Woodrow Wilson International Center for Scholars

ONE ISSUE TWO VOICES

PRIVACY AND INFORMATION SHARING: **The Search for an Intelligent Border**

MARY ELLEN CALLAHAN + WESLEY WARK

ISSUE 13 OCTOBER 10

1

2

INTRODUCTION Since the Al Qaeda strikes on September 11, 2001, a major priority in United States–Canada relations has been the security of their long common border. In the intervening years, both countries have implemented new laws—the *USA Patriot Act* and the *Canadian Anti-terrorism Act*—and initial problems in ensuring the secure flow of people and trade goods have been addressed. The one area where Canada and the United States have reacted differently, and where greater cooperation is needed to avoid further conflict, is on the vital issue of intelligence sharing and privacy.

The United States has been the pioneer in privacy legislation and in efforts to provide for transparency in government operations. In her essay, Mary Ellen Callahan, the chief privacy officer of the U.S. Department of Homeland Security, sets out the privacy framework for information sharing and shows how the department is mandated to involve its Privacy Office in making

all its policies and programs before they are launched. As DHS Secretary Janet Napolitano explained, "We need to protect both our national security and our national values" of the individual's right to privacy.

Wesley Wark, a professor in the Munk School of Global Affairs at the University of Toronto, agrees that information sharing between the two countries is essential today but admits that Canada's privacy commissioner is not seen as a "key stakeholder" in discussions about national security issues in Canada. Rather, the commissioner acts as an advocate for the privacy rights of Canadians.

The key question, Wark argues, is whether the United States and other partner nations such as Canada can meet the challenges of privacy protection in a 21st-century environment. As the volume of electronic information increases and the capacity for storage expands, there is a relentless erosion of privacy. National security agencies exploit the global information infrastructure to acquire intelligence, major commercial entities build customer databases to manage their business, and millions of people post their personal profiles online. The very concept of privacy is in dispute.

In such an environment, the traditional balance in all democratic societies between the protection of individual privacy and the demands for personal information for reasons of national security can easily break down. Despite the creation of privacy offices, privacy frameworks, and privacy commissioners, bureaucratic routines can soon dull genuine mediation efforts, and citizens lose interest in the process. The best check on abuse, Wark suggests, is for governments on both sides of the Canada–United States border to take the lead in forging a security/privacy culture that has the full support and attention of the people.

The Canada Institute thanks the authors for their critical and insightful analyses of a complex issue in the ongoing bilateral dialogue. We would like to express our gratitude to *Maclean's* magazine for sponsoring this thirteenth issue of *One Issue Two Voices*. We would also like to recognize the late C. Warren Goldring and AGF Management for their initial support of this series.

STEPHANIE McLUHAN
Program Consultant (Toronto)
Canada Institute
October 2010

Cover Image: A sign at a Transportation Security Administration (TSA) checkpoint instructs passengers about the use of the full-body scanner at O'Hare International Airport in Chicago, Illinois. The Backscatter Advanced Imaging Technology scanners were scheduled to be put into use at the airport on March 15, 2010. Twenty U.S. airports are now using full-body scanners.

Mary Ellen Callahan

THE PRIVACY FRAMEWORK FOR INFORMATION SHARING IN SECURITY AND BORDER MANAGEMENT: A U.S. PERSPECTIVE

President Obama stated clearly in his inaugural address, "We reject as false the choice between our safety and our ideals."[1] As chief privacy officer of the U.S. Department of Homeland Security (DHS), the government's largest privacy office, I am charged with implementing and overseeing compliance with U.S. law and DHS privacy policy for all policies and programs emanating from the department. The United States and Canada share many of the same border security issues. We also share many of the same privacy principles and best practices for the protection of personal information. Although our countries have different systems to protect personal data, ultimately both systems provide individuals with effective protection when law enforcement authorities handle such information.

"PRIVACY" IN THE UNITED STATES

In the United States, "privacy" can mean many things, including privacy of person or home. However, with the growth of technology and increasing demands for the government to provide security, privacy is now most often discussed in the context of data privacy. In other regions of the world, it is termed "data protection."

The concept of privacy is embedded in our constitution, laws, policies, and international commitments. As an individual right, it is rigorously applied and enforced by our government's system of checks and balances. The concept of privacy was among the first rights provided by the U.S. Constitution's Bill of Rights. Our Fourth Amendment prohibits the government from conducting unreasonable searches, arrests, and seizures of property and people and requires that all warrants issued for searches and seizures are based on "probable cause."[2]

In addition to this constitutional guarantee, Congress adopted the *Privacy Act*, the first national privacy act, in 1974. With regard to the systems of records maintained by federal agencies, this Act established a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information (PII) about individuals. These fair information practice principles (FIPPs) are internationally recognized, having been articulated and echoed in the Organization for Economic Cooperation and Development (OECD) Guidelines, the European Union Directive 95/46/EC, and the Asia Pacific Economic Cooperation (APEC) Privacy Framework. Even though there are differences in emphasis, interpretation, and implementation, the fair information principles defined in these guidelines are generally the same.

At DHS, privacy law and policy is implemented and enforced through the Privacy Office—the first statutorily mandated privacy office at any U.S. federal agency. Its mission is to protect privacy, particularly an individual's personal information and dignity, while serving the DHS mission to secure America. My authority as chief privacy officer requires me to:

- assure that new technologies do not erode privacy;
- assure that personal information in *Privacy Act* Systems of Records is handled in compliance with the fair information principles as set out in the Act;

At DHS, privacy law and policy is implemented and enforced through the Privacy Office—the first statutorily mandated privacy office at any U.S. federal agency. Its mission is to protect privacy, particularly an individual's personal information and dignity, while serving the DHS mission to secure America.

A Transportation Security Administration (TSA) volunteer demonstrates a full-body (Backscatter Advanced Imaging Technology) scanner at O'Hare International Airport in Chicago, Illinois.

- evaluate new legislation on personal information;
- report to Congress; and
- coordinate with the DHS Office for Civil Rights and Civil Liberties on all of the above.[3]

TRANSPARENCY IN THE U.S. PUBLIC SECTOR

Transparency is the foundation for DHS privacy practices. Perhaps no other agency provides as much notice to the world on its privacy systems. All DHS systems, including those that contain border-crossing data, airline passenger name records (PNR) or other passenger data, trusted traveler programs, or any other system that collects personally identifiable information, are subject to the oversight of the chief privacy officer and the requirements of U.S. data privacy laws.

In April 2010 Secretary Janet Napolitano addressed a regional aviation security conference and confirmed that transparency and respect for privacy are fundamental values of all democracies. She noted that all countries have unique legal traditions, cultural differences, and political realities, but any differences should not hinder us from working toward a common goal and even stronger partnership with respect to security and privacy.[4] Simply put, understanding each others' similarities and differences makes for stronger partnerships.

The U.S. statutory framework for protecting privacy in the public sector includes the following laws:

- The *Privacy Act of 1974* governs the handling of personally identifiable information and requires every government system that collects such information to publish a system of records notice (SORN) outlining the authority and reason for collection and the allowable uses of that information.[5]
- The *E-Government Act of 2002* requires that privacy impact assessments (PIAs) be performed for new systems and updated as necessary when a system change creates new potential privacy risks.
- The *Freedom of Information Act* (1966) (also known as *FOIA*) provides the right for anyone, regardless of citizenship or location, to request access to federal agency records and information.
- The *Homeland Security Act of 2002* created the position of chief privacy officer within DHS, with responsibilities to ensure that privacy and transparency are implemented.
- The *Implementing Recommendations of the 9/11 Commission Act of 2007* requires that federal agencies appoint a senior official for privacy matters[6] and amends the *Homeland Security Act* to give new investigative, training, and reporting authorities to the chief privacy officer.

Transparency is the foundation for DHS privacy practices. Perhaps no other agency provides as much notice to the world on its privacy systems. All DHS systems are subject to the oversight of the chief privacy officer and the requirements of U.S. data privacy laws.

