. We argue that Canadians need to know about, and understand, the changes being made to one of their fundamental citizenship documents and how these changes are taking place, particularly in light of the increasing global significance placed on identification.

## Borders and Bordering

Borders have operated as sites to control the flow of populations between states for centuries. It is only recently, however, that socio-technical and bureaucratic systems "have actually developed the capacities necessary to monopolize the authority to regulate movement."[13] Processes of regulating movement extend beyond the capacities of the state alone: nation-states, corporate vendors, and technical standards bodies collaborate with one another to establish a "card cartel" that is responsible for articulating cardholders' identities.[14] The passport is an "expression of the attempt by modern nation-states to assert their exclusive monopoly over the legal means of movement."[15] As a document, the passport constitutes a particularized socio-technical expression of belonging to a citizenry and degree to which a nation-state enfolds its members.

An identity document, be it for international or national travel, is principally meant to enable "the reliable identification of each member of the

[13] J. Torpey, *The Invention of the Passport: Surveillance, Citizenship, and the State* (Cambridge: Cambridge University Press, 2000), 7.

[14] C.J. Bennett and D. Lyon, eds. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (New York: Routledge, 2008), 11–12.

[15] J. Torpey, *Coming and Going: On the State Monopolization of the Legitimate Means of Movement* (Irvine: University of California, Irvine, Center for the Study of Democracy, 1997), 13, http://escholarship.org/uc/item/2n49r2s3;jsessionid=67BB0DE2AAE2C45D590A13ABB7FF25271.

population to which it is issued."[16] "Identification" should not be read as a fixed or settled claim; contemporary identity systems rely on regularly updated and modified databases, situated perceptions, and ongoing governmental decision making and are thus temporally specific claims of a traveller's identity. Such dynamism demands a focus on the very practices and modes of identification that are responsible for making identity claims possible,[17] which necessitates reflecting on the conditions of the border itself and its associated politics.

The identities of the traveller, as well as key notions of safety and security, are layered in oft-invisible logics that are tied to borders themselves. Borders operate as "overdetermined," or multiply contested, political spaces; they are not mere boundaries between states but instead manifest a world-configuring function by establishing the condition of states, geopolitics, and citizenship itself.[18] In effect, borders are essential to make claims about travellers' legitimacy, normalcy, and capacity to integrate peacefully and successfully across different political spaces—all such concepts are predicated upon, or co-originate with, the concepts of statehood and borders. Borders are also polysemic—expressing multiple, related, but different meanings. This character is demonstrated through their lack of a common international and national meaning that adheres across all members of either domain. One set of meanings may apply for wealthy businessmen—shifts between legal norms, cultural expectations, administrative responsibilities, basic rights—and others for disadvantaged individuals. The disadvantaged are far more likely to perceive the border as "an obstacle which is very difficult to surmount . . . a place he runs up against repeatedly, passing and repassing through it as and when he is expelled or allowed to rejoin his family, so that it becomes, in the end, a place where he *resides*."[19] Further, the border of the early nineteenth century—a site of porous state-guided expressions of identity and power—is complicated today given that the border may actually form well behind its physically demarcated point, within a complex association of international decisions and processes. Their internationalized governance structure, and overdetermined nature, causes the border to be realized as essentially undemocratic: it is an institution that lacks the democratic conditions required for citizens and travellers alike to engage, question, and legitimately revise them save for in the most extreme of circumstances.[20]

---

16 F. Stalder and D. Lyon, "Electronic Identity Cards and Social Classification," in *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, ed. D. Lyon (New York: Routledge, 2003), 83.

17 L. Amoore, "Governing by Identity," in *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, ed. C.J. Bennett and D. Lyon (New York: Routledge, 2008), 22.

18 E. Balibar, *Politics and the Other Scene* (New York: Verso, 2002), 79.

19 Ibid., 83.

20 E. Balibar, "World Borders, Political Borders," in *We, The People of Europe? Reflections on Transnational Citizenship*, ed. E. Balibar (Princeton: Princeton University Press, 2004), 108–9.

The stated aim of bordering processes is to enhance travellers' protection and bodily security by identifying and reacting to risks before such risks manifest as threats or actual harms. Borders, and the identity documents required to "legitimately" engage with them, are thus facets of the growing risk (averse) culture percolating throughout the contemporary configuration of the bureaucratic state. To minimize risks, controls on travellers and citizens are not merely "efficient" but "prefficient," by eliminating problems prior to their suspected emergence.[21] Such efficiencies rely on surveillance and securitization systems that themselves depend on contemporary digital technologies to link the probable, possible, and real prior to a traveller approaching a border's geophysical manifestation. Using these systems, a territorial principle of control is maintained by supervising the terrain of the state and international systems, knowing who are (and are not) residents, and recording the behaviours of resident and transient populations.[22]

In addition to shaping the conditions of felt and perceived state power, borders and the imposition of identity mediate the population's very understandings of being "secure" or "safe" in one's person. From the state's perspective, security and safety at a border mutually depend on the traveller literally giving their physical and data bodies to the state: names and numbers must be given, fingerprints captured, faces photographed, and possibly other biometric information provided to receive and validate documents and travel processes. Such transactions draw the body beyond itself, grafting the flesh to a "digital bitscape"[23] that is used to establish travel identities. The combined, compressed bio-social fact of the traveller trades security and rapidity of travel for absolute subversions of traditional notions of bodily privacy, integrity, dignity, and the conditions necessary to assert one's identity before the state system.[24]

