Smart Borders, Virtual Borders or No Borders: Homeland Security Choices for the United States and Canada[1]

REY KOSLOWSKI*

I. Introduction

In the wake of the September 11th attacks on the World Trade Center and the Pentagon, the United States rapidly stiffened its border controls. Given the initial perception in the United States that the Canadian border was a sieve through which terrorists could easily pass, the United States redeployed Border Patrol officers to the U.S.-Canadian border. While the initial response to September 11 involved a massive increase of inspections at border crossings with Canada, this quickly led to traffic back-ups of fifteen hours at the border – delays that could not be economically sustained.

In response to these conflicting security and economic imperatives, discussions between the United States and Canada increasingly explored the possibility of building a "North American Perimeter" modeled after the European Union, whereby internal border controls are lifted as a common external border is established. These talks shifted focus toward international cooperation that would leverage information technology, yielding an "Action Plan for Creating a

Secure and Smart Border," which was announced on December 12, 2001 (White House 2002a). The initiatives to create a "Smart Border" of the future became a central feature of the subsequent National Homeland Security Strategy (White House 2002b). According to a White House statement:

> The border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory, and inspections at the border and measures within the United States to ensure compliance with entry and import permits . . . Agreements with our neighbors, major trading partners, and private industry will allow extensive pre-screening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic. The use of advanced technology to track the movement of cargo and the entry and exit of individuals is essential to the task of managing the movement of hundreds of millions of individuals, conveyances, and vehicles (White House 2002).

In a dramatic illustration of the Administration's agenda, Richard Falkenrath, former Deputy Assistant to the President and Deputy Homeland Security Advisor, drew an analogy likening the revolution in military affairs of the 1990s to the "revolution in border security" that

is taking place now.[2]

With respect to border control, the U.S. National Homeland Security Strategy is largely based on policy proposals to "push U.S. borders out" (Flynn 2000) beyond U.S. territorial boundaries. U.S. border control authorities have deputized airline agents to inspect the travel documents of United States-bound passengers. There has been increasing forward deployment of U.S. Immigration and Customs Enforcement (ICE) as well as Customs and Border Protection (CBP) officers, and the information technology to support them, such as electronic submission of passenger and cargo manifests in advance of departure to the United States. The electronic submission of data, collection of biometrics at U.S. consulates abroad, and development of an automated entry-exit system was increasingly described by the U.S. Department of Homeland Security (DHS) officials in terms of the emergence of "virtual borders."[3]

In this paper, I consider the options of developing smart borders, moving toward virtual borders, and eliminating border controls between the United States and Canada. I argue that smart borders cannot be totally virtual and significant physical infrastructure investments at the border will be necessary in order to enable new technologies to work their magic. These barriers have become particularly apparent through analysis of the new entry-exit system, US-VISIT,

which was not part of the original Smart Border agreements but is now becoming the largest DHS information technology deployment. Moreover, the smart borders approach is not necessarily complementary with proposals for a "North American Perimeter," even though they are often conflated in the broader context of bilateral cooperation between the United States and Canada.

II. Border Control After Sept. 11, 2001 and the "Smart Borders" Response

The DHS was established to increase transportation and border security, minimize the risk of another terrorist attack, and prepare to respond to any future attacks that may occur. The DHS' Bureau of Customs and Border Protection (CBP) has the task of intercepting terrorists at over 300 ports of entry and along the 5,525 mile U.S.- Canadian Border and the 1,989 mile U.S. – Mexican border. During the 1990s, the total U.S.-Canadian surface trade increased from $223 billion to $347 billion (DHS 2003) while the overall volume of U.S. international trade doubled. Given that Customs inspection personnel increased only by 7 percent during the decade (MITRE 2000), CBP screened potentially dangerous cargo and people out of the flows of legitimate trade and travel with only three-fifths of the human resources relative to the increased flows.

Moreover, the attacks demonstrated the vulnerability of the U.S. economy to shutdowns

of the transportation system. The grounding of commercial air traffic and heightened border security after the September 11th attacks amounted to the United States doing to itself what no enemy has done before: an embargo on trade (Flynn 2002). This self-embargo demonstrated the vulnerability of extended supply chains and trans-border just-in-time manufacturing, most dramatically on the U.S.-Canadian border. Up to ten million vehicles annually cross the Ambassador Bridge between the Windsor, Ontario and Detroit, Michigan, along with approximately 25 percent of U.S.-Canadian merchandise trade. Shortly after the attacks, traffic backed up to fifteen hours at the U.S.-Canadian border. Within days of the attacks, Daimler-Chrysler announced that it would have to stop several U.S. assembly lines for want of Canadian parts caught in the traffic back-ups at the border. Ford followed suit shortly thereafter.

In terms of growing flows of people, 440 million people entered the United States through U.S. ports of entry and a total of 358,373,548 entered through land ports with Canada and Mexico during fiscal year 2002 (DHS 2003: 1, 16). It has been estimated that there are now 9.6 million undocumented migrants in the United States (Passel, Capps, Fix 2004), about 30 to 40 percent of whom entered legally but overstayed their visas. The September 11 attacks exposed the security consequences of increasing migration and travel, as terrorists used the same

modalities of visa abuse and identity document fraud characteristic of illegal migration to the United States. At least two of the hijackers used fraudulent passports (9/11 Commission 2004): one with a student visa never showed up for class; three had stayed in the United States after their visas expired; and several purchased fraudulent New Jersey driver's licensees and Virginia ID's on the black market that primarily services illegal migrants. Al-Qaeda operated a "passport office" at the Kandahar airport to alter travel documents and train operatives, like Mohamad Atta (9/11 Commission 2004a: 169). Contrary to the initial discussions that all the 9/11 hijackers entered legally and that border controls were irrelevant to their entry, the 9/11 Commission concluded that "15 of the 19 hijackers were potentially vulnerable to interception by border authorities" (9/11 Commission 2004a: 384).

It became clear that terrorists could take clandestine routes used by transnational criminal organizations to smuggle illegal migrants into the United States. For example, a month after the September 11th attacks, Italian authorities found Amir Farid Rizk, an Egyptian-born Canadian national, inside a shipping container bound for Canada along with a global satellite phone, laptop computer, airport maps, airport security passes, and an airplane mechanic's certificate. Italian authorities suspected that he was an Al Qaeda operative and arrested him under Italy's new anti-

terrorism law but then released him several weeks later (Toronto Star 2001). The case demonstrated how easy it might be for a terrorist to enter the United States in the same way that migrants have been smuggled in shipping containers. The 9/11 Commission staff report on terrorist travel details links between human smugglers, Al-Qaeda, and other terrorist groups in need of travel facilitation (9/11 Commission 2004a).