Additional laws provide that the government must access and use personally identifiable information only for lawful and proper purposes. Multiple privacy-related laws allow individuals, regardless of citizenship or location, to seek redress for misuse of such information. These laws include the:

- *Computer Fraud and Abuse Act* (1984)
- *Electronic Communications Privacy Act* (1986)
- *Federal Information Security Management Act* (2002)[7]

In addition to these acts, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act) established the DHS Traveler Redress Inquiry Program (DHS TRIP) and authorized judicial review of Transportation Security Administration (TSA) Orders.[8]

Privacy Act

This Act provides for transparency throughout the entire governmental process—from the inception of the proposed database through its implementation and data retention. Its purpose is to balance the government's need to maintain information about individuals with individuals' right to be protected from unwarranted invasions of their privacy. The Act's objectives include restricting disclosure of personally identifiable information maintained by agencies; granting individuals[9] a right of access to and amendment of records; establishing a "code of fair information practices" that regulates the collection, maintenance, use, and dissemination of such information; and granting private rights of action against agencies for violations of the Act.

The origins of the *Privacy Act* lie in the government's need to access additional personally identifiable information to implement social programs and provide citizens with benefits. Just as Congress began to address privacy concerns and to draft legislation to ensure proper use of this information, the Watergate scandal and other abuses revealed examples of improper government surveillance. The *Privacy Act* was groundbreaking in that it imposed new obligations on the U.S. government in its handling of information concerning individuals. It was the first national law related to privacy and government use of data, and it was based on groundbreaking work by the U.S. Department of Health, Education and Welfare.[10] Many of the fair information practice principles in the *Privacy Act* and in multinational frameworks were derived from that seminal work.

The establishment of the fair information practice principles in the *Privacy Act* reduced the unnecessary collection of private information by the federal government, prevented improper disclosure of such information, and gave individuals tools to determine what information the government held about them and how to correct errors in the records. By requiring U.S. agencies to justify their collection of personally identifiable information, the Act effectively limited collection to "relevant and necessary" information needed by the agency to accomplish a particular purpose required either by statute or by executive order of the president.[11]

The *Privacy Act* also requires each agency to publish a system of records notice in the *Federal Register*, the official journal of the U.S. government that contains most routine publications and public notices of government agencies.[12] This notice must describe, among other things, the purpose of the collection, the rules for third-party information sharing, the categories of records collected and the individuals covered, the rules for record retention and destruction, and the way records are retrieved within the system. Such notices must be published before the agency begins to operate the system, allowing for comments from the public and providing for increased transparency. Any person who is interested in what systems of records are kept by DHS may access these notices on the DHS Privacy Office website.[13]

E-Government Act

Recognizing that improvements in technology were also changing how the government managed personally identifiable information, the U.S. Congress passed the *E-Government Act* in 2002. Its objective was to institutionalize more privacy protections by requiring that these protections be built into new electronic and existing paper-based programs and systems. The Act ensures "sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic government." It requires agencies to conduct, update, and post privacy impact assessments (PIAs) before they develop or procure information technology systems that could have an impact on individuals' privacy. In addition to requiring that privacy protections be built into all new programs and systems, the Act emphasizes that these assessments must be posted publicly, thereby providing an additional layer of transparency and accountability.

In 2004 the DHS Privacy Office wrote comprehensive guidelines on conducting a privacy impact assessment to assist its component agencies in creating transparency and establishing public trust in our operations—including DHS components such as U.S. Customs and Border Protection and the Transportation Security Administration. By documenting the procedures and measures through which it protects the privacy of individuals, DHS can better carry out its mission.[14] In its most basic form, a privacy impact assessment is an analysis of how personally identifiable information is collected, used, disseminated, and maintained. It is a vital tool that evaluates possible privacy risks and the mitigation of those risks both at the beginning and throughout the development of a program or system. The transparency and analysis of privacy issues provided by such an assessment demonstrate that DHS actively engages program managers and system owners on the mitigation of potential privacy risks.

Transparency is not the sole purpose of privacy impact assessments. They result from a lengthy process of engagement among the Privacy Office and various DHS programs, offices, and system owners. They also show ongoing compliance with the privacy requirements placed on DHS by Congress, the Office of Management and Budget (OMB), and the public at large. Programs comply with the requirements not just because it is the right thing to do but because there are budgetary consequences to noncompliance. As part of the annual budget process, the Privacy Office reviews DHS programs. These reviews can place programs on hold until their assessments are completed and before they are submitted to Congress or to the Office of Management and Budget. DHS programs have been canceled or suspended because they did not meet the rigorous requirements of the privacy compliance process. This review and coordination between chief information officers and chief privacy officers demonstrates that privacy protections are key foundational elements to information security in U.S. federal agencies. Such cooperation (including the public disclosure of privacy protections) allows chief privacy officers to leverage their authority to ensure that federal programs consider the full impact of privacy concerns.[15]

Freedom of Information Act

The *Privacy Act* strives for transparency throughout a program's lifecycle, and the *Freedom of Information Act* provides an additional layer of transparency. It allows for the full or partial disclosure of previously unreleased information and documents controlled by the U.S. government and provides that anyone, regardless of citizenship or residence, has the right to request access to federal agency records and information.

The *Privacy Act* strives for transparency throughout a program's lifecycle, and the *Freedom of Information Act* provides an additional layer of transparency. It gives anyone, regardless of citizenship or residence, the right to request access to federal agency records and information.

Under this Act,[16] all individuals may challenge an agency's response to their requests for disclosure in federal court. If they believe DHS improperly conducted a search, wrongly withheld records, or otherwise failed to follow this law, they are entitled to challenge those decisions in an administrative appeals process and, later, may bring civil actions against DHS to compel release of non-exempt material. Ultimately, individuals may be entitled to appeal their cases for access all the way to the U.S. Supreme Court. Indeed, the personal information of any individual has been protected from disclosure by the highest court of the United States. DHS takes this responsibility very seriously. In Fiscal Year 2009, for example, DHS processed more than 160,000 *Freedom of Information Act* requests at a cost of more than $43 million.[17]

EFFECTIVE OVERSIGHT THROUGH A SYSTEM OF CHECKS AND BALANCES

To understand how our privacy framework can be effective, it is important to understand how the U.S. government provides oversight and holds itself accountable. That is done via the three branches of the U.S. government: Executive (the president and his executive offices, such as departments and agencies), Legislative (Congress), and Judicial (courts). All have oversight responsibility for privacy policies and practices. All have a role in the checks-and-balances approach to government in the United States, and each is held accountable to the other two branches for its actions.

Transparency brings accountability to our system. Unless a program has met the high standard for restricted access, reports generated by any of the three branches of government are public, usually posted on the Internet, and open for interpretation and comment by the other branches, the media, and the general public. The opportunities and challenges posed by technology and the availability of information are at the cutting edge of the role of government and how it serves the people.

Executive Branch

The executive branch implements privacy laws through regulations, executive orders, notices, and directives. The statutes giving the DHS chief privacy officer the authority to evaluate DHS programs, systems, and initiatives for their potential impact on privacy and to mitigate any such impact have already been noted.

The Office of Management and Budget,[18] an office within the White House that reports directly to the president, provides leadership to all executive agencies by issuing directives and memoranda on how best to implement privacy laws. Circular A-108 is particularly significant for foreign audiences: it bridges the limitations of *Privacy Act* coverage to U.S. persons only[19] by directing that, "where a system of records covers both [U.S. persons] and [non-U.S. persons], only that portion which relates to [U.S. persons] is subject to the Act, but agencies are encouraged to treat such systems as if they were, in their entirety, subject to the Act." DHS enacted this directive via Privacy Policy Guidance Memorandum 2007-01,[20] which sets out DHS policy regarding privacy protections afforded to non-U.S. persons for information collected, used, retained, and/or disseminated by DHS in so-called mixed systems. This policy commitment protects all personal information in DHS systems regardless of an individual's citizenship status, and it was implemented, in part, through the creation of various administrative redress programs within DHS.