The identities required to pass through borders, no matter how transparent, are often jeopardized with each border crossing. In an era where miscomprehension carries with it typically uncorrectable errors (e.g., membership on the American "no fly" list) or deleterious impacts (e.g., torture or extraordinary rendition to hostile locations), travellers become suspicious of themselves: are they the identity articulated by the state, or has the state misarticulated or misunderstood their identity? In the absence of a democratic governance regime that is accountable to the traveller—nonstate members of the "card cartel" seldom field citizen queries or complaints—the socio-technical travel regimes are hard to question, modify, or receive responses from. It is with considerable concern that we see Canada integrating

---

21 W. Bogard, "Welcome to the Society of Control: The Simulation of Surveillance Revisited," in *The New Politics of Surveillance and Visibility*, ed. K.D. Haggerty and R.V. Ericson (Toronto: University of Toronto Press, 2006), 60.

22 Ibid., 68.

23 I. van der Ploeg, "Biometrics and the Body as Information: Normative Issues of the Socio-technical Coding of the Body," in *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, ed. D. Lyon (New York: Routledge, 2003), 63.

24 Ibid., 70–71.

itself yet further with this cartel by adopting the hyper-technical ePassport regime and continuing to enhance cross-border database integration.

## Passports and Trusted Identification

Although alternative border crossing documents, such as enhanced driver's licenses and trusted traveller cards, exist in some jurisdictions, the most frequently used, and "only universally accepted identification document"[25] for travelling between countries is a passport. A passport as an identifier has two key functions: to provide a reliable or trusted link back to the issuing authority and to authenticate a specific individual within the political body of that authority. The trusted link relies on establishing the authenticity of the document and assumes that the issuing authority has established an individual's entitlement and status as a citizen at the point of enrolment—that due diligence is performed based on reliable foundation documents. Over time a number of security strategies have been incorporated into the passport document to ensure its authenticity. Such strategies are intended to prevent circumvention and counterfeiting and to protect the trusted nature of identity enrollment. They use mechanisms such as: global standardization of the document by governing bodies like the League of Nations (prior to WWII) and ICAO (after WWII), special paper and printing techniques, and difficult to replicate watermarks, emblems, and seals.

The second function of the passport is to authenticate that the enrolled individual is the same person as the one presenting the document at the border. The modern ePassport, in addition to the conventional biographical data, uses biometric representation, a digitized facial image of the enrolled individual, as part of the strategy to link the bearer with the individual enrolled by the trusted authority. Although criticized since their initial inclusion on travel documents,[26] photographs of faces have become the dominant form of identification and remain the principal means for linking a specific real-world body to a particular data record.

The photograph and the passport regime, at least in part, relies on rhetorical slippage between knowing who an individual is (his or her institutional identity) and understanding what that individual may do (his or her intent). Such slippage conflates being identifiable with being trusted and assumes that by knowing who someone is, you know they are "safe," unless there are indications to the contrary in the linked database records. It further rests on the accuracy of the identities that are ascribed to document holders, based on information they have provided and that which the state (and its associates) has added to the holders' autobiographical disclosures. Thus, with ePassports, not only is the individual known at a bio-algorithmic level based on their own self-disclosures, but this violation of a normative privacy barrier is then

[25] Canada Border Services, "Documents for Entry into the United States" (2010), http://www.cbsa-asfc.gc.ca/whti-ivho/tourist-touriste-eng.html

[26] A. Pegler-Gordon, *In Sight of America: Photography and the Development of U.S. Immigration Policy* (Berkeley: University of California Press, 2009).

compounded with the addition of intelligence gathered behind the scenes that contributes to a traveller's state-backed identity profile. There is no accountability for the collection or use of this intelligence, although we occasionally see the results, for example, in cases related to a "no fly" list.

## A Long and Winding Path: From Passport to ePassport in Canada

The Canadian passport has seen relatively few major updates throughout the past half-century, which is one reason why the presently proposed major changes are far from "passport bureaucracy as usual." The current (2011) Canadian passport contains biographical data and a digitally printed photo, and it includes a variety of physical security features. Biographical data is accessible via a machine-readable zone (MRZ) for optical scanning. Passport Canada, created in 1981, is the government agency responsible for issuing Canadian Passports, establishing who is eligible for a passport, and ensuring the rigor of the application process. In 1990, Passport Canada was designated as a Special Operating Agency (SOA) of the Ministry of Foreign Affairs and International Trade; a SOA operates on a cost-recovery model and is intended to provide "greater flexibility and scope to employees and managers. . .to encourage high performance in the delivery of services."[27] Passport Canada's SOA status means that it operates with relatively little Parliamentary oversight beyond an annual report; as a consequence, there is relatively little involvement in decision making about the passport by either elected politicians or the citizens they represent. Instead, as we discuss here, the impetus for changing the Canadian passport format and issuing practices is being driven largely by outside forces, including US security concerns and the requirements of the ICAO standards body (in which the United States plays a formative role).