The post-9/11 approach to border control taken by the Bush Administration was perhaps first articulated in the U.S.-Canadian Smart Borders declaration. The action plan includes using biometric identifiers for permanent resident cards and travel documents, sharing advance passenger information from the U.S. Advanced Passenger Information System (APIS) and its Canadian counterpart, developing compatible immigration databases, such as Canada's Support System of Intelligence, and expanding the NEXUS pre-approved passenger vehicle program as well as the NEXUS air pilot program (White House 2002a). Frequent travelers who enroll in the NEXUS program submit information for criminal and terrorist background checks. An enrollee then receives a radio frequency identification (RFID) proximity card. The RFID tag on this card is read at the port of entry and pulls up background information and a photo for an inspector. The inspector can then quickly verify the NEXUS cardholder's identity and wave him or her

through.

The Smart Borders plan is premised on bilateral cooperation that enables the United States to deploy information technology in order to practice risk management targeting of vehicles, shipments, and travelers, and to push the United States' "borders out," while at the same time it attempts to minimize the impact of border controls on trade and travel. By the spring of 2003, significant strides were made in realizing many of the specific objectives in the U.S.-Canadian agreement (Meyers 2003). Further progress on the U.S.-Canadian Smart Border agreement was announced on October 3, 2003, highlighted by completed NEXUS implementations at nine ports of entry (U.S. and Canada 2003). As of September 2005, there were 11 NEXUS crossings and 80,000 U.S. and Canadian nationals enrolled in the program (Bonner 2005).

Although the NEXUS program is perhaps the quintessential example of the smart borders approach, physical infrastructure approaching some border crossings inhibits participation. For example, when traffic is backed up on the Ambassador Bridge, drivers enrolled in NEXUS often cannot get to the NEXUS lane because the bridge lanes (usually two going each way but can also be switched to three one way and one the other) are open to all traffic, NEXUS and non-NEXUS

alike. This is one reason that there are more NEXUS program participants at the Blaine, Washington area crossings than in the Detroit-Windsor area crossings, even if Detroit-Windsor has a much greater population.

These Smart Border Agreements are complementary, if not integral, to several major U.S. border security initiatives. In January of 2002, U.S. Customs Commissioner Bonner announced the Container Security Initiative (CSI) that pre-screens cargo containers at ports of origin or transit rather than when they reach the United States (Bonner 2002). The In-Transit Container Security Initiative between the United States and Canada was a Smart Border Accord action item that deployed U.S. Customs inspectors in Halifax, Vancouver, and Montreal, Canadian inspectors in Newark and Seattle, and became a model for CSI.

In April 2002, Commissioner Bonner announced the creation of the Customs-Trade Partnership Against Terrorism (C-TPAT), a public-private partnership to increase the security of cargo while facilitating trade. As Commissioner Bonner put it, "The message should be clear-if a business takes steps to secure its cargo against terrorism, we will give it the "fast lane" through the border (U.S. Customs 2002)." Seven companies helped to establish the program – BP America, Daimler Chrysler, Ford Motor Company, General Motors Corporation, Motorola Inc.,

Sara Lee Corporation, and Target (U.S. Customs 2002). It is not an accident that the big three automakers figure prominently among the founders. Over 7,000 companies have signed agreements.

In a certain sense, the forward deployment of U.S. Customs personnel with the CSI draws on the model of longstanding cooperation between the United States and Canada on immigration. U.S. immigration inspectors have long operated beyond U.S. borders in Canada. Since an agreement signed in 1894, U.S. inspectors posted at Canadian ports of entry have inspected U.S.-bound immigrants. Immigration inspectors were subsequently posted to Canadian airports to conduct "pre-inspections," which essentially cleared U.S.-bound passengers flying from abroad and connecting through Canadian airports. If a person flies into the United States from Japan via Vancouver or Toronto, he or she will be greeted by U.S. Customs and Border Protection inspector.

Point 8 of the U.S.-Canadian Smart Border Agreement outlines an agenda for cooperation on advanced passenger data, and Point 17 deal with customs data. The Aviation and Transportation Security Act passed by Congress in the fall of 2001 requires that airlines with U.S.-bound international flights electronically submit a passenger manifest with data including

full name of each passenger, date of birth, sex, passport number and country of issuance, and U.S. visa number or alien card number.[4] The subsequent 2002 U.S. Enhanced Border Security and Visa Entry Reform Act requires commercial airlines and ships to electronically submit passenger and crew manifests before arrival to the United States via the Advanced Passenger Information System (APIS), and sets out fines for non-compliance and loss of landing rights for those airlines that have not paid their fines.[5]

Canada also deployed its passenger information system (PAXIS) at Canadian airports in October 2002 and began collecting passenger name record (PNR) data (Auditor General 2004). Canada and the United States have agreed to share passenger manifests and passenger name records using an automated data-sharing program that will also assess risks of the passengers in question (U.S. and Canada 2003). Canada also agreed to share passenger data with the United States on a case-by-case basis, in which Canada's PAXIS and the U.S.'s APIS will use risk management criteria common to both countries in automated risk-scoring of the PNR data to determine which data will be shared.

In order for CSI's vision of pre-screening containers in the port of origin to work, CBP needs information about the contents of containers in order to determine whether or not they

should be x-rayed and/or physically inspected. On December 2, 2002, U.S. Customs instituted a new regulation requiring advanced electronic submission of cargo manifests twenty-four hours before U.S.-bound sea containers are loaded (Bonner 2002a). Electronic manifest information must be submitted two hours before arrival into the United States by train and one hour prior to arrival for trucks, unless they are in the Free and Secure Trade (FAST) program, which can submit data up to thirty minutes before arrival.[6] In response to these advanced electronic data submission requirements, David Bradley, President of the Canadian Trucking Alliance expressed concern about these requirements and noted that "if just-in-time becomes problematic, industry will just ship production to the U.S." (Quoted in Halifax Daily News 2003). Despite such concerns, companies have managed to meet advanced data submission requirements. In the future, customs authorities could tap private sector logistics systems to such an extent that border controls may begin at the point a shipping notice is entered in manufacturers' inventory, warehousing, and distribution systems.

The June 2005 Security and Prosperity Partnership of North America, which superseded the Smart Border Accords, outlines a set of ambitious goals for traveler and cargo security. For example, "test technology and make recommendations, over the next 12 months, to enhance the

use of biometrics in screening travelers destined to North America with a view to developing compatible biometric border and immigration systems," "devise a single, integrated global enrollment program for North American trusted traveler programs within the next 36 months," and complete "the negotiation of the Canada-U.S. visa information sharing agreement within 18 months" (Canada, U.S. and Mexico 2005: 30).

In short, the United States and Canada have taken major strides to implement border control information technologies, share data, and set out an ambitious agenda. The technological intensity and corresponding cooperation may very well be the greatest along the border between any two countries in the world. Nevertheless, this may not be enough, particularly for the U.S. Congress, which has mandated implementation of technologies that would go beyond those outlined in the Smart Borders Accord and the Security and Prosperity Partnership and with expectations and a schedule that will be difficult, if not impossible, to meet, as illustrated with the following case study of the implementation of US-VISIT.