Inspectors general are appointed by Congress and imbedded in all large federal agencies. By the authority of the *Inspector General Act* (1978), inspectors general conduct independent investigations, audits, inspections, and special reviews of individual actions and programs to detect and deter waste, fraud, abuse, and misconduct.[21] In addition to mandatory reports to Congress twice yearly, Congress may require that the inspectors general either provide specialized reports or determine independently to initiate an investigation. Such investigations frequently include privacy-related issues.

Legislative Branch

Congress creates the laws that agencies, such as DHS, must implement. The collection by DHS of passenger name records for all flights to and from the United States, for example, is required by the *Aviation and Transportation Security Act of 2001*, a bill that received support from an overwhelming majority in Congress.

A U.S. Customs and Border Protection officer enters in information received from a license plate to determine its validity.

Oversight of this collection has been enacted by audits by the Office of the Inspector General, the U.S. Government Accountability Office (GAO), the DHS Privacy Office, and the European Union (through two joint reviews), as well as via Congressional oversight hearings.[22] The system of records notice and the privacy impact assessment for the system that maintains the passenger name records (the Automated Targeting System) are available to the public on the DHS website,[23] so anyone may know what information is gathered and how it is used. Concerned travelers may find out through the *Freedom of Information Act* what passenger name records data DHS holds, and, through redress options, may request to have any inaccuracies corrected.

The Government Accountability Office is an independent, nonpartisan agency that works for Congress. Often called the "congressional watchdog," it investigates how the federal government spends taxpayer dollars. Its mission is to support Congress in meeting its constitutional responsibilities and to help improve the performance and ensure the accountability of the federal government. It conducts investigations and audits as mandated by law or at the request of congressional committees, and it reports on how well government programs meet their objectives.

One DHS program that receives significant scrutiny by the Government Accountability Office is the Secure Flight program. As was required by Congress, DHS created Secure Flight to take on the pre-screening of passenger names against a watchlist—a function previously performed by air carriers. Due to robust oversight from the outset, including oversight of privacy issues, the Secure Flight system that now exists minimizes the potential privacy impact on passengers and further protects passenger rights while simultaneously implementing the law. The Government Accountability Office has also published a number of reports on its website on DHS programs, including the Privacy Office.[24]

Individual congressional committees have oversight authority for both DHS and its agencies, and, in addition, they monitor the performance of the Executive Branch and investigate allegations of wrongdoing. They hold hearings and may require Executive Branch agencies to give testimony and produce documents. They may revise laws to require the agencies to change their practices, or they may withhold funding from programs. This oversight and investigative authority has a major influence on the agencies and programs within DHS. It also promotes accountability through public and political pressure.

Due to robust oversight from the outset, including oversight of privacy issues, the Secure Flight system that now exists minimizes the potential privacy impact on passengers and further protects passenger rights while simultaneously implementing the law.

Judicial Branch

The Judicial Branch of the U.S. government adds one more layer of oversight and accountability in enforcing the various statutes cited here. Under the *Freedom of Information Act*, for example, all individuals may challenge an agency's response to their requests for information in federal court. Individuals may also, in certain circumstances, seek additional court review under the *Administrative Procedure Act* for such things as deletion of records or orders against certain disclosures.

REDRESS FOR ALL

Many travelers to the United States know that, to assist in determining admissibility, their personal information is often sent forward to the appropriate authorities before they arrive by air or that information is collected from them when they cross the border by land. Fewer are aware, however, despite publicity in multiple websites and publications, of the comprehensive system of privacy protection that accompanies the transmission of that data and of the ways in which individuals can ensure that their privacy is being protected. If questions or concerns remain, or if individuals believe that their personal information has been misused, there are multiple options for fair and effective redress.

The starting point for any redress opportunity is access to the information held in a U.S. government database. The *Freedom of Information Act* provides that all individuals have the right to request records held by a U.S. federal agency and to seek relief in federal court if their demand is not met.

An essential component of DHS accountability is the DHS Traveler Redress Inquiry Program (DHS TRIP), a single point of contact for individuals who have inquiries or who seek resolution for difficulties they experienced during their travel screening at transportation hubs—ports, airports, and train stations—or when crossing U.S. borders. Difficulties might include continual referrals for additional screening or denied or delayed airline boarding or entry into and exit from the United States at a port of entry or border checkpoint. This program not only brings inaccuracies to the attention of the record keepers but also serves as a central gateway to address misidentification issues on a watch-list.[25]

In some cases, individuals may go beyond DHS TRIP and seek judicial relief under the *Administrative Procedure Act* for agency decisions and actions—such things as deletion of records or orders against certain disclosures. Finally, as the chief privacy officer, I have broad investigatory powers. In the event that individuals are not satisfied with how their requests have been handled or wish to make inquiries or report an incident, my office is empowered to address the matter either by providing administrative redress or investigating the original matter.

EMBEDDED PRIVACY PROTECTIONS

The United States takes privacy very seriously, has a robust system of laws and policies to protect privacy, and has an authoritative system of accountability and redress to ensure those laws and policies are honored. Further, DHS's commitment to privacy enjoys support from the highest levels of the U.S. government, as Secretary Napolitano made clear in July 2010 at the Atlantic Council. She noted that the DHS Privacy Office is an "active participant in formulating policies before policies are implemented. And privacy protection is designed into our programs before they are begun … and fully integrated in the decision-making process at the department, throughout its many components."[26]

The Privacy Office works with every DHS component and program to ensure that privacy considerations

are addressed when planning or updating any program, system, or initiative. We strive to ensure that technologies used at the department sustain, and do not erode, privacy protections. We do not believe that privacy protections should be balanced against national security initiatives; in fact, any balance that is struck is made in Congress by politically accountable representatives of the U.S. population. Privacy is embedded into the lifecycle of DHS programs and systems to inform departmental policy making and to ensure effective privacy protections. The DHS Privacy Office strives every day to protect both American safety and its ideals.

NOTES

1 "As for our common defense, we reject as false the choice between our safety and our ideals. Our Founding Fathers, faced with perils that we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man—a charter expanded by the blood of generations. Those ideals still light the world, and we will not give them up for expedience sake."

2 U.S. Constitution, Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

3 http://www.dhs.gov/xabout/structure/gc_1265225837602.shtm

4 Secretary Janet Napolitano on the eve of the African regional aviation security conference, April 11, 2010: http://www.dhs.gov/ynews/releases/pr_1271085587404.shtm

5 This publication happens in the *Federal Register* for public review. At DHS we also publish our SORNs on our website: www.dhs.gov/privacy.

6 Section 1062.

7 The *Computer Fraud and Abuse Act (CFAA)* criminalizes intentional unauthorized access (or exceeding authorized access) to obtain information from a U.S. government computer system. For recent examples of CFAA enforcements, see www.justice.gov/criminal/cybercrime/cccases.html. *The Federal Information Security Management Act (FISMA)* strengthens information-system security by requiring agencies to implement policies and procedures to reduce information technology security risks to an acceptable level; it also requires annual reviews of agency information system programs submitted to the Office of Management and Budget (OMB) and to Congress.

8 §1606; Appeal and Redress Process for Passengers Wrongly Delayed or Prohibited from Boarding a Flight (49 USC § 44926), amends the Judicial Review of TSA Orders (49 USC § 46110 (a)) of the *9/11 Act*, Establishing DHS TRIP and Judicial Review of TSA Orders, established a single point of contact for individuals who have inquiries or who seek resolution of difficulties they experienced during their travel screening.

9 "Individuals" defined by the Privacy Act include U.S. citizens and legal permanent residents.

10 Report of the Secretary's Advisory Committee on Automated Data Systems commissioned by the U.S. Department of Health, Education and Welfare: http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

11 *Privacy Act*, 5 USC s. 552a(e)(1)

12 See 5 USC 552a(e)(4). A system of records is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

13 www.dhs.gov/privacy

14 DHS has updated its privacy impact assessment guidance several times, most recently in June 2010 under my leadership. The most recent guidance emphasizes the privacy analysis and imbedded protections, providing more clarity and transparency to the public. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

15 Section 803 of the *Implementing Recommendations of the 9/11 Commission Act* requires the designation of a senior official with privacy responsibilities similar to those of the DHS chief privacy officer in other executive branch agencies.