## International Agreements and Standards

The ePassport path in Canada has been long, low-profile, and firmly entangled in a variety of international initiatives. Just three months after 9/11, the United States moved to tighten its border controls with the *Enhanced Border Security and Visa Entry Reform Act*. As part of this Act (passed in 2002), visa waiver countries were required to implement travel documents with machine-readable biometric identifiers by 2006 or be ineligible to continue in the visa waiver program.[28] The standard chosen in this Act was then under development by ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) working group. Stanton argues "the 2002 passage of this bill provided substantial new impetus to TAG/MRTD's new technologies working group, which held primary responsibility for the development of the biometric component of a machine readable passport."[29] TAG/MRTD

[27] B. Rogers, "Special Operating Agencies: Human Resources Management Issues", Canadian Centre for Management Development, (1996), i, http://publications.gc.ca/collections/Collection/SC94-62-14-1996E.pdf

[28] See generally Stanton, "ICAO and the Biometric RFID Passport."

[29] Ibid., 260.

endorsed facial recognition as the global biometric standard for travel documents in 2002, and they adopted new international passport specifications that establish facial recognition as the standard biometric identifier and require the inclusion of electronic storage technology in May 2003. While Canada is not among the visa waiver countries, the United States pressed Canada to adopt similar measures at the same time.

In the decade since 9/11, there have been three significant agreements between the United States and Canada addressing border issues. The *Canada–US Smart Border Declaration* and 32-point action plan, signed in December 2001, was a bilateral agreement with the United States meant to ensure the "secure flow of people, the secure flow of goods, a secure infrastructure, and the coordination and sharing of information in the enforcement of these objectives."[30] The first point of the action plan focused on biometric identifiers. In March 2005, the Security and Prosperity Partnership (SPP) was initiated between the United States, Canada, and Mexico, with the aim of advancing collaboration between the three countries in a variety of areas, including security. Under the title "North American Smart, Secure Border," the rhetoric of "smart borders" is used to describe a strategy reliant on technology, information sharing, and biometrics.[31] The most recent political agreement regarding border security, "Beyond the Border: A shared vision for perimeter security and economic competitiveness," was issued as a joint declaration by the Prime Minister of Canada and the President of the United States of America on February 4, 2011. This agreement moves toward establishing a common security perimeter, focusing on simplifying travel and trade, increasing information sharing, and further integrating cross-border law enforcement operations. The agreement states a shared commitment to working "together to establish and verify the identities of travelers and conduct screening at the earliest possible opportunity" as well as working toward common technical standards for biometric data processing.[32] In December 2011, the "Perimeter Security and Economic Competitiveness Action Plan" was released. It includes proposals to "implement a systematic and automated biographic information-sharing capability by 2013 and biometric information-sharing capability by 2014 to reduce identity fraud and enhance screening decisions." Although it is not specified, the new Canadian ePassport is the logical tool to provide the biometric information to be shared and used in the context of "enhanced, scenario-based passenger targeting methodology."[33]

---

30 Foreign Affairs and International Trade Canada, "Building a Smart Border for the 21st Century on the Foundation of a North American Zone of Confidence" (2001), http://www.lac-bac.gc.ca/webarchives/20070221041710/http://geo.international.gc.ca/can-am/main/border/smart_border_declaration-en.asp.

31 A. Clement et al., "Toward a National ID Card for Canada?: External Drivers and Internal Complexities," in *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, ed. C.J. Bennett and D. Lyon (New York: Routledge, 2008), 233–50.

32 Harper, "Beyond the Border."

33 Government of Canada, "Perimeter Security and Economic Competitiveness Action Plan" (2011), http://actionplan.gc.ca/grfx/psec-scep/pdfs/bap_report-paf_rapport-eng-dec2011.pdf.

On the international stage, the G8 adopted a *Secure and Facilitated International Travel Initiative* in 2004, in which G8 countries agreed to "Accelerate development of international standards for the interoperability of government-issued smart chip passports and other government-issued identity documents."[34] The standards referred to in the G8 agreement were those developed by ICAO; between 2003 and the present, Passport Canada reports extensive participation in the ICAO's various committees and working groups related to ePassport development. This includes service on the board of the ICAO's Public Key Directory, which provides Canada the opportunity to offer direct feedback on the ePassport security initiative.[35] Passport Canada was also an active member of the Implementation and Capacity Building Working Group (ICBWG), from which the agency helped develop the Working Group's *Guide for Assessing Security of Handling and Issuance of Travel Documents*. The *Guide* includes recommended best practices and a tool for assessing passport issuing processes. There is also a strong Canadian presence on ICAO's New Technologies Working Group, which is chaired by Gary McDonald, the Director General of Legislation and International Relations at Passport Canada. This group develops policies, specifications, and guidance material for the manufacture, security, testing, issuance, deployment, and globally interoperable use of travel documents. It also functions in an advisory capacity to the Technical Advisory Group (TAG), which is responsible for developing specifications for globally interoperable travel documents. Passport Canada is also a member of TAG.

The repeated agreements to pursue border security through biometric identification point to the durability of the vision of "security through identification," which has survived intact through significant leadership change in both countries. Despite evident external pressure, the pace of implementation has been remarkably slow. Beside the formidable technical difficulties in building new, large-scale identification infrastructures, domestic factors have also played a role.

## Domestic (In)Activity and Announcements

The Government of Canada's 2004 National Security Policy moved to implement the security provisions agreed to within the G8 and the Smart Borders agreement, and as required by the American *Enhanced Border Security Act* and the WHTI. Passport Canada was tasked with developing a Canadian ePassport, a document that had to contain biometric data as specified in these multiple agreements. Amendments to the *Canadian Passport Order* were brought into force in September 2004, two of which allowed Passport

[34] Government of Canada, "Canada's G8 Website, Secure and Facilitated International Travel Initiative" (2005), http://www.canadainternational.gc.ca/g8/summit-sommet/2005/travel-voyage_05.aspx?view=d.