III. Virtual Borders: Entry-Exist Systems and US-VISIT[7]

Section 110 of the U.S. Illegal Immigration Reform and Immigrant Responsibility Act of 1996 had mandated that the Immigration and Naturalization Service (INS) develop an automated

entry-exit control system that would "collect a record of every alien departing the United States and match the records of departure with the record of the alien's arrival in the United States."[8] This was to be done by the end of 1998. Congress pushed back the deadline for implementation of the law in October 1998 after lobbying by U.S. business groups, states, and localities bordering Canada and Mexico (Cohn 1999). These groups pointed out that registering every person who crosses into the United States from Canada or Mexico, even using then-existing smart card technology, would still require enough processing time to back up traffic at the border for hours, especially at the Detroit-Windsor crossing.[9]

The Data Management Improvement Act (DMIA) of 2000 amended section 110, mandating the development of an entry-exit system to be put in place at all air and seaports by the end of 2003, at the fifty most highly trafficked land ports of entry by the end of 2004, and at all ports of entry by the end of 2005. In practical terms, however, the DMIA deflected the creation of a full-fledged entry-exit system with a complete database since it limited data collection to that which was already being collected by the INS by existing authorities of law and disallowed collection of any new entry-exit data.[10]

The entry-exit tracking system that existed prior to September 11, 2001, primarily

covered passengers arriving by airplane and consisted of a paper I-94 form stamped at the port of entry. The I-94 form was supposed to be collected by the airline upon departure, given to the INS, then sent by the INS to a contractor who manually entered the data into the database of the legacy INS Nonimmigrant Information System (NIIS). Due to lost forms, incomplete or inaccurate data entry, exit by land border, and incomplete deployment of the system, missing exit data corrupted the database, leaving inspectors with no effective way of knowing if individuals had overstayed their visas (Bromwich 1999). This was the case with several of the September 11th hijackers.

In response to the September 11th attacks and the failures of government information systems that they exposed, Congress passed and President Bush signed into law entry-exit system provisions in the USA PATRIOT Act[11] and in the Enhanced Border Security and Visa Entry Reform Act of 2002.[12] Both pieces of legislation reiterated the DMIA mandate for implementation of an entry-exit system and added requirements for collection of biometrics. The Enhanced Border Security and Visa Entry Reform Act, passed in the Senate by a margin of 97 to 0 and in the House 411 to 0. Most recently, the Intelligence Reform and Terrorism Prevention Act of 2004 called for an acceleration of the full implementation of an automated biometric

entry-exit data system, including collection of biometric exit data from all those required to provide biometrics upon entry; integration of all databases that contain information on aliens and interoperability with the entry-exit system; policies and procedures to maintain accuracy and integrity of entry-exit data; frontline personnel training; and a registered traveler program that is integrated into the automated biometric entry-exit system.[13]

In 2003, the DHS established the US-VISIT program to

> collect, maintain, and share information on foreign nationals, including biometric identifiers, through a dynamic, interoperable system that determines whether the individual: should be prohibited from entering the U.S.; can receive, extend, change, or adjust immigration status; has overstayed or otherwise violated the terms of their admission; should be apprehended or detained for law enforcement action; needs special protection/attention (i.e., refugees) (DHS 2003a: 8).

In accordance with congressional mandates, US-VISIT is being implemented incrementally (DHS 2003a; GAO 2005). Increment 1 of US-VISIT went live January 5, 2004, when DHS began to collect digital photographs and fingerprint scan biometrics from those individuals traveling on a nonimmigrant visa to the United States upon entry at 115 airports and

fourteen seaports. Increment 2A was to deploy equipment and software at all ports of entry to capture biometric data from machine-readable travel documents by October 26, 2004, but this deadline was extended. Increment 2B deployed the entry capabilities of Increment 1 at the fifty highest-volume land ports of entry by December 31, 2004. Increment 2C involves pilot deployment of a radio frequency (RF) system that captures biographical data at exit as well as entry at one or more land ports of entry by June 30, 2005. Increment 3 extends Increment 2B capability to the remaining 115 land ports of entry by December 31, 2005. Increment 4 will be an expanded set of releases of the envisioned, integrated solution to be developed by an Accenture-led team over the coming years.

US-VISIT only added an average of only fifteen seconds to the entry process and thus did not significantly impair travel flows at the airports and seaports where it was deployed. By the end of 2004, US-VISIT processed 16.9 million foreign visitors (DHS 2005). Increment 2B was rolled out at the fifty busiest land border crossings without any appreciable disruptions of traffic flows because at land borders, enrollment in US-VISIT can be performed in secondary inspection since it is only mandatory for those individuals who require an I-94. Enrollment in US-VISIT is only required of those traveling on a regular visa or entering under the Visa Waiver

Program. Enrollment in US-VISIT is not required of U.S. citizens, permanent resident aliens, visa-exempt Canadian nationals,[14] or the seven million plus Mexicans with border crossing cards, who together constitute the four largest categories of entries. Initially, the requirement for biometric enrollment in US-VISIT upon entry into the United States did not apply to nationals of the twenty-seven states in the U.S. Visa Waiver Program who are permitted to enter and stay in the United States without a visa for up to ninety days. Starting September 30, 2004, the DHS required nationals from Visa Waiver Program countries to enroll in US-VISIT and submit to a digital photograph and finger scanning upon entry. In FY2002, regular visa and visa waiver entries constituted only 6.3 million of the 358.3 million total land border entries (DHS 2003a: 12), or approximately 1.7 percent. If current entry rates follow recent historical patterns, only 1.5 to 2 percent of those people entering the United States over land borders are being enrolled in US-VISIT.

Although there were no shutdowns at the end of 2004 when US-VISIT was deployed at the Ambassador Bridge, there could be significant slowdowns at land borders due to more stringent travel document inspection made necessary by the need to verify the identity of those exempt from US-VISIT (i.e., U.S. citizens, legal permanent residents, visa-exempt Canadians,

and Mexicans with border crossing cards). For example, upon entry at land borders, U.S. citizens may make an oral declaration of their citizenship, and the inspector, using his or her judgment, may allow the person to enter if satisfied with the totality of information available or ask to see proof of citizenship (usually a passport). There are 320,000 records of lost or stolen U.S. passports reported since 2002 (DHS-OIG 2004: 7). Currently, anyone crossing a land border can declare his or her U.S. citizenship to avoid US-VISIT. In order to address this problem, the Intelligence Reform and Terrorism Prevention Act of 2004 stipulates that as of January 1, 2008, it will be unlawful for U.S. citizens to enter the United States without bearing a valid U.S. passport or other designated documentary proof of citizenship. Similarly, all Canadian and Mexican nationals will be required to present their passports or other proof of citizenship.[15]

When the US-VISIT enrollment exemption for nationals of Visa Waiver Program countries was eliminated at the end of September 2004, Canada became the only country whose nationals could enter the U.S. without submitting biometrics. This made Canadian passports increasingly valuable on the black market serving human smugglers, especially those issued before the passports with digitized embedded photos began to be issued in May 2002 and were

fully deployed by the end of 2003. Older passports valid for up to five years from date of issuance have laminated photos that are more easily altered by photo substitution and used by another person. Increased demand for stolen Canadian passports may not only present an increasing problem for Canadians traveling abroad; the Royal Canadian Mounted Police are concerned that criminals and terrorists may use these passports. There are already more than 25,000 Canadian passports reported lost or stolen each year. Although the Canadian Passport Office began deactivating lost and stolen passports beginning in April 2003, due to privacy considerations the Passport Office did not share its list of deactivated passports with Citizenship and Immigration Canada. The inspectors at Canadian ports of entry could not identify deactivated passports (Auditor General 2004: 31-32).