16 http://www.justice.gov/oip/foia_guide09/introduction.pdf

17 http://www.dhs.gov/xlibrary/assets/foia/privacy_rpt_foia_2009.pdf

18 For a complete set of privacy guidance directives issued by OMB, see its website at http://www.whitehouse.gov/omb/privacy/index.html.

19 Defined as U.S. citizens and legal permanent residents.

20 http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

21 www.dhs.gov/oig. DHS inspector general reports, resources, and testimonies released to the public are available from this site.

22 The reports from all these audits and hearings are or will be publicly available on the Internet.

23 http://www.dhs.gov/files/publications/editorial_0514.shtm#5

24 www.gao.gov

25 Access DHS TRIP at http://www.dhs.gov/trip. The information a traveler provides is shared in accordance with the provisions of the *Privacy Act* and as established in the privacy impact assessment published for the DHS Traveler Redress Inquiry Process.

26 http://www.acus.org/event/transatlantic-security-data-sharing-privacy-protection/transcript

Wesley Wark

THE SEARCH FOR AN INTELLIGENT BORDER: A CANADIAN PERSPECTIVE

Since the 21st century dawned and gave us the inferno of the Al Qaeda strikes on September 11, 2001, many countries have been forced to redefine their concepts of border security. This task has not been an easy one, nor has it yet been resolved. The threat environment has changed radically, old and sometimes cherished myths about the border have been abandoned, and new and hastily assembled models have been tried, tested, and often found wanting. Searching for a better idea of border security to meet new threats and safeguard citizens has had the unexpected effect of challenging concepts of delivering security and, more fundamentally, of questioning concepts of the border itself and ideas about state sovereignty.[1]

These general effects have been felt in many parts of the world where concerns about global, transnational terrorism have either added a new dimension to border security or layered an additional problem onto already complex or festering issues of protecting borders. The Canada-U.S. border is but one case study embedded in this global effect, shaped inevitably by unique factors: tradition; the pursuit of national self-interest; the framing of an understanding of threat; and the dynamics of the Canada-U.S. relationship, including our very close economic, political, and cultural ties. The search for a new and secure border in Canadian-American relations involves many strands—most commonly, intertwined concerns about security, sovereignty, and trade.

The pursuit of acceptable levels in all three of these public goods is a delicate balancing act. Canadian business elites, for example, were early and vigorous proponents of a new concept of the border—one that matched a more fully integrated North American economy with an integrated Canada-U.S. security system.[2] The sovereignty tradeoff was clear, though little discussed. In this scheme, the Canada-U.S. border would be transformed into a "shared checkpoint within the Canada-U.S. economic space."[3] But enthusiasm for advancing economic and security integration in lockstep as a necessary response to the new security landscape soon cooled, and eventually this idea produced little more than the summit diplomacy enshrined in the now-forgotten Security and Prosperity Partnership.

As the idea of economic integration dissipated, its early twin, security integration, had an unexpectedly bumpy ride. To understand what happened, we need to appreciate the shock of the 9/11 attacks as they were experienced in Canada. The shock was political, psychological, and economic. The Canadian government had to reassess its capacity to provide security within Canada and, inevitably, it shared the widespread fear at the time of the possibility of second-wave Al Qaeda strikes of equal or more devastating magnitude. The government had to reassure its citizens that it was capable of providing them with public safety. From the outset, it also had an unfamiliar border problem. The "longest undefended border" in the world had changed from a comforting myth into a threat itself. Despite the fact that the 9/11 attacks had nothing to do with the Canada-U.S. border—no hijacker crossed that border; no "Canadian connection" lurked; no Canadian logistical, financial, or other resources were provided to back the plot—securing the border became a top priority issue in Canadian-U.S. relations.

For the United States, the visceral shock of homeland vulnerability compelled an all-out effort to provide defense against attacks from outside. The effort at the northern border gained momentum from persistent fears in some political circles in the United States that Canada was somehow soft on security. These fears were perhaps understandable, usually not malicious, and most often based on ignorance about Canadian practices.[4]

From the Canadian perspective, the high priority attached to achieving a new border security regime with the United States was in part a reflection of U.S.

A Canada Border Services Agency detector dog and handler inspect a passenger vehicle.

fears. Canadian policy fell back on an old doctrine, nicely captured by political scientist Nils Orvik in 1973, about "defence against help."[5] To avoid overweening pressure ("help"), Canada would have to step up its own security measures and prove its stature as a worthy continental security partner. American fears were not just foisted on Canada; they mirrored Canadian fears. What if Canada had been penetrated by Al Qaeda and was hosting, unbeknownst to it, Al Qaeda cells or operatives determined to target Canada or the United States? This concern was not an idle fear. The Canadian Security Intelligence Service (CSIS) had been monitoring the rise of Sunni Islamic extremism throughout the 1990s, and counter-terrorism investigations had slowly risen to the top of its priorities since the end of the Cold War. What was new after 9/11 was the sheer dominance of the Al Qaeda threat as the prime investigative and analytical target of Canada's national security agencies.

Still, the economy was the greatest driving force behind Canadian efforts to tighten border security in combination with the United States. The closure of North American airspace and the lock-down at the border in the immediate aftermath of the 9/11 attacks offered a frightening vision of permanent and extremely damaging changes to the basic tenets of Canada-U.S. free trade and the fundamentals of Canadian economic prosperity.

The Canadian government strove mightily to prevent such a vision becoming any part of reality by engaging in high-level negotiations with the United States to define a new border strategy. The outcome was the Smart Border Declaration signed on December 12, 2001. That declaration used the phrase "zone of confidence against terrorist activities" to describe the plan for a strengthened border. The words were telling because they spoke to the basic lack in confidence both partners suddenly felt about the border problem. The Smart Border plan promised to harmonize policies and integrate efforts based on four "pillars": the secure flow of people; the secure flow of goods; a secure cross-border critical infrastructure; and coordination and information sharing.[6]

The Smart Border Declaration was an undoubted victory for Canadian diplomacy, at least in the short term.[7] It offered a solution for achieving security and the continuance of vital trade at the border while conveying the realization of a "harmonized" and "integrated" secure border (whatever that might mean) to bureaucracies in both countries who set to work on what was initially a 30-point action plan.

A new border, new laws, and new money were the hallmarks of national security policy in the first phase of Canada's response to the post-9/11 security environment.

The declaration is also significant as one of three great efforts made by the Canadian government in the most extreme phase of the 9/11 security crisis. Achieving a new deal on border security was arranged alongside the effort to pass Canada's first anti-terrorism legislation and the commitment of unprecedented fiscal resources to increasing Canada's national security capabilities. All three were finalized in December 2001. A new border, new laws, and new money were the hallmarks of national security policy in the first phase of Canada's response to the post-9/11 security environment. Of the three, only the passage of anti-terrorism legislation occasioned heated Canadian debate, with concerns expressed that Canada's anti-terrorism legislation was unnecessary, at odds with Canadian legal and democratic traditions, and even "draconian."[8] Critics aligned the *Canadian Anti-terrorism Act* with the passage of the *USA Patriot Act*, fearing that both laws were the product of undue panic and tilted the balance between state powers and civil liberties. The Canadian government responded by making some changes to the draft legislation and by proudly (and prematurely) proclaiming that the Act was "charter proof"—that it would uphold the bedrock principles of Canada's Charter of Rights and Freedoms.