[35] See Passport Canada, "Preparing for Change."

Canada to include biometrics in passports.[36] The first gave Passport Canada the authority to convert any information submitted by an applicant into a digital biometric format for insertion into a passport. The second authorized Passport Canada to convert an applicant's photograph into a biometric template to verify the applicant's identity.[37] Also in 2004, the Canadian Passport Order was amended to allow the Minister of Foreign Affairs to refuse or revoke a passport where a person poses a threat to the national security of Canada or the international community. These amendments "provide the foundation for a Passport Canada that takes a strategic view of identity and security issues."[38] This overt positioning of Passport Canada as a key player in a border security strategy is a significant move that marks a visible shift in its role. Passport Canada also undertook an evaluation of concepts and products for facial recognition technology during the 2004/2005 reporting period.

In the 2008 Canadian federal budget, it was announced that Canada would be adopting a "higher security electronic passport" with 10-year validity by 2011—a deadline subsequently extended to 2012, then to 2013.[39] That same year, Passport Canada launched an ePassport pilot project, issuing the first such document in January 2009. The pilot documents were tested and approved by both Canadian and US border agencies as meeting ICAO standards, and more than 4,000 diplomatic and special passports were issued by March of 2009.[40] The commitment to ePassports was repeated in the Speech from the Throne of March 3, 2010, including the "new biometric passport" in a list of promises focusing on "modernizing" security in a variety of areas, ranging from airport screening technologies to developing a cyber-security strategy to protect digital infrastructure.[41]

The path of ePassports in Canada has indeed been long. To clarify the timeline, the key events are summarized in Table 1. Despite the long lead-up to this substantial revision of Canada's universally accepted travel document, there has been very little public attention solicited for, or paid to, this issue. The relatively brief mentions of the ePassport initiative in various Speeches from the Throne and Budget speeches over the past eight years have been Canadians' primary official exposure to the concept of

---

36 "Order Amending the Canadian Passport Order," PC 2004-951, *Canada Gazette Part II*, vol. 138, no. 19 (September 1, 2004), 1, http://www.ppt.gc.ca/publications/pdfs/order_04_113.pdf

37 L. Acharya and T. Kasprzycki, "Biometrics and Government, Industry, Infrastructure and Resources Division," Publication No. 06-30E (Library of Parliament Background Paper, April 16, 2010), http://www.parl.gc.ca/Content/LOP/ResearchPublications/06-30-e.pdf

38 Passport Canada, "Laying a Foundation: Annual Report 2004–2005" (Ottawa: Public Works and Government Services Canada, 2005), http://publications.gc.ca/collections/Collection/FR2-1-2005E.pdf.

39 Government of Canada, "Budget 2008—Budget in Brief" (Ottawa: Department of Finance Canada, 2008), http://www.budget.gc.ca/2008/glance-apercu/brief-bref-eng.html

40 Passport Canada, "Preparing for Change," 27.

41 Government of Canada, "Speech from the Throne" (March 3, 2010), http://www.speech.gc.ca/eng/media.asp?id=1388

**Table 1**
ePassport Timeline

| Year | Event |
|---|---|
| 1998 | Malaysia introduces the first ePassport |
| 2001 | Canada/US *Smart Border Declaration* (December) |
| 2002 | TAG/MRTD endorses facial recognition as the international biometric standard for travel documents |
| 2003 | ICAO adopts passport specifications establishing facial recognition as the biometric standard and requiring electronic storage technology |
| 2004 | Belgium issues first ICAO-compliant ePassport |
| | WHTI passes in the United States, requiring Canadians to present passports at land, sea, and air borders within specified deadlines |
| | G8 adopts the *Secure and Facilitated Travel Initiative* |
| | Passport Canada asked to develop and implement a Canadian ePassport |
| 2005 | *Security and Prosperity Partnership* between the United States, Canada, and Mexico |
| | Negative Auditor's report of Passport Canada resulted in significant organisational restructuring and delayed all projects, including ePassports |
| 2006 | Passport application volume increases 22% in advance of 2007 WHTI deadline, again delaying the ePassport project within Passport Canada |
| 2007 | Homeland Security Appropriations Act extended the WHTI deadline for Canadians crossing land or sea borders to 2009 |
| 2008 | Canadian Federal Budget speech announces ePassports to be introduced in 2011 |
| 2009 | Passport Canada launches ePassport pilot project, using diplomatic and special passports as the test documents |
| 2010 | Commitment to ePassports reiterated in Speech from the Throne |
| 2011 | *Beyond the Border: A shared vision for perimeter security and economic competitiveness* jointly declared by the United States and Canada |
| 2013 | ePassports will be issued to Canadians as of July 1, 2013 |

ePassports, although many border security-related agreements and initiatives have mentioned the key features of ePassports—namely biometric identifiers and chip technology—as essential to speed data reading, speed data sharing, and improve international border security. Canadians could also learn about the ePassport initiative through participation in a public consultation process.