As of February 2004, data on lost and stolen passports has been manually entered into RCMP databases (Passport Office 2004), but the 2004 Auditor General report noted high error rates and data entry lags (Auditor General 2004: 31). The 2005 Auditor General Report notes improvement in that entry lag: reports of lost passports were entered into the Canadian Policy Information Centre database within thirty-five days on average as opposed to seventy days during the previous year (Auditor General 2005: 13-14). If data on lost and stolen Canadian

passports are not also shared with U.S. authorities, Canadian passports stolen in Canada or abroad could be photo substituted and used by individuals to enter the U.S. without submitting biometrics or being subject to criminal and terrorist biometric watch lists.

There is a possibility that US-VISIT exemptions for Canadians could be terminated. In FY2002, visa-exempt Canadian nationals comprised 14 percent of all entries. The DHS inspector general expressed "concern" over visa-exempt Canadian travelers and noted the interception of eight Canadian citizens at airports between January and August of 2004 who were suspected of terrorist activities. "(B)ecause visa exempt Canadians are not enrolled in US-VISIT, the likelihood of intercepting those same Canadian citizens at land (ports of entry) is small" (DHS-OIG 2005: 18). If, however, Canadians lost their exemption from US-VISIT entry-exit requirements at land borders, it may be impossible to direct all those who need to enroll in US-VISIT to secondary inspection because parking space would quickly fill at many ports of entry and lead to gridlock with back-ups into the primary inspection booths.

As Geronimo Gutierrez, the undersecretary for North America at the Mexican Secretariat of External Relations, stated, "We have pre-NAFTA infrastructure at our borders" (Gutierrez 2004). With new data collection requirements in addition to increasing trade and travel flows, it

may become impossible to process visitors and shipments without backing up traffic, unless larger secure areas at border crossings are cleared for inspection lanes and booths and more bridges and tunnels are built, especially between the Canada and the United States.

At certain ports of entry such as the Detroit-Windsor Tunnel, the busiest passenger crossing on the U.S.-Canada border, there is little space available on the Detroit side to expand the number of lanes and booths for secondary or primary inspections. Such physical constraints on expanding existing ports of entry, combined with expectations of increasing trade and travel over the coming decades, has led to many proposals for building additional bridges and tunnels between the United States and Canada, particularly at the Detroit-Windsor crossing. These proposals have been thwarted by the dynamics of not-in-my-backyard (NIMBY) interest group politics, the political maneuvering of the privately-held Ambassador Bridge Company (which seeks to build a new span itself and minimize competition in the meantime), and a lack of political will on the part of state and national governments to raise the taxes necessary to build additional publicly-funded bridges.

Congressional mandates refer to an "automated entry and exit process," but there is not yet much of an automated exit process in place at land borders. At most land border crossings

there are currently no facilities for outbound inspections. The existing exit data collection at land borders involves those traveling on visas and those under the Visa Waiver Program depositing their I-94 forms in drop boxes when they leave, usually at CBP secondary inspection locations on inbound lanes. At some crossings into Canada, Canadian inspectors will collect the I-94 forms and send the forms across the border to be added to the drop box collection. Contactors then enter the information written on the forms into a database, which can be compared to entry records.

Although there are currently no exit controls at most U.S. land borders, one could envision exit controls at land borders that would mirror entry controls with the construction of additional lanes and booths, the installation of biometric readers and workstations, and the hiring of inspectors to process departing foreigners and record exit data for US-VISIT. Instead, the US-VISIT program plans to use RF technology to expedite travelers through border controls. In January 2005, the DHS announced planned tests for using RF technology for entry and exit at land borders (DHS 2005a) and in February issued an environmental assessment statement on the Increment 2C proof of concept at the selected land ports of entry where it would be piloted (DHS 2005b). Although RF-enabled exit controls at land borders that do not include a primary

inspection by a DHS officer might save billions of dollars, they cannot determine whether someone has overstayed or should be apprehended when leaving because there are limits on what processes can be securely automated in the collection of exit data. An RF-based exit system may record the exit of an RF-enabled travel document, but one can only be certain that the person exiting with the document is the same person who entered with that document if that person is physically checked against the picture on the document and the biometric on the chip.

The Increment 3C proof of concept at five land ports of entry proposes to use automatic identifiers (a-IDs) to register exits. When a foreign national enters at one of the 2C pilot land ports of entry, he or she will go to secondary inspection to submit biographical and biometric data for I-94 processing and will be issued an a-ID. The a-ID will have a number that is linked to a database with the traveler's biographical and biometric data. No biographical or biometric data are stored on the a-ID itself. The system will then register entries and exits of the traveler with the a-ID when crossing in a vehicle. The RF readers appear to be similar to those used for EZ-Pass and other automated toll systems, some of which now read radio frequency identification (RFID) tags on cars passing by at fifty-five miles per hour.

It is hard to envision how an RF system could automatically "check out" holders of a-ID

cards as they drive through exit lanes and determine whether the person leaving is the same person who arrived. For example, a criminal or terrorist could overstay his visa but be registered as having "checked out" by paying a Canadian national to take his RF-enabled a-ID and exit the United States as a passenger of a car driven through the exit lane into Canada.

To deal with this problem, US-VISIT officials have suggested that a wireless biometric card could be used. As individuals are enrolled in US-VISIT upon entry, they would be given an RF-enabled entry-exit card with a wireless fingerprint reader that could transmit a live read of the individual's fingerprint as the person exited to verify that the person did indeed leave with the entry-exit card.[16] As drivers and passengers subject to US-VISIT exit requirements cross the land border out of the United States, they would put their finger on the finger scan section of the card as they pass under the RF readers. The reader would collect the data transmitted from the card and the digitized finger scan biometric. The biographical data would register an exit to correspond to the individual's entry, and the finger scan biometric would be matched to the finger scan collected upon enrollment to verify the identity of the individual exiting. However, there are no currently available off-the-shelf wireless fingerprint reader cards that are appropriate for the US-VISIT exit process at land borders,[17] and operable wireless fingerprint exit

verification will have to wait to be part of the final increment of US-VISIT.