Building new laws was clearly a matter of public concern in Canada, but building a new border was left to the bureaucrats and technocrats assigned to formulate the necessary action plans.[9] The pace of the work had its critics, notably in the Canadian Senate Committee on National Security and Defence (SCONSAD), chaired by the vigorous and media savvy Senator Colin Kenny. But the philosophy of a secure border achieved through harmonized and integrated efforts troubled few.[10]

The philosophy was advanced further when the Canadian government issued its national security policy statement, "Securing an Open Society," in April 2004. This policy identified three core national security interests: to protect Canada; ensure that Canada is not a launching pad for threats against allies; and contribute to international security. The ally that was of greatest concern, although curiously unnamed as such, was the United States. In addition to this unremarkable statement of core objectives, the statement listed eight contemporary national security threats, ranging from terrorism to pandemics and natural disasters.[11]

Described as an "all hazards" approach to thinking about security threats, in contrast to the United States' focus on the "war on terrorism," the Canadian policy statement was, in fact, a failed attempt to elucidate the reality of the new, national security environment. None of the threats listed were prioritized or described in any detail; how they compared was left mysterious, as was the notion that an integrated (e.g., cost-effective) system could be developed to respond to them all. The national security policy was framed by a desire to comfort the public, avoid priority setting that might entail further rounds of costly spending, and reassure close allies such as the United States.

One chapter of the national security policy was devoted to border security. Much of it detailed the progress made since 2001 in improving border security and implementing the Smart Border Declaration. Canada and the United States were described as "partners" in "systems and programs that expedite the flow of low-risk goods and people while increasing the information that is needed to screen higher-risk flows." The policy went so far as to celebrate the Smart Border plan as a model to be expanded into a trilateral North American context and exported globally.

Even as the national security policy was launched, however, one voice on the periphery of the national security community was calling attention to the underside

of the Smart Border Declaration—its heavy reliance on intelligence sharing. This critic was the federal privacy commissioner, an independent ombudsman and officer of Parliament, whose mandate involved not just upholding Canada's privacy laws but acting as a public spokesman on trends in the privacy sphere which might have implications for Canadian rights.[12] The privacy commissioner is not usually seen as a key stakeholder in discussions about national security issues in Canada, although this officer audits national security agencies for compliance with privacy legislation and evaluates "privacy impact assessments" relating to initiatives by government agencies, including those in the loosely defined Canadian security and intelligence community. Successive privacy commissioners have been determined to play a broader, almost Cassandran role in warning about the implications of new security policies, such as those adopted at the border.

The first public criticism by a privacy commissioner came in the 2001–2 annual report issued by George Radwanski. He warned that the "floodgates appear to have burst" and that government national security actions showed an increasing indifference to privacy concerns. His message was stark and critical: Big Brother was coming, based on the use of what he called the "magic incantation" of September 11 to "stifle debate, disparage critical analysis and persuade us that we live in a suddenly new world where the old rules cannot apply." Radwanski blamed the United States for this worrying state of affairs. He saw the U.S. hand in the push for extraordinary surveillance and the erosion of Canadian rights, and he warned against any unthinking mimicry of an American "war on terrorism."[13]

This was powerful stuff, and it spoke to a segment of Canadian concerns about the post-9/11 world. The problem, though, was that Radwanski was operating on the basis of anecdotal evidence and politicized fears rather than on any intimate knowledge of national security policy making. His message, while fiercely protective of Canadian privacy rights, was uninformed and ultimately unhelpful about the requirements and pressures of national security.

Radwanski soon got into trouble on other grounds and was dismissed from his office. Jennifer Stoddart,

Successive privacy commissioners have been determined to play a broader, almost Cassandran role in warning about the implications of new security policies, such as those adopted at the border.

his successor as privacy commissioner, took a more nuanced approach. Beginning with her annual report for 2003–4, she argued that a balance had to be struck between security and rights. Stoddart said she was not opposed to improving security; rather, "the question is how to do it in a way that does not destroy the fundamental values of our society."[14] Although she doubted the efficacy of a national security policy that maximized the volume of intelligence collection and worried in particular about the onward march of data mining in both the public and the private sectors, Stoddart believed that some reasonable ground rules could be established. She saw the Office of the Privacy Commissioner as having a central role in creating a new informational playbook for the post-9/11 age. That playbook would include rules around the protection of information, its retention, and its sharing.

Stoddart gave close attention to the implications of the Smart Border Declaration and enhanced intelligence sharing between Canada and the United States. She was concerned that information flows across the border for the purposes of achieving a Smart Border diluted Canadian privacy rights, because of differences in the legislative basis for national security actions between the *USA Patriot Act* and Canada's *Anti-terrorism Act*, because of weaker oversight of privacy rights in the United States, and because U.S. *Privacy Act* protection does not apply to foreign nationals.[15] In other words, cross-border intelligence sharing entailed a loss of control over information and a weakening of Canadian-style protections.

However much Stoddart brought a new style and nuance to arguments about balancing security and rights, the Office of the Privacy Commissioner remained a player on the peripheries of the national security debate in Canada—one still devoted to tilting at occasional windmills. Among these windmills was the *Anti-terrorism Act*, the efficacy and necessity of which Stoddart continued to doubt, and such new institutions as the Integrated Threat Assessment Centre, a nascent intelligence fusion centre created and housed at CSIS, which Stoddart feared might become the locus for an unbridled sharing of information across borders and within Canada.[16]

As Radwanski had earlier argued, privacy rights continued to be dangerously abstract for many citizens, and their defense an uphill battle, especially in the face of new demands created after September 11. Yet by 2007 the Office of the Privacy Commissioner believed that its outsider battle was beginning to show signs of success. Stoddart wrote in her annual report for 2006–7 that she had a sense "we may be turning a corner," after several years of erosion of rights in the name of increased national security.[17] There was greater reflection, she reported, an increased awareness of the dangers of and the need for more accountability and constraints. Much of this upbeat mood was based on the way another story had played out—that of Maher Arar. The Arar saga translated abstractions about the loss of privacy rights into a concrete and compelling narrative about national security excesses and abuses. Stoddart wrote, "As we have seen in the case of Maher Arar, the transfer of individuals' personal information outside Canada can have disastrous consequences."[18]

To recap the details briefly, Arar was a Canadian consultant and businessman who was detained in the United States in 2002 during a return trip to Canada from a family vacation in Tunisia. He was subsequently rendered to Syria on suspicion that he was connected to Al Qaeda. He spent a year in a Syrian prison, where he was subjected to torture, before finally being released to Canada—a release facilitated by high-level Canadian entreaties (including one from an emissary of the prime minister) and the fact that Syrian authorities found no evidence under which to charge him.[19]

A chain of events, beginning with an emotive telling of his story on his return to Canada and a subsequent botched RCMP raid in search of possible security leaks on the home of an Ottawa journalist, led the government to establish, reluctantly, a full public judicial inquiry into the case. The commissioner, Justice Dennis O'Connor, was charged with investigating Canadian officials' treatment of the Arar case and recommending necessary changes in policy. The Arar case and its ramifications had shocked the nation.

The O'Connor Inquiry was the most significant investigation into national security activities in Canada since the McDonald Inquiry in 1977–81, which led to the dissolution of the RCMP security service and the creation of the civilian Canadian Security Intelligence Service (CSIS). What was under the microscope in the Arar inquiry was intelligence sharing between Canada and the United States, one of the key tenets of the new national security environment and of the Canadian-initiated Smart Border plan. While O'Connor upheld the necessity of cross-border intelligence sharing in his report released in 2006, he was deeply critical of slipshod practices, the inability to exercise sufficient control over intelligence-sharing protocols, and the talent and capacity of key national security institutions—in particular, the RCMP. His overall message was that Canada was not yet institutionally smart about the handling and sharing of intelligence, and that it had to raise standards quickly in order to avoid future egregious failures such as the Arar case. O'Connor attributed Arar's fate at the hands of American officials to the RCMP's unwise and profligate sharing of uncorroborated and insufficiently analyzed intelligence with the United States.[20]

O'Connor recommended a follow-on internal judicial inquiry into Canadian intelligence-sharing practices with foreign agencies in the context of three other Canadian citizens who were jailed in the Middle East under suspicion of involvement in terrorism. This inquiry was headed by retired Supreme Court justice Frank Iacobucci. In his report, Iacobucci found that intelligence sharing conducted by CSIS and the RCMP with foreign agencies, including U.S. agencies, "indirectly" contributed to the detention and

International air travelers are electronically fingerprinted as they are processed by U.S. Customs and Border Protection agents upon arrival to Bradley International Terminal at Los Angeles International Airport (LAX) in Los Angeles, California.

torture of Abdullah Almalki, Ahmad About-Elmaati, and Muayyed Nureddin, all of whom wound up in national security jails in Syria and Egypt in the period between late 2001 and 2004. [21] All three individuals were eventually released without charge and allowed to return to Canada. The fact-finding Iacobucci report, unlike O'Connor's, contained no recommendations for policy changes and was, in that sense, of doubtful value. In combination, however, the O'Connor and Iacobucci inquiries put the information-sharing pillar of the Smart Border Declaration, one of the central and basically unchallenged assumptions of Canadian national security and Canada-U.S. border security, under notice.