## Consultation Processes

Passport Canada conducted public consultations about ePassports on the issue of the extension of the validity of passports to 10 years (in 2009) and under the requirements of the User Fees Act (in 2010 and 2011). The 2009 consultation consisted of 20 interviews carried out with representatives in the travel industry. Emerging from this consultation, Passport Canada registered support for the 10-year passport, along with questions and concerns about what the

ePassport would entail.[42] The 2010 user fees consultation activities included the objective to "raise awareness about . . . ePassports, and its benefits" and to "seed an informed public dialogue about Passport Canada's business model, products and services"[43] and consisted of three roundtables, an online questionnaire, and the opportunity to provide written submissions. The 2011 follow-up asked for written comments on the "fee-for-service proposal" developed subsequent to the initial consultations. These objectives emphasized the marketing of ePassports and positioned citizens as consumers of services rather than engaged participants in decision making about identification schemes. In terms of the timing of the consultations, it is notable that they occurred *after* ICAO's global standards for ePassports were set and beyond the point at which Canada's government representatives at ICAO could bring the concerns of Canadians forward. In general, the response rate for the two portions of the consultation open to members of the public was quite low.[44]

Notably absent from these consultations was any substantive engagement with the privacy, security, and related civil liberties issues that such large-scale, biometric ID schemes have raised in other jurisdictions, such as recently in the United States (REAL ID) and the United Kingdom (National ID card). There was no proactive provision of materials to help inform Canadian citizens of the potential risks, nor was there invitation to discuss the thorny issues at stake. Potential implications of ePassports include, for example, the likelihood that they may enhance and accelerate data sharing between national and international organisations, expose individuals to identity theft due to data breaches, subject citizens to potentially inaccurate categorizations, and permit or even encourage actuarial modes of risk analysis. When weighed against these potential consequences for privacy and civil liberties, the framing of the consultations was overly narrow. Consultation participants did, however, engage with some of these issues to the extent possible within the confines of the process. From the results published in *What Passport Canada Heard from Canadians: Public Consultation Findings Report*,[45] it is evident that concerns were raised surrounding privacy and the implications of decisions about how information is stored on the passport's microchip. While an initial Privacy Impact assessment was conducted in 2005, a promised update has never been released.

## Areas of Concern

As is evident when tracing the ePassport's development path in Canada, much of the impetus for changing this technology comes from beyond

[42] Phoenix Strategic Perspectives Inc., *Final Report: Passport Canada Consultation on Passport Services: In-Depth Interview Report* (2010), http://www.ppt.gc.ca/publications/consultations/2010-01.aspx?lang=eng.

[43] Government of Canada, "What Passport Canada Heard from Canadians: Public Consultation Findings Report" (2010), http://www.ppt.gc.ca/publications/consultations/1-2010.aspx?lang=eng.

[44] See generally, ibid.

[45] Ibid.

Canada's borders. During the passport's history, there have been numerous discussions and disputes about border security between Canada and the United States, including during the US Civil War and World War II; the tension after 9/11 is merely the most recent iteration of a post-crisis attempt to strengthen borders and secure citizens from the potential dangers lurking beyond. However, the current reactionary focus on securing the borders has gained remarkably widespread acquiescence, to the point that it is virtually inarguable. In 1939, when a Canadian hearse was searched at the American border, people rioted.[46] In 2011, when told that Canadians must carry documents that permit personal information to be recorded on chip technologies that meet questionable security standards, and that information will be shared with the United States where it may be stored and used for any purpose deemed consistent with its original "security purpose," there was a profound lack of outcry. Perhaps this is the result of searches being technologically mediated and thus distanced from individual bodies. While the introduction of body scanners at airports still provokes some opposition—they incite discomfort by focusing on the body itself—ePassports operate less visibly and have yet to generate such dissent. This is troubling given that the "junk" that can be touched, tracked, categorized, and stored in the online world is at least as sensitive, if not as sensational, as that threatened by a body search.[47] The Office of the Privacy Commissioner (OPC) of Canada agrees that this information sharing is potentially problematic. In a recent report addressing privacy issues raised by the "Beyond the Border" agreement, the OPC recommends that "no subsequent agreements should be put in place for information sharing until an enhanced legal framework has been put in place to allow proper oversight and privacy protections and through a concerted public discussion and debate in our respective legislatures."[48]

This is particularly crucial in light of the provisions in the "Beyond the Border" agreement that propose to "establish coordinated entry and exit systems at the common land border" that will "include the exchange of data on all travelers at all automated common land border ports of entry" by 2014.[49] The ePassport is only one small piece of the larger border security puzzle, but it supplies a key element—biometric identification data—that many of the processes seem to be predicated upon. We say "seem" because the actual mechanics of information sharing, including the massive infrastructure to store, annotate, and access citizen data, and the processes

[46] Passport Canada, "History of Passports" (2011), http://www.ppt.gc.ca/pptc/hist.aspx?lang=eng.

[47] K. Zetter, "TSA Investigating 'Don't Touch My Junk' Passenger," *Wired* (November 16, 2010), http://www.wired.com/threatlevel/2010/11/tsa-investigating-passenger/

[48] Office of the Privacy Commissioner (OPC) of Canada, "Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness: Submission by the Office of the Privacy Commissioner of Canada to the Government of Canada's Beyond the Border Working Group Public Consultation" (2011), 15, http://www.priv.gc.ca/information/pub/sub_bs_201106_e.pdf.