Even if such an RF-enabled exit process can be developed, there is a major problem with its practical application. The proposed RF-enabled exit process would be very susceptible to deception by those who wish to register an exit but then overstay their visas. A finger scan reader on a wireless entry-exit card is much more susceptible to "spoofing" than enrollment in US-VISIT at ports of entry. There have been several experiments showing that finger scan readers can be spoofed with fake fingers made of gelatin and other materials (Van der Putte and Keuning 2000; Matsumoto, et. al. 2002). Someone could make a fake finger (following instructions readily available in Internet articles) and have someone drive it over the border while pressed on the finger scan reader of the wireless entry-exit card. Antispoofing techniques include supervised enrollment, enrolling several biometric samples, e.g., two fingers instead of one, and multimodal biometrics, e.g., facial and fingerprint (Schuckers 2002). Enrollment in US-VISIT at ports of entry employs all three.

Even if a criminal or terrorism suspect attempted to exit without pressing his finger to the finger scan reader or if the RF system registered a "hit," what could U.S. authorities do if the suspect had already crossed the border into Canada or Mexico, especially if the individual in

question holds a Canadian or Mexican passport? Are the enforcement measures in this situation as good as what could be attained with an exit inspection process that was similar to the entry process (that is, presentation of travel documents to an inspector, identity check based on facial recognition and fingerprint scan, watch list check, and optional secondary inspection)?

It is unlikely that a secure land border exit process in which the automobile does not stop is viable. At best, an automated, self-service exit station could be envisioned. Individuals could drive up to the exit station; drivers and passengers could use their wireless entry-exit cards to transmit their finger scans to the RF reader. When the exit is recorded, the station would print out paper receipts, and the barrier would lift to allow the car to pass. If the exit generated a lookout hit, the barrier would not raise and CBP officers could pull the vehicle over for secondary inspection. This solution would still be susceptible to deception with fake fingers. The only secure solution would be to require supervised collection of scans of at least two, if not ten, fingers and a digital photo.

The physical limitations of US-VISIT implementation imposed by deficient land border crossing infrastructure, particularly at bridges and tunnels in bi-national urban areas, may be partially overcome by intensified international law enforcement cooperation. Instead of building

exit booths and staffing them with CBP officers to conduct primary exit inspections, Canadian Border Services Agency officers could simultaneously conduct their entry inspections together with U.S. exit inspections, so-called "reversed inspections." Canadian officers would collect biographical and biometric data and enter that exit data into US-VISIT.[18]

Canada and the United States have already shared in infrastructure development at two ports of entry (Oroville, Washington, and Sweetgrass, Montana) and have agreed to a land pre-clearance pilot project at the Buffalo-Fort Erie Peace Bridge that will move all U.S. primary and secondary inspections to the Canadian side of the bridge. For Canadian officials to assume responsibility for the US-VISIT exit process would require significant cost sharing and a high level of mutual trust. Nevertheless, it may be the best, if not the only, secure option short of building and staffing an exit infrastructure comparable to the existing entry infrastructure.

IV. Smart Borders vs. North American Security Perimeter

Although the idea of a North American perimeter had been discussed long before September 11, 2001, reactions to the attacks and to the clampdown by the United States at the border quickly raised the profile of the discussion. A week after the attacks, former U.S. Ambassador to Canada Paul Cellucci said in response to a question, "I think that if we had

policies on immigration and refugee status that were more common we could establish this perimeter to protect the United States and Canada, and I think that is where we should be headed" (Cellucci 2001). Canadian business groups were quick to endorse the approach. Perrin Beatty, President and CEO of the Canadian Manufacturers and Exporters (CME) argued, "A perimeter approach to security would ensure the protection of both Canada and the United States from external threats while allowing relatively free movement between the two countries" and 88 percent of the respondents to a questionnaire distributed at the CME convention also favored a North American perimeter (Canadian Newswire 2001). Members of the Canadian government, however, were not that interested in adopting harmonized security and immigration policies. Foreign Affairs Minister John Manley said "the notion that we can somehow or another solve a perceived problem by something called a perimeter is just rather simplistic to me" (quoted in Fraser 2001). After announcing that Canada and the United States were discussing moves to reduce the difference between the two in the list of countries whose nationals are required to have a visa for entry, former Immigration Minister Elinor Caplan remarked, "When you say 'perimeter,' people think the European model where you erase the internal borders. That is not what we are talking about" (quoted in Alberts 2001).

In response to the reluctance of the Canadian Government, Fred McMahon, Director of the Centre for Globalization Studies at The Fraser Institute, argued:

> Imagine the boost to Canadian businesses if goods could move across the Canada-US border as quickly as they can the German-French border. Imagine the convenience for individual Canadians crossing the border. . . . The European model would require some coordination of Canadian immigration policy with that of the United States, something European nations have already put in place. This hardly means that immigration policies must be identical in the US and Canada and Mexico any more than they are identical in Europe (McMahon 2001).

In comments at a meeting to commemorate the tenth anniversary of NAFTA, Former Prime Minister Brian Mulroney also weighed into the debate in favor of a security perimeter saying:

> The NAFTA partners must dedicate themselves as a matter of the greatest urgency to building an area of security in North America, one that denies terrorism a foothold on our continent and insures uninterrupted legitimate flows among us. Such common action is also essential to allow us to protect the great

> North/South flows of goods, people, technology that underpins our shared prosperity. Our internal borders will only be smart if our external perimeter is secure (Mulroney 2002).

Mr. Mulroney's speech propelled the notion that efforts to modernize borders between the United States and Canada through the deployment of new technology must be complemented by building a North American perimeter through the harmonization of policies. In the rest of this section, I will critically examine the European model for North American border control and consider the extent to which smart borders are complementary to a North American perimeter.

During the 1980s, intra-European trade and intra-European travel increased while, at the same time, shipments increasingly went by truck and more Europeans drove cars. This became a recipe for huge backups at borders as trucks and tourists stopped at borders for passport inspections. A trans-European shipment could easily involve crossing two or three borders with waits totaling longer than the time on the road between borders. Since the European Community (EC) member states had entered into a customs union in 1968, the cargo that trucks carried was not subject to duty payments when crossing internal borders. To address this problem of long border waits, Germany, France, Belgium, the Netherlands, and Luxembourg signed an

agreement in 1985 in the small Luxembourg border town of Schengen to gradually abolish internal border checks. Shortly thereafter the members of the EC signed the 1986 Single European Act, which set out a course for realizing the free movement of goods by eliminating non-tariff barriers to trade and establishing free movement in services and persons by 1992.