In retrospect, as the first decade of the 21st century closes, we should never have treated intelligence sharing between our two countries as anything but problematic. O'Connor had it right when he stated: "Information sharing is vital, but it must take place in a reliable and responsible fashion. The need for information sharing does not mean that information should be shared without controls … Nor does it mean exchanging information without regard to its relevance, reliability, or without regard to laws protecting personal information or human rights."[22] O'Connor also stated: "Controls [on information sharing] are meant to facilitate and promote the orderly flow of information, not to impede or stop it."[23] Canadian national security agencies have found that it is easier to agree to this advice than to carry it out—a fact that has led to sustained tensions since 2006 between U.S. and Canadian authorities.

We have now come to another realization—that in fashioning an informational border security policy, we put the proverbial cart ahead of the horse. Intelligence taps were opened to maximum flow before we had a tool for assessing common threats which could help us define how best to share intelligence. Perhaps we assumed early on that such a tool would emerge organically, or that, given the power imbalance between Canada and the United States, along with their differing approaches to achieving global security,

21st-century border security depends on the continual building of an intelligent border with just the right calibration of intelligence flows and controls.

the effort was bound to fail and therefore not worth trying. However, a corner has been turned on this kind of thinking as well.

Beginning with a joint ministerial statement issued in May 2009 by Public Safety Minister Peter van Loan and Secretary of Homeland Security Janet Napolitano, the Canadian and U.S. governments committed themselves to the project of developing joint assessments to "assist the two countries in forming an understanding of the threats and risks we face."[24] As with the original Smart Border Declaration, the new project for an intelligent border has been initiated and pressed by the Canadian government. The hope is that a common threat assessment, if it can be crafted, will allow for more tailored intelligence sharing—and so get Canada off the "Arar hook." Much of the work on this initiative has proceeded in secret. A brief progress report was issued in a bilateral meeting in Washington, D.C., between Public Safety Minister Vic Toews and Secretary Napolitano in July 2010.[25] The "Joint Border Threat and Risk Assessment" was promised for release "later this summer." Although no release has yet occurred, that delay need not be taken as a sign of failure.

But whatever the shape of the report, whenever it is released, 21st-century border security depends on the continual building of an intelligent border with just the right calibration of intelligence flows and controls. Beyond that, all nations await another debate on what "just intelligence," based on the same principles as the "just war" doctrine, might look like. [26] Those basic principles are just cause, proportionality, right authority, and the reasonable prospect of success. The one principle from the just war doctrine we would have to discard is "last resort." It's a fine idea to make war a last resort, but in the 21st-century security environment, intelligence and its sharing between states has come to be a "first resort."

NOTES

1 John Winterdyk and Kelly W. Sundberg, eds., *Border Security in the Al-Qaeda Era* (London: Taylor and Francis, 2010).

2 Wesley K. Wark, "Smart Trumps Security: Canada's Border Security Policy since 11 September," in Daniel Drache, ed., *Big Picture Realities: Canada and Mexico at the Crossroads* (Waterloo, Ontario: Wilfrid Laurier University Press, 2008), 139–52.

3 Thomas d'Aquino, "Security and Prosperity: The Dynamics of a New Canada–United States Partnership in North America," Presentation to the Annual General Meeting of the Canadian Council of Chief Executives, Toronto, January 14, 2003. Available online at http://www.ceocouncil.ca. See also Wendy Dobson, "Shaping the Future of the North American Economic Space: A Framework for Action" *Commentary*, Issue 162, April 2003 (Toronto: C.D. Howe Institute).

4 The Canadian Embassy in Washington, D.C., made persistent efforts to correct misperceptions about Canadian security. See, for example, the op ed by Ambassador Michael Kergin published in the *Washington Times* on January 16, 2003. Available online at http://www.canadianembassy.org/ambassador/030116-en.asp

5 Nils Orvik, "Defence against Help: A Strategy for Small States," *Survival*, 15 (September/October 1973): 228–31; Donald Barry and Duane Bratt, "Defence against Help: Explaining Canada-US Security Relations," *American Review of Canadian Studies* 38 (March 2008): 63–89.

6 Canada-US Smart Border Declaration, December 12, 2001. Available online at http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp.

7 Reg Whitaker, "Securing the 'Ontario-Vermont Border': Myths and Realities in Post-9/11 Canadian-American Security Relations," *International Journal* 60 (winter 2004–5), 53–70; Wark, "Smart Trumps Security," 141.

8 The flavor of the Canadian debate in 2001 over the passage of the *Anti-terrorism Act* is captured in a conference publication from the University of Toronto Faculty of Law: Ronald J. Daniels, Patrick Maclem, and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (Toronto: University of Toronto Press, 2001).

9 Government of Canada, Department of Foreign Affairs and International Trade, "Thirty-Two Point Action Plan," January 13, 2005. Available online at http://www.dfait-maeci.gc.ca/can-am/main/border/32_point_action-en.asp.

10 Academic critics existed and gave voice to concerns about both human rights tradeoffs and immigration and refugee policies. See Howard Adelman, "Governance, Immigration Policy and Security:

Canada and the United States, Post 9/11," in John Tirman, ed., *The Maze of Fear* (New York: New Press, 2004), 109–30; Sharryn J. Aiken, "Risking Rights: An Assessment of Canadian Border Security Policies," in Ricardo Grinspun and Yasmine Shamsie, eds., *Whose Canada? Continental Integration, Fortress North America and the Corporate Agenda* (Montreal: McGill-Queen's University Press, 2007), 180–203.

11 Government of Canada, "Securing an Open Society: Canada's National Security Policy" (Ottawa: Privy Council Office, 2004). Available online at http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat_e.pdf.

12 A description of the mandate and mission of the Office of the Privacy Commissioner of Canada can be found on the official website at http://www.priv.gc.ca.

13 Canada, Office of the Privacy Commissioner, *Annual Report to Parliament on the Privacy Act, 2001–02*. Available online at http://www.priv.gc.ca/information/ar/02_04_10_e.cfm.

14 Canada, Office of the Privacy Commissioner, *Annual Report to Parliament on the Privacy Act, 2003–04*. Available online at http://www.priv.gc.ca/information/ar/200304/200304_e.cfm.

15 Canada, Office of the Privacy Commissioner, *Annual Report to Parliament on the Privacy Act, 2006–07*. Available online at http://www.priv.gc.ca/information/ar/200607/200607_pa_e.cfm.

16 Canada, Office of the Privacy Commissioner, *Annual Report to Parliament*, *2003–04* and *2006–07*.

17 Canada, Office of the Privacy Commissioner, *Annual Report to Parliament on the Privacy Act, 2006–07*, "Message from the Commissioner."

18 Ibid., "Transferring Information: A Risk Business."

19 Kerry Pither, *Dark Days: The Story of Four Canadians Tortured in the Name of Fighting Terror*, foreword by Maher Arar (Toronto: Viking Canada, 2008); Monia Mazigh, *Hope and Despair: My Struggle to Free My Husband, Maher Arar* (Toronto: McClelland & Stewart, 2008).

20 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. See, especially, chapter 1, "Overview," and chapter 9, "Recommendations."

21 Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nureddin (October 2008), *Executive Summary*, pp. 29–39.

22 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*, chapter 9, Recommendation 6, p. 331.