[49] See Government of Canada, "Perimeter Security."

around it, are unlikely to be made public. Security infrastructures are always deemed sensitive and their processes cloaked in secrecy, but it is arguable that this trend has accelerated, particularly in North America since the 9/11 attacks. Much of the focus of the investigation after the attacks was on identifying and tracing the terrorists; it was concluded that better tracking of foreign nationals might have prevented the tragedy, and thus subsequent policies, as Hosein notes, "increase the collection of information and surveillance of individuals to an unprecedented level."[50] As citizens become more transparent to governments, the development of security tools and processes becomes ever more opaque, as do their results. This is partially because of sheer technological complexity, but it is also due to deliberate measures taken to shield organisations from view and accountability. Meyer provides one example of this shielding in relation to the "Beyond the Border" agreement when he notes that "if pre-clearance is eventually implemented for passengers, the public will have little to no knowledge of whether the system is working, since approved travelers will not see who is rejected."[51] In addition, as we see in the case of the Canadian ePassport, processes linked to security become increasingly subject to outside influences as nations enact legislation that effectively creates "obligations upon other countries to amend their own laws or otherwise face sanctions."[52]

The ePassport development and implementation process also raises wider issues about Canadian sovereignty and governance. While international travel is greatly facilitated by adopting uniform standards for travel documents (and without an international body such as ICAO it is unlikely that such standards would come to pass), the point remains that the standards-setting process lacks democratic accountability. A handful of elected and non-elected governmental officials, along with small sets of nonstate actors, have been permitted to pursue their own agendas beyond the accountability or transparency provisions that ought to apply between any government and its citizenry. For example, Stanton suggests that the United States pursued a strategy of "transferring the detailed decision making into an international forum that could not as easily be scrutinized as a domestic body"[53] when promoting biometric passport standards at ICAO, a process that has been referred to as "policy laundering."[54] In Canada's development of the ePassport, there has been ongoing participation by key members of Passport Canada at ICAO, but this participation was not made visible to ordinary Canadians, or, for that matter, to parliamentarians. As the opening to this article suggests, MPs were uninformed about Passport Canada's ongoing role in assisting to

---

50 I. Hosein, "Transforming Travel and Border Controls: Checkpoints in the Open Society," *Government Information Quarterly* 22, 4 (2005), 595.

51 C. Meyer, "Pre-clearance Will Be Major Hurdle in Perimeter," *Embassy: Canada's Foreign Policy Newsweekly* (December 14, 2011), http://embassymag.ca/page/view/perimeter-12-14-2011

52 Hosein, "Transforming Travel and Border Controls," 595.

53 Stanton, "ICAO and the Biometric RFID Passport," 265.

54 See generally I. Hosein, "Sources of Laws: Policy Dynamics in a Digital and Terrorized World," *The Information Society* 20, 3 (2004).

develop technology and policy standards around biometric identifiers and travel documents. ICAO itself, as described by Barry Steinhardt of the American Civil Liberties Union (ACLU), has been highly resistant to letting representatives from privacy and civil liberties groups join their process or even attend their meetings "to a degree that would not be possible with a domestic government decision-making body."[55]

The Canadian Government has regularly followed the US lead and bowed to political pressure in the interests of preserving economic and diplomatic ties. Although Canadian participants have played key roles on ICAO committees responsible for standards development, it was the US push for adding biometric technologies shortly after 9/11 that sped ICAO to establish such standards. Further, the invocation of "international standards for document security" becomes a mantra that is at once soothing and unchallengeable. "Everyone else is doing it" probably is not an excuse that gets a child far with her mother, but it seems to carry considerable weight at the international and national levels.

## Points of Resistance

What then can be done at a citizen level to question and resist, or at least to ensure some accountability surrounding, the introduction of the ePassport and other ID schemes that change the relationship between citizens and the state?

We can start by asking what characterizes the problematic identification legacy of 9/11. First, there have been significant changes, and proposed changes, to the identity apparatus designed to verify citizenship and facilitate border crossings for those deemed "safe." These changes are technical (i.e., adding biometrics and radio frequency identification chips to documents such as the enhanced driver's license and ePassport) and organizational/institutional (i.e., new and changed legislation, regulations, and procedures). The public interest or imagination has not been captured by these changes, which have been conducted largely out of public view in incremental steps. Second, through the use of consistent rhetoric, initially designed to play on (and perhaps respond to) the fears dominating public discourse about safety and security right after 9/11, a "new normal" possessing several recurring characteristics has formed. Most fundamental is the emergence of what we may refer to as the "identity myth," or the idea that requiring individuals to identify themselves to authorities through the production of ID documents is effective in addressing security threats. We can see a sign of the widespread acceptance of this need to present ID in the results of a public opinion survey conducted shortly after 9/11. On October 6, 2001, *The Globe and Mail* newspaper reported that 80% of Canadians would submit themselves "to providing fingerprints for a national identity card that would be carried on your person at

[55] B. Steinhardt, "Problem of Policy Laundering" (August 13, 2004), 3, http://26konferencja.giodo.gov.pl/data/resources/SteinhardtB_paper.pdf.

all times to show police or security officials on request."[56] This represented a significant shift in public opinion, which until then had generally been opposed to a national ID card. It appears that many people are willing to subject their own lives to scrutiny, secure in the knowledge that they themselves are of no threat and that an examination of their history will confirm this fact. In exchange, they want everyone else to be subject to this regime, thereby "outing" the dangerous ones.