The rights of nationals of one EC member state to work in another does not mean unimpeded travel across borders; however, given the growing lines at the border, there was increasing pressure for EC member states to lift border controls between states. Therefore, a subset of EC member states built on the 1985 Schengen Agreement by signing Schengen Convention in 1990. The Schengen Convention harmonizes asylum application procedures and mandates that asylum seekers may only apply in one country. It also calls for a common visa policy, harmonization of policies to deter illegal migration, and an integrated automated information system so as to coordinate actions regarding individuals who have been denied entry. All customs controls at internal borders within the newly established European Union were lifted in 1993, and the Schengen Convention went into effect in 1995, lifting internal border controls among its signatory states while establishing a common external border around them. Mr. McMahon is correct; in order for the United States, Canada and Mexico to adopt the

European model, immigration policies would not have to be identical; however, the European model presupposes a customs union and requires identical visa policies.

There are some difficult political questions for those who argue for lifting internal border controls within a North American perimeter, beginning with the question of Cuba. Would the United States and Canada be able to come to agreement the same set of tariffs on goods imported from Cuba? As to the Canadian case, I will leave this question to those more knowledgeable of Canadian domestic politics. The prospect of President Bush proposing to lift the embargo on Cuba for the sake of harmonizing tariffs with Canada is rather dim, given that the support of those Cuban Americans who oppose lifting the embargo has been essential to victory in Republican presidential primaries in Florida as well as winning general elections in the swing state of Florida. Even if President Bush were to expend the political capital to propose lifting the embargo, it is questionable as to whether or not a sufficient number of Republicans in Congress would support him. While the election of a Democratic president may change the political dynamics, if John Kerry had been elected president it is unlikely that he would have called for lifting the embargo. Although Kerry was quoted in a 2000 interview calling a reevaluation of the trade embargo "way overdue," in a radio interview during the 2004 campaign he stated, "I'm

pretty tough on Castro, because I think he's running one of the last vestiges of a Stalinist secret police government in the world . . . and I voted for the Helms-Burton legislation to be tough on companies that deal with him" (quoted in Wallsten 2004). So, if it is unlikely that the United States would drop its trade embargo on Cuba in the near future, would Canada be willing to join in the embargo for the sake of lifting internal border controls with the U.S.?

There are similar challenges for developing a common visa policy. In order to enter the United States, visitors from all but the twenty-seven Visa Waiver Program countries and Canada must apply for and receive a visa. The Visa Waiver Program has specific requirements of states as discussed above and states may be added or dropped from the program. Canada has similar policies exempting nationals of some states from the requirement to have a visa for entry. The United States and Canadian exemption lists do not, however, coincide. For example, nationals of Botswana, the Republic of Korea, Mexico and residents of Hong Kong and a host of British dependencies and Commonwealth countries do not need a visa to enter Canada but these countries are not in the U.S. Visa Waiver Program (see table 1).

Table 1

Comparison of visa free travel to the U.S. and Canada[19]	
U.S. Visa Waiver Program Countries	**Canadian Visitor Visa Exemptions**
Andorra	Andorra
	Antigua and Barbuda
Australia	Australia
Austria	Austria
	Bahamas
	Barbados
Belgium	Belgium
	Botswana
Brunei	Brunei
	Cyprus
Denmark	Denmark
Finland	Finland
France	France
Germany	Germany
	Greece
	the Holy See
	Hong Kong[20]
Iceland	Iceland
Ireland	Ireland
	Israel (National Passport holders only)
Italy	Italy
Japan	Japan
Liechtenstein	Liechtenstein
Luxembourg	Luxembourg
	Malta
	Mexico
Monaco	Monaco
	Namibia
Netherlands	Netherlands
New Zealand	New Zealand
Norway	Norway
	Papua New Guinea
Portugal	Portugal
	Republic of Korea
	St. Kitts and Nevis
	St. Lucia
	St. Vincent
San Marino	San Marino
Singapore	Singapore
	Solomon Islands
	Swaziland

Slovenia	Slovenia
Spain	Spain
Sweden	Sweden
Switzerland	Switzerland
	Western Samoa
United Kingdom	United Kingdom[21]
	Anguilla, Bermuda, British Virgin Islands, Cayman Islands, Falkland Islands, Gibraltar, Montserrat, Pitcairn, St. Helena or the Turks and Caicos Islands[22]

Given that visa-free travel to Canada not only reflects strong historical ties but also corresponds to major tourist flows and business relationships, how realistic would it be for Canada to cut its visa exemption list to that of the United States? Given that after September 11, 2001, members of Congress had entertained the idea of eliminating the Visa Waiver Program all together, it is unlikely that major expansion of the Visa Waiver list to encompass the Canadian list is politically feasible in the near future. Moreover, even if Congressional support emerges for adding particular countries to the Visa Waiver Program, such as the recent introduction of Congressional resolution in support of Poland's petition for visa-free travel, these countries might not coincide with the Canadian list – thereby widening rather than narrowing the discrepancies among the visa exemption lists of both countries. Even if the United States were to expand its visa waiver list as Canada's contracted, those countries added would have to meet

biometric passport requirements that EU member states will have difficulty meeting in the near future. In light current political dynamics, would it be politically feasible for Canada to require visas of fellow members of the British Commonwealth or the rich Hong Kong Chinese investors that Canada so successfully recruited to immigrate to Canada in the 1990s?

Without even moving onto the issues of harmonizing asylum policies and establishing an integrated information system, the political barriers to a customs union or common visa policy between the United States and Canada will be difficult to surmount. It is possible that leaders of both countries may some day overcome these obstacles, but unlikely within the timeframe of the border security legislation passed by the U.S. Congress.

V. Conclusion

Smart borders are not just a matter of deploying hardware and software; they require international cooperation – and lots of it. Existing smart border agreements lay out an agenda for extensive international cooperation, but even more cooperation will be necessary to collect the necessary data for the smart border concept to work in practice. The "revolution in border security" that moves from smart borders to virtual borders, ironically, requires significant physical infrastructure investments at or near the border in order to work as envisioned.

International cooperation can also reduce the overall costs of necessary infrastructure, however, international cooperation in joint border infrastructure development and joint inspections may be too controversial politically in the immediate future. The upshot: significant economic and political barriers to implementing the smart borders concept remain outstanding.

An alternative to making borders smarter is to get rid of borders altogether within a North American perimeter. If policymakers are convinced that lifting internal border controls by establishing a North American perimeter is the best way to proceed, it makes little sense to invest billions of dollars in acquiring land and building infrastructure at the border only to have cars and trucks speed through abandoned facilities after border controls are lifted. If a customs union, harmonized visa policy, and harmonized asylum policy are judged to be politically feasible in the next few years, then those policymakers who believe in the North American perimeter idea should press forward and begin harmonizing policies immediately before billions are wasted on border infrastructure.

If a North American perimeter is not realistic politically, yet still held out as an alternative to building physical infrastructure, the hope for a North American perimeter could reduce political support for the increases in budgets, taxes, and fees necessary to realize the

"smart borders" vision in practice. Rather than taking an either/or position, one could advocate moving forward with the smart borders initiatives while at the same time reducing discrepancies in customs duties, harmonizing visa and asylum policies, as well as building up border control capabilities at external border of the North American community (see, e.g., Dobson 2002: 30, Hufbauer and Vega-Canovas 2003). This is a very reasonable strategy but political capital is not infinite. Political leaders must pick and choose their battles.