23 Ibid.

24 United States Department of Homeland Security, "Joint Statement by Secretary Napolitano and Canadian Public Safety Minister Peter Van Loan on the Canada-US Border," May 27, 2009. Available online at http:///www.dhs.gov/ynews/releases/pr_1243434829897.shtm.

25 Government of Canada, Public Safety Canada, "Public Safety Minister Toews and Secretary Napolitano Announce New Cooperative Initiatives to Combat Threats and Expedite Travel and Trade," July 13, 2010. Available online at http://www.publicsafety.gc.ca/media/nr/2010/nr201007/13-eng.aspx?rss=true.

26 See David Omand, *Securing the State* (New York: Columbia University Press, 2010), pp. 286–87.

MARY ELLEN CALLAHAN'S RESPONSE TO WESLEY WARK

In reading Wesley Wark's "The Search for an Intelligent Border" counterpoint to my essay on privacy and security, I was struck by the fact that "privacy" was not even mentioned until the latter half of his essay, and even then in a passing manner. Instead, Wark focused almost exclusively on security elements—national security, homeland security, international terrorism— without addressing how to incorporate privacy protections or the impact of these activities. His approach, and the clear separation between the security and privacy issues in Canada as he describes, illuminates the different attitudes to privacy and security between the United States and Canada. The U.S. Department of Homeland Security (DHS) does not attempt to "balance" border security and information sharing with privacy and civil rights but instead involves its Privacy Office from the outset of program- and policy-making processes, acknowledging what we see as inherent interdependency from the beginning.

The DHS Privacy Office works to ensure that privacy is protected when personally identifiable information is collected, used, shared, or maintained by the department. As Wark notes, information sharing is critical in today's global market. However, what is lacking in his description of the Canadian system is whether privacy leaders are ever included at the negotiating tables and policy forums to embed privacy considerations from the outset; to the extent this point is addressed in Wark's essay, he seems to indicate that Canadian privacy leaders are "not usually seen as a key stakeholder in discussions about national security issues in Canada." As I describe in my opening essay, this is not the case in the United States, and specifically at DHS. Secretary Janet Napolitano recognizes that security/privacy is "not an either/or problem."[1] She noted that "we need to protect both our national security and our national values"—not one over the other, but both. What we need to recognize in the global economy we live in today, however, is that we cannot allow relatively minor legal or cultural differences or, worse, misperceptions to derail security effort altogether. Of course, every nation has different laws, customs, and policies governing how information about its citizens is collected, stored, and shared. But the differences should not be used to suggest that one nation values privacy more than another, or that different privacy laws and legal systems are incompatible.

In the United States, chief privacy officers are included within federal agencies to work with policy makers and program managers to embed privacy protections into programs before they are launched. My role as the DHS chief privacy officer affords me the opportunity to influence new and existing DHS programs and policies before they begin. As Wark points out, Canada has an "independent" data-protection official with broad responsibilities for both public- and private-sector adherence to Canadian privacy laws. The privacy commissioner of Canada is an officer of Parliament who reports directly to the House of Commons and the Senate. The commissioner is an advocate for the privacy rights of Canadians and, by Wark's own admission, can frequently "only tilt at windmills."[2] The commissioner cannot issue orders or injunctions or impose penalties but instead uses the media effectively to carry out an advocacy role. The same is true for counterparts at the provincial and territorial level. By contrast, the DHS chief privacy officer and the U.S. Office of Management and Budget have the authority to prevent

The clear separation between the security and privacy issues in Canada illuminates the different attitudes to privacy and security between the United States and Canada.

DHS programs from going forward if they lack effective privacy compliance.

The privacy commissioner of Canada may not report publicly on the privacy management practices of government institutions, nor are government departments and agencies required by law to report on privacy-related activities. In contrast, the DHS chief privacy officer must submit not only an annual report to Congress but also quarterly reports covering all privacy protection activities of the department.[3] In addition, the DHS chief privacy officer submits annual reports on the department's data-mining activities.[4] This scrutiny alone should prove that there is not, as Wark suggests, "weaker oversight of privacy rights in the United States."

Other than U.S. law and the role of the DHS Privacy Office, we should also consider the unique relationship between the United States and Canada. Because we share the longest land border in the world, our economies, our cultures, and our security are inextricably linked. The economic data illustrates the close partnership between our two countries: roughly 300,000 people and US$1.5 billion in trade cross the border every day—the largest trade relationship in the world.

Protecting that border and trade, as well as our democratic way of life, requires diligence and cooperation. Justice Dennis O'Connor was correct when he stated, "Information sharing is vital, but it must take place in a reliable and responsible fashion. The need for information sharing does not mean that information should be shared without controls … Nor does it mean exchanging information without regard to its relevance, reliability or without regard to laws protecting personal information or human rights."[5] These core values are the cornerstone of the information-sharing principles articulated in July 2010 between Secretary Napolitano and Public Safety Minister Vic Toews when they agreed to move forward on a joint security vision. Such an effort includes the need for better information sharing and a common effort to address political and legal impediments to such sharing, while recognizing that any such approach must address current data privacy concerns and internal processes in both countries.

NOTES

1 Secretary Napolitano's address to the Atlantic Council, July 2010, http://www.acus.org/new_atlanticist/transatlantic-data-sharing-moving-forward-moving-backwards

2 The privacy commissioner's authority includes investigating complaints, conducting audits, and pursuing court action under the two federal privacy laws; publicly reporting on the personal information-handling practices of public and private sector organizations; supporting, undertaking, and publishing research into privacy issues; and promoting public awareness and understanding of privacy issues. See http://www.priv.gc.ca/aboutUs/mm_e.cfm.

3 As required by section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, PL 110–53.

4 Pursuant to section 804 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, entitled "The Federal Agency Data Mining Reporting Act of 2007" (Data Mining Reporting Act).

5 As quoted in Wark's essay.

WESLEY WARK'S RESPONSE TO MARY ELLEN CALLAHAN

The United States, as Mary Ellen Callahan's essay makes clear, was a pioneer in privacy legislation and in efforts to provide for accountability and transparency in government operations. Its privacy and freedom of information legislation preceded Canada's own laws and helped to inspire them. The past efforts of the United States in the area of privacy protection and its accompanying legislation deserve praise. The issue now is whether the United States, along with other partner nations such as Canada, can meet the challenges of privacy protection in a 21st-century environment. When it comes to the intersection of national security demands and privacy rights, the United States and Canada share broadly common problems and pursue generally common goals.

Among these problems is the relentless erosion of the sphere of privacy—indeed, the growing confusion about the very meaning and nature of privacy. Parts of this erosion and confusion are the product of efforts on the part of national security agencies in both countries to exploit the global information infrastructure as a means of acquiring worthwhile intelligence against a wide range of threats. Intelligence services still have an interest in "opening the mail" in their hunt for information. But the nature of that mail has radically changed.

Much of the mail is now electronic in nature, and the volume of information flows and information storage for use by both the commercial sector and the government is immense. Mysterious things (at least to the lay person) called algorithms shape data searches. Software programs, feeding on hard-to-imagine degrees of computational power, engage in data mining, deep penetrations, or surface stripping of the informational strata on which modern society depends. But if intelligence collectors have come up with new and ingenious ways to tap into the information revolution, it would be wrong to imagine them as the sole source of our privacy dilemma.

The issue now is whether the United States, along with other partner nations such as Canada, can meet the challenges of privacy protection in a 21st-century environment.

The erosion of the sphere of privacy that attends new forms of electronic intelligence gathering has been matched by rising confusion about what constitutes the sphere of privacy itself. Globalized communications, the creation and dissemination of electronic personal profiles by millions of people, and the efforts of major commercial entities to build customer-profile databases for the efficient and profitable management of their enterprises have all led to a significant reduction of both the idea and the reality of privacy.

In a world in which there are tremendous pressures on privacy from both the public and the private sectors, and in which traditional concepts of privacy are being rapidly abandoned, it is difficult to know where to draw the line. This effort constitutes a particular challenge in the field of national security.