This depends on some questionable assumptions, most notably that the identification apparatus will function infallibly. In particular, it assumes innocents will not come up as false positives, even though there are prominent examples of false accusation and consequent mistreatment (e.g., Maher Arar). The assumption that those with harmful plans will reveal this in their records is just as faulty. Most of the 9/11 attackers had "clean records" in terms of terrorism threat. Databases only contain records of prior actions, which bear a loose relation to future intent. Once this myth takes hold, and citizens are habituated to requests for identity documents, it will be difficult to reverse. A related characteristic includes shifting the burden of proof away from organizations to demonstrate the need for identification, as is generally required by law when asking for personal information, and onto individuals to ensure that they are successfully identified and therefore "safe." As the onus shifts to individuals, the basic identity model changes from one predicated on credentials of entitlement, such as an authentic, valid passport being sufficient to enter a country, to one based on full identification, in which one's whole biography is potentially interrogated. This form of identification typically requires accessing a database that accumulates information over time and makes personal data and transactional information available for ongoing analysis. The ePassport clearly falls into this model. A third characteristic of the new normal is the rise to dominance of a "security" approach, which treats questioning of identification requests or asking for explanations of rationales as suspicious and threatening to security processes.

Resistance and active pursuit of alternatives could address various facets of this problematic legacy. While addressing these facets in detail is beyond the scope of this article, here are three approaches we have taken in related research:

1. Draw attention to the various shortcomings in the proposed ID schemes, through technical demonstrations, satire, and public exposure of flaws. See, for example, "Playing with Surveillance,"[57] which provides a brief, lighthearted exposure to living with insecure, invasive technologies, in this case those used in the "Enhanced" Driver's Licence.

---

[56] D. Leblanc, "80 Percent Would Back National ID Cards," *Globe and Mail* (October 6, 2001), A1.

[57] See generally K.L. Smith et. al. "Playing with Surveillance: The Design of a Mock RFID-Based Identification Infrastructure for Public Engagement," *Surveillance & Society* 9, 1–2 (2011).

2. Develop practical identification alternatives that people can adopt in an ongoing way. Such alternatives should enable people to gain an experiential understanding of identification approaches based on credentials rather than full identification with links to back-end databases. For example, in the Proportionate-ID Project the research team designed identity card overlays for existing driver's licences and health cards. These overlays enact a data minimization approach and provoke discussions surrounding what information is actually needed for a transaction. We have also developed an Android application that exemplifies this principle for electronic transactions.[58]
3. Assume that the shift to identity-based service provisioning and security is an enduring feature of contemporary life and so bring identification more into a regime of individual rights, organizational transparency, and effective oversight.[59] One strategy to address incursions into the personal identity realm is through more rigorously enforcing, and potentially extending, existing privacy frameworks to examine how subjects are assigned to identity categories. Where privacy frameworks focus generally on information collection and use, a privacy-based framework for the analysis of identity regimes should focus more specifically on decisions made about subjects based on collected information. In particular, attention should be paid to how subjects are assigned to identity categories, as this social sorting is potentially consequential for a subject's immediate transactions and life chances more generally.

## Conclusion

Hosein claims, "What began with a war on terrorism has now transferred to a new security agenda. What began with increasing powers for government agencies to combat terrorism has resulted in the increasing of Government powers generally."[60] We clearly see this trend in changes to identification practices and processes in Canada and beyond since 9/11. Identification is about much more than the state and the citizen. Increasingly, there are outside forces at work, both in the international policy arena, such as the imposition of (negotiated) international standards by bodies such as ICAO, and in the marketplace, as corporate vendors develop advisory relationships with governments and standard-setting bodies. Simultaneously, these same vendors compete to ensure that the multibillion dollar contracts involved in "upgrading" identity documents to meet border requirements are awarded for technologies that they sell. What the political rhetoric of the day makes sound very simple—better ID protects our borders and makes us more

58 See "Prop-ID: Towards a Citizen-Centric System," http://propid.ischool.utoronto.ca.
59 A. Clement, "Toward Identity Integrity Principles," in *Privacy in America: Interdisciplinary Perspectives*, ed. W. Aspray and P. Doty (Lanham, MD: Scarecrow Press, 2011), 85–111.
60 Hosein, "Transforming Travel and Border Controls," 616.

secure—runs into complications on multiple fronts. What is really better and for whom? What does it mean to be secure?

Despite the important role that the ePassport will (rhetorically) assume in improving border security, there is a lack of transparency and public accountability in the technical and policy development processes surrounding it. Technical development projects at Passport Canada, which in turn are based on their prominent participation in key ICAO working groups involved in developing biometric standards for digitized facial images and technical standards for contactless chip technologies, have not been publicized beyond mention in Passport Canada's annual reports. This lack of communication is partly due to the arms-length nature of Passport Canada as a SOA of the government; this status, while demanding annual reporting to Parliament and Canadians, allows the agency to continue development work, in association with ICAO, with very little day-to-day public scrutiny. Indicative of the bureaucratic processes guiding the ePassport, it just took a small amendment to the Order of Council in 2004 to legitimate the ePassport's technical and functional characteristics. This step, unsurprisingly, drew minimal public attention.