If business groups support politicians who tell them what they want to hear about borders disappearing behind a North American perimeter and withhold their support from politicians who call for raising taxes and fees to build more bridges, exit lanes, and exit booths at the border, as well as hiring more inspectors to staff them, it is unlikely that border controls meeting the security requirements set by the U.S. Congress will come into being. If voters withdraw support from politicians who call on all Canadians to enroll in US-VISIT and who call on U.S. citizens to accept passports with fingerprint biometrics, it is unlikely that border controls meeting the security requirements set by the U.S. Congress will come into being. If politicians will not expend the necessary political capital and business leaders and citizenries do not support them, it is more likely that a core part of the "smart borders" approach, US-VISIT, will follow in

the path of the entry-exit system mandated by 1996 legislation – partial deployment that ultimately cannot effectively achieve its objectives.

References:

9/11 Commission 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton 2004).

9/11 Commission 2004a. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*. Downloaded Aug. 19 *at*: http://www.9-11commission.gov/staff_statements/index.htm.

Alberts, Sheldon 2001. "Border Deal Would Screen Travelers Before they Arrive," *National Post*, Nov. 9, 2001.

Auditor General 2004. "National Security in Canada-the 2001 Anti-Terrorism Initiative," Chapter 3 of the *2004 Report of the Auditor General of Canada to the House of Commons*. Accessed March 30, 2004 *at*: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/04menu_e.html.

Auditor General 2005. "Passport Office – Passport Services," Chapter 3 of the *2005 Report of the Auditor General of Canada to the House of Commons*. Accessed June 15, 2005 *at*: http://www.oag-bvg.gc.ca/domino/reports.nsf/html/05menu_e.html.

Bonner, Robert C. 2002. "U.S. Customs Commissioner Robert C. Bonner Speech Before the Center for Strategic and International Studies (CSIS)," Washington, D.C. Jan. 17, 2002.

Bonner, Robert C. 2002a. "Remarks of U.S. Customs Commissioner Robert C. Bonner," Trade Support Network, Oct. 9, 2002 *at:* http://www.customs.gov/about/speeches/speech101002.htm.

Bonner, Robert C. 2005. "Remarks by Robert C. Bonner Canadian/American Border Trade Alliance Washington", D.C. Sept. 12, 2005. Accessed Sept. 20, 2005 *at*: http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/09122005_speech.xml.

Bromwich, Michael R. 1999. “Statement before the House Judiciary Committee”, Subcommittee on Immigration and Claims, Mar. 18, 1999.

Canada, Mexico and U.S. 2005. Security and Prosperity Partnership of North America, Report to Leaders, Governments of Canada, Mexico and the United States, June 2005.

Canadian Embassy 2003. “Governor Ridge and Deputy Prime Minster Manley Issue One-Year Status Report on the Smart Border Action Plan,” Press Release, Canadian Embassy Washington, DC, Oct. 3, 2003.

Canadian Newswire 2001. “Canada-U.S. Border Concerns Prompt Support for Perimeter Approach to North American Security,” *Canadian Newswire,* Oct. 2, 2001.

CBP 2004. “United States - Canada NEXUS Program,’ Customs and Border Protection website. Downloaded Sept 8, 2004 *at*:

http://www.cbp.gov/xp/cgov/travel/leavingarrivinginUS/arrival_departure/nexus.xml.

Cellucci, Paul 2001. Remarks by Ambassador Paul Cellucci at the Canadian Club of Ottawa, September 18, 2001. Downloaded Mar. 20, 2004 *at*: http://www.usembassycanada.gov/content/content.asp?section=embconsul&document=cellucci_0918

Cohn, Theodore H. 1999. "Cross-Border Travel in North America: The Challenge of U.S. Section 110 Legislation," *Canadian American Public Policy* No. 40, Oct. 1999, Occasion paper Series of the Canadian-American Center, University of Maine at Orono.

DHS 2003. "Data Management Improvement Act (DMIA) Task Force Second Annual Report to Congress," Department of Homeland Security, 2003.

DHS 2003a. "Request for Proposals for US-VISIT Program Prime Contractor Acquisition," RFP No. HSSCHQ-04-R-0096, US-VISIT Office, Department of Homeland Security, Nov. 28, 2003.

DHS 2005. "DHS Entry-Exit System Meets 2004 Goals Ahead of Schedule," press release, Department of Homeland Security, Jan. 2005.

DHS 2005a. "Homeland Security Announces Plans to Test Radio Frequency Identification Technology at Land Borders," Department of Homeland Security, Jan. 27, 2005.

DHS 2005b. *Draft Environmental Assessment, US-VISIT Increment 2C Proof of Concept at Select Land Ports of Entry*, Department of Homeland Security, Feb. 24, 2005.

DHS n.d. "US-VISIT Fact Sheet: U.S. Land Borders" Downloaded Mar. 28, 2004 *at*: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0371.xml.

DHS-OIG 2004. "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States," Department of Homeland Security, Office of Inspector General, OIG-05-07 Dec. 2004.

DHS-OIG 2005. "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program at Land Border Ports-of-entry," Office of Inspector General, Department of Homeland Security, OIG-05-11, Feb. 2005.

Dobson, Wendy 2002. "Shaping the Future of the North American Economic Space: A Framework for Action," *Commentary*, C.D. Howe Institute, No. 162, April 2002.

Flynn, Steven E. 2000. "Beyond Border Control," *Foreign Affairs*, Vol. 79 no. 6 (Nov./Dec.), pp. 57-68.

Flynn, Stephen, E. 2002. "America the Vulnerable," *Foreign Affairs*, Vol. 81, No. 1 (Jan./Feb.) pp. 60-74.

Fraser 2001. "Border 'not a problem,' Manley says," *Toronto Star*, Oct. 5, 2001.

GAO 2005. "Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant

Status Indicator Technology Program," Government Accountability Office, GAO-05-202, Feb. 2005.

Gutierrez, Geronimo 2004. "Remarks by Germonimo Gutierrez, Mexican Secretariat of External Relations," *North American Integration: Migration Trade, and Security*, Institute for Research on Public Policy, Ottawa, April 1-2, 2004.

Halifax Daily News 2003. "A North American Perimeter may be Canadian Business's Only Hope," *The Halifax Daily News*, Feb. 16, 2003.

Hufbauer, Gary and Gustavo Vega-Canovas 2003. "Wither NAFTA: A Common Frontier?" in Peter Andreas and Thomas J. Biersteker, *Rebordering of North America: Integration and Exclusion in a New Security Context* (London: Routledge, 2003).

INS 2002. Data Management Improvement Act (DMIA) Task Force First Report to Congress, Immigration and Naturalization Service, Dec. 2002.

Matsumoto, T. et. al. 2002. “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems,” Proceedings of SPIE 4677 (Jan. 2002).