Traditionally, democratic societies have sought a balance between privacy protection and the potentially intrusive demands for personal information for reasons of national security. That balance was erected in part through the establishment of a mediation system between national security agencies and privacy watchdogs, both of whose boundaries were set by legislation and mandates. Callahan's office within the Department of Homeland Security is clearly meant to function as a key component of mediation. The same could be said for the differently constituted federal Office of the Privacy Commissioner in Canada. Yet such mediation systems can easily be beset by standoffs and polarized arguments, especially in a post-9/11 world of rising domestic security requirements and

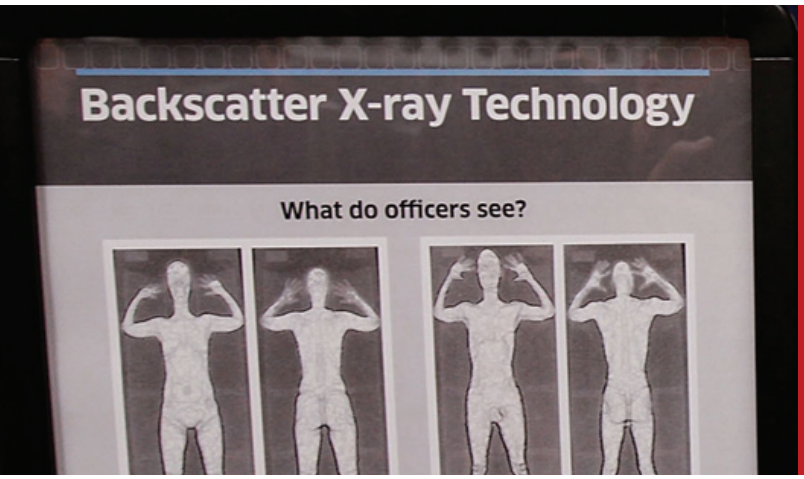
The erosion of the sphere of privacy that attends new forms of electronic intelligence gathering has been matched by rising confusion about what constitutes the sphere of privacy itself.

shrinking concepts of privacy. In the Canadian system, as I suggested in my essay, the federal privacy commissioner has played a Cassandran role in decrying the informational demands of national security, without making a sustained contribution to a genuinely mediated vision of what constitutes a convergent system of privacy protection and national security requirements.

Bureaucratic routines can also dull genuine mediation. I find it interesting to note that one "vital tool," as Callahan describes it, used by the DHS Privacy Office is that of privacy impact assessments. This exact same tool is used in the Canadian federal system, in which federal departments are required to submit to the Office of the Privacy Commissioner all such assessments of significant initiatives for new programs. The mediation architecture in Canada is fairly clear: departments defend new initiatives, and the privacy commissioner probes these initiatives in order to defend the public from privacy violations. In theory, privacy impact assessments are meant to be posted online as a measure of public transparency. In practice, the requirement is abused by delay, by obfuscation, and by national security overrides. Even when such assessments are available, they fall into a vacuum of complete public disinterest.

What can get lost in such a system, whether the architecture is Canadian or American, is genuine mediation. Departments and offices will always put forward their best and most generalized case in support of a new program, even as they inevitably downplay any potential privacy harms. Privacy watchdog officials will then do their best, from the outside, to hunt for possible privacy violations. In a static world in which the requirements for national security information were relatively unchanging and the concepts of privacy were relatively fixed, such a system might have worked. In a 21st-century context of flux everywhere, I have to wonder whether it can work. Callahan suggests that "privacy protections are key foundational elements to information security in U.S. federal agencies." We need something more, if privacy protections are truly to be regarded as foundational elements for national security—and vice versa.

Rather than hoping for mediation and balance through essentially adversarial approaches, a better system to defend both security needs and privacy rights might be to have national security agencies and privacy watchdogs jointly embrace the responsibility to advocate for national security requirements and privacy protections. In this way we might come closer to generating a security/privacy culture of the sort that is the best check on abuse. Governments on both sides of the border have an important leadership role to play in forging such a culture. But governments alone cannot legislate a security/privacy culture into existence. It has to conform to societal needs and desires. In this area, legislation governing access to information and freedom of information is another vital tool. At least in Canada, that tool is broken. I leave it to my American friends to say whether their system is faring any better.



About the Authors

1

In March 2009 **Mary Ellen Callahan** was appointed the chief privacy officer and chief *Freedom of Information Act* officer in the Department of Homeland Security. Her role there is to preserve and enhance privacy protections for all individuals, to promote the transparency of Homeland Security operations, and to serve as a leader in the federal privacy community. Ms. Callahan holds a Juris Doctor from the University of Chicago Law School and, before joining DHS, she was a partner with the law firm of Hogan & Hartson (now Hogan Lovells), where she specialized in privacy and data security law. She is a frequent author and speaker on privacy issues and serves as vice-chair of the American Bar Association's Privacy and Information Security Committee (Antitrust Division).

2

Wesley Wark, one of Canada's leading experts on intelligence and national security issues, is a professor in the Munk School of Global Affairs, University of Toronto. He is a past-president of the Canadian Association for Security and Intelligence Studies (1998–2000 and 2004–6) and has served on both the Prime Minister's Advisory Council on National Security and the Advisory Committee to the Canada Border Services Agency. He is completing a book on the history of Canada's intelligence community in its formative years and also writing a study of contemporary Canadian national security policy and counter-terrorism. His most recent publication is an edited volume, *Secret Intelligence: A Reader* (2009), and he is currently serving as an expert witness in several national security certificate cases before the Federal Court of Canada.

THE WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS is the living, national memorial to President Wilson established by Congress in 1968 and headquartered in Washington, D.C. It is a nonpartisan institution, supported by public and private funds, engaged in the study of national and world affairs. The Wilson Center establishes and maintains a neutral forum for free, open and informed dialogue. The Center commemorates the ideals and concerns of Woodrow Wilson by providing a link between the world of ideas and the world of policy and fostering research, study, discussion and collaboration among a full spectrum of individuals concerned with policy and scholarship in national and world affairs.

Lee H. Hamilton, *President and Director*

Board of Trustees
Joseph B. Gildenhorn, *Chair*
Sander R. Gerber, *Vice Chair*

Public Members: Melody Barnes, designated appointee from within the Federal Government; Hon. James H. Billington, Librarian of Congress; Hilary R. Clinton, Secretary, U.S. Department of State; G. Wayne Clough, Secretary, Smithsonian Institution; Arne Duncan, Secretary, U.S. Department of Education; David Ferriero, Archivist of the United States; James Leach, Chairman, National Endowment for the Humanities; Kathleen Sebelius, Secretary, U.S. Department of Health and Human Services

Private Citizen Members: Charles Cobb, Jr., Robin Cook, Charles L. Glazer, Carlos M. Gutierrez, Susan Hutchison, Barry S. Jackson, Ignacio E. Sanchez

PHOTOGRAPHS:
pp. 1, 4 © Scott Olson/Getty Images; p. 8 courtesy of U.S. Customs and Border Protection; p. 12 courtesy of Canada Border Services Agency; p. 16 © David McNew/Getty Images.

2010 WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS, WASHINGTON, D.C.

Woodrow Wilson International Center for Scholars
Canada Institute

THE CANADA INSTITUTE is an integral program of the Woodrow Wilson International Center for Scholars. The aim of the Canada Institute is to increase knowledge about Canada in the policymaking community, to focus on current U.S.-Canada issues and common challenges, and to keep an eye on the future, looking ahead to long-term policy issues facing the two countries in a variety of areas. The Canada Institute brings together top academics, government officials, and corporate leaders to explore key questions in the bilateral relationship through seminars, conferences, research projects, and publications.Woodrow Wilson International Center for Scholars

CANADA INSTITUTE
Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, NW
Washington, DC 20004-3027
canada@wilsoncenter.org
T (202) 691-4270
F (202) 691-4001
WWW.WILSONCENTER.ORG/CANADA

THE CANADA INSTITUTE deeply appreciates the support of ROGERS PUBLISHING LTD., MACLEAN'S MAGAZINE, and IBM for making this publication possible.

ROGERS™

MACLEAN'S

IBM®