Proponents of an ePassport in Canada position it as a minor change involving technological "enhancements" to increase the security of the passport document itself and ensure its integrity. The ostensible goals are to let Canada meet international agreements and obligations, keep pace with other nations, and improve border security. It is reasonable, however, for Canadians to ask about the *actual* security that ePassports provide and whether the goals they permit Canada to achieve are in fact worthwhile or desirable. That discussion is beyond the scope of this article; our argument here is merely that the discussion needs to be held. As Hosein points out, "maybe we must see discourse and deliberation as a good in itself," and "the lack of public discourse was the first and greatest casualty in this new security environment."[61]

Balibar suggests that applying democratic practices to borders would challenge those responsible for establishing modes of border-domination and require accountability to egalitarian democratic principles. This would not necessarily abolish borders but would remodulate the authorities that wield sovereign power.[62] When it comes to the ePassport process, Canadians could do worse than ask their government to return to the democratic principles of accountability or to challenge the recently formed, but already firmly entrenched, new normal of security. After all, as Bruce Schneier has written, "Security is not about technology. It's about risks and different ways to manage those risks . . . Good security systems usually involve technology and people working together, but the people have to run the technology, not vice versa."[63] If security is about risks, then it behooves us to ask what

---

61 Hosein, "Transforming Travel and Border Controls," 620.
62 Balibar, *Politics and the Other Scene*, 84–85.
63 B. Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus, 2003), 146.

risks we address by altering the Canadian passport and the infrastructures that support it and, concurrently, if we introduce new risks with the change. While significant democratic debate has not occurred to date, on June 13, 2011, the Department of Foreign Affairs and International trade announced that ePassports will be delayed once again, with a new launch date of July 2013. There is still time for the government to support rigorous democratic debate and test the legitimacy of Passport Canada's decisions over the past decade, and such debate is critical because, as Webb has stated, "it is through understanding what is really at risk, that we best guarantee our safety and freedom."[64]

**Abstract**

A lasting surveillance legacy that Canadians experience post-9/11 is the transformation of identification techniques, practices, and policies, particularly those associated with travel and border crossing. Ongoing securitization of ID documents, by way of adding radio frequency identification tags, facial recognition, and other biometric techniques, has been accompanied by a rhetoric that equates knowing individuals with knowing whether they represent a threat. This logic of threat analysis and identity management makes individuals responsible for proving they are "safe," while simultaneously marginalizing civil liberties concerns accompanying (potentially) intrusive new forms of identification and surveillance. This article examines the 9/11 ID legacy in relation to the hesitant, but ongoing, development of the Canadian ePassport. Building on Clement et al. (2008), we trace the main drivers of Canadian policies and associated implementation initiatives. These include international policy laundering of standards for the biometric ePassport through the International Civil Aviation Agency, as well as policy actions that are more specific to Canada/US relations and linked to border-related security agreements over the past decade. We argue that the lack of transparency and public accountability in technical and policy development processes and weak resistance from individuals and civil society organisations have led to increased information asymmetry between Canadian citizens and their government.

**Keywords:** identification, borders, surveillance, ePassports

**Résumé**

Suite aux évènements du 11 septembre 2001, un legs durable de la surveillance sur les Canadiens est la transformation des techniques, des pratiques et des politiques d'identification, notamment celles associées au voyage et au passage des frontières. La sécurisation actuelle des documents d'identification, soit par l'ajout d'une étiquette d'identification par radiofréquence, d'une reconnaissance faciale ou d'autres techniques biométriques, a été accompagnée par une rhétorique selon laquelle connaître des individus est équivalent à savoir s'ils représentent un risque. Cette logique de l'analyse des risques et de la gestion de l'identité fait en sorte que les individus

[64] Maureen Webb, *Illusions of Security Global Surveillance and Democracy in the Post-9/11 World* (San Francisco: City Lights, 2007), 8.

sont responsables de prouver qu'ils sont sans risque, en plus de marginaliser les libertés civiles par l'introduction attentatoire (potentielle) de nouvelles formes d'identification et de surveillance. Examinant le legs des documents d'identification à la suite des évènements du 11 septembre 2001, cet article se penche sur le développement lent, quoique continu, du passeport électronique canadien. En s'appuyant sur Clement et al (2008), les auteurs identifient les principaux moteurs des politiques canadiennes ainsi que des initiatives de mise en œuvre. Parmi ceux-ci, on compte notamment le blanchiment des politiques internationales sur les normes biométriques du passeport électronique à l'aide de l'Organisation de l'aviation civile internationale, ainsi que les mesures liées aux ententes en matière de sécurité aux frontières entre le Canada et les États-Unis au cours de la dernière décennie. Selon les auteurs, le manque de transparence et de responsabilité publique relatif aux développements des politiques et des processus technologiques ainsi que la faible résistance des individus et des organisations civiles ont entraîné une asymétrie accrue de l'information entres les citoyens canadiens et le gouvernement.

**Mot clés :** identification, frontières, surveillance, passeport électronique

Brenda McPhail
Faculty of Information, University of Toronto
140 St. George Street
Toronto, ON M5S 3G6
brenda.mcphail@utoronto.ca

Christopher Parsons
Department of Political Science, University of Victoria
3800 Finnerty Road
Victoria, BC V8P 5C2

Karen Louise Smith
Faculty of Information, University of Toronto
140 St. George Street
Toronto, ON M5S 3G6

Joseph Ferenbok
Faculty of Information, University of Toronto
140 St. George Street
Toronto, ON M5S 3G6

Andrew Clement
Faculty of Information, University of Toronto
140 St. George Street
Toronto, ON M5S 3G6