McMahon, Fred 2001. “Perimeter Puzzle,” *Fraser Forum*, Dec. 2001.

MITRE, 2000. “MITRE helps U.S. Customs modernize its business systems,” *MITRE Matters*, September 2000. Downloaded July 1, 2001 *at*: http://www.mitre.org/news/matters/09-00/mm_09-00_6.shtml.

Mulroney, Brian 2001. “Notes for an Address by the Right Honorable Brian Mulroney,” *NAFTA at 10: Progress, Potential and Precedents*, Washington, DC, Dec. 9-10, 2002.

Meyers, Deborah Waller 2003. “Does ‘Smarter’ Lead to Safer? An Assessment of the Border Accords with Canada and Mexico.” *MPI Insight* Migration Policy Institute, June 2003, No. 2.

Passport Office 2004. “Passport Office Responds to Auditor General’s Report,” Press Release, #49, Passport Office, Department of Foreign Affairs and International Trade, Canada, Mar., 30, 2004.

Passel, Jeffrey S., Randy Capps, and Michael Fix 2004. “Undocumented Immigrants: Facts and Figures,” Urban Institute Immigration Studies Program, Jan. 12, 2004. Downloaded on Mar. 20, 2004 *at*:

http://www.urban.org/Template.cfm?Section=Home&NavMenuID=75&template=/TaggedContent/ViewPublication.cfm&PublicationID=8685.

Schuckers, S.A.C. 2002. “Spoofing and Anti-spoofing Measures,” *Information Security Technical Report* 7, no. 4 (2002), 56-62.

Toronto Star 2001. “Italian Court Frees Canadian Suspect,” *Toronto Star*, Nov. 16, 2001.

U.S. Customs 2002. “U.S. Customs Service Launches Customs-Trade Partnership Against

Terrorism" Press release, April 16, 2002.

U.S. and Canada 2003. “Smart Border Action Plan Status Report,” Office of Deputy Prime Minister Manley and DHS Press Office, Oct. 3, 2003.

Van der Putte T. and J. Keuning 2000. “Biometrical Fingerprint Recognition: Don’t Get Your Fingers Burned,” *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications* (Kluwer Academic Publishers: 2000).

Wallsten, Peter 2004. “Kerry's stances on Cuba open to attack,” *Miami Herald*, Mar. 14, 2004.

White House 2002. “Fact Sheet: Border Security,” The White House, Jan. 25, 2002. Downloaded on Jan 27 *at*: http://www.whitehouse.gov/news/releases/2002/01/20020125.html.

White House 2002a. “Action Plan for Creating a Secure and Smart Border: U.S. and Canada,” Press Release, Office of Homeland Security, December 12, 2001 Downloaded

Mar. 20, 2002 *at*: http://www.whitehouse.gov/news/releases/2001/12/20011212-6.html.

White House 2002b. "National Strategy for Homeland Security" Office of Homeland Security White House, issued July 16, 2002. Downloaded on Jan. 25, 2002 *at*: http://www.whitehouse.gov/homeland/book/index.html.

1. This article is a revised version of a paper "International Cooperation to Create Smart Borders," prepared for the conference on *North American Integration: Migration, Trade and Security*, organized by the Institute for Research on Public Policy (IRPP), Ottawa April 1-2, 2004. It incorporates insights and information from a May 2004 visit to Canada supported by the Canada Institute of the Woodrow Wilson International Center for Scholars. The research for this paper was supported by a fellowship from the Woodrow Wilson International Center for Scholars. I am very grateful to the Wilson Center for its support. The paper also incorporates information gathered in November

2004 visit to the Detroit-Windsor area funded by the Migration Policy Institute to whom I am very grateful.

* Associate Professor of Political Science, Rockefeller College of Public Affairs and Policy, University at Albany (SUNY). He also holds a joint appointment in UAlbany's College of Computing and Information. He is also Director of the Center for Policy Research Program on Border Control and Homeland Security.

2. Richard Falkenrath, Response to author's question at "Transatlantic Homeland Security? European Approaches to 'Total Defense,' 'Societal Security' and their Implications for the U.S." Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University (Feb. 19, 2004).

3. Customs and Border Protection Commissioner Robert Bonner used the term "virtual borders" in remarks at reception preceding the 2003 Customs and Border Protection Trade Symposium, Nov. 19, 2003 and the term was used extensively in US-VISIT Office, Department of Homeland Security, Request for Proposals for US-VISIT Program Prime Contractor, RFP No. HSSCHQ-04-R-0096 (Nov. 28, 2003). *See also* DHS 2003a.

4. Aviation and Transportation Security Act, Pub. L. No. 107–71, § 115 (2001).

5. Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107–173, § 402.

6. Trade Act of 2002, Pub. L. No. 107-210, § 343

7. The discussion in this section is more fully developed in Rey Koslowski, *Real Challenges for Virtual Borders*, (Migration Policy Institute, MPI Insights, June 2005), *available at*: http://www.migrationpolicy.org/pubs/Koslowski_Report.pdf.

8. Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, § 110.a.1; H. REP. 104-828 § 110 ((1996) (Conf. Rep.).

9. Senate Judiciary Committee Report, submitted with The Border Improvement and Immigration Act of 1998, S.1360, S. REP. NO. 105-197.

10. *See* Data Management Improvement Act of 2000, Pub. L. No. 106-21.

11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 414.

12. Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107–173, § 302.

13. The Intelligence Reform and Terrorism Prevention Act of 2004, H.R. 108-796, § 7208.

14. Canadian nationals entering the United States for short stays are exempt from most visa requirements and also from US-VISIT; however, those who are entering the United States on a visa are required to be enrolled in US-VISIT.

15. The Intelligence Reform and Terrorism Prevention Act of 2004, H.R. 108-796, § 7209 (b).

16. Robert Jacksta, U.S. Customs Perspective on US-VISIT, Address at Smart Borders: The Implementation of US-VISIT and other Biometric Control Systems, Alexandria, VA, (Oct. 26-27, 2004).

17. *Id.*

18. This had been recommended in the DMIA Task Force's first Report to Congress (INS 2002), at 37, *available at* http://www.azmc.org/downloads/DMIAReportCongress2002.pdf.

19. *See* U.S. Department of State, Visa Waiver Program, *available at* http://www.travel.state.gov/visa/temp/without/without_1990.html#15 (last visited Sept. 10, 2005)*; see also* Canadian "Visitor Visa Exemptions," Citizenship and Immigration Canada, Countries and Territories Whose Citizens Require Visas in Order to Enter Canada as Visitors, *available at* http://www.cic.gc.ca/english/visit/visas.html (last visited Sept. 10, 2005).

20. Persons holding a valid and subsisting Special Administrative Region passport issued by the Government of the Hong Kong Special Administrative Region of the People's Republic of China.

21. British citizens and British Overseas Citizens who are re-admissible to the United Kingdom

22. Citizens of these British dependent territories who derive their citizenship through birth, descent, registration or naturalization.