
20. USING BIOMETRICS TO REVISUALIZE THE CANADA—U.S. BORDER

SHOSHANA MAGNET*

- i. The Longest Undefended Border in the World: Maintaining the Boundary Between the United States and Canada 359
- ii. The Post-9/11 U.S.—Canada Border 361
- iii. Rumors that the 9/11 Hijackers came from Canada 361
- iv. The Reconfiguration of Canada in the U.S. Imaginary: from Friendly Neighbor to Terrorist Haven 362
- v. Making the U.S.—Canada Border Visible 364
- vi. Biometrics and Bordering 365
- vii. Outsourcing the Border 367
- viii. Biometric Failure 370
- ix. Conclusion 375

I. THE LONGEST UNDEFENDED BORDER IN THE WORLD: MAINTAINING THE BOUNDARY BETWEEN THE UNITED STATES AND CANADA

Stretching between the two countries for more than 5000 miles, the boundary between the United States and Canada is described as the longest undefended border in the world. More than 200 million people cross the border annually, making it the world's largest trading relationship.¹ Bilateral trade between the two countries is valued at close to \$680 billion Canadian dollars. More than \$1.5 billion dollars is exchanged across the border on a daily basis.² Extensive partnerships between the United States and Canada govern this border. From the Free Trade Agreement (FTA) and North American Free Trade Agreement (NAFTA) to North American Aerospace Defense Command (NORAD) and North Atlantic Treaty Organization (NATO) military accords, the list of bilateral initiatives between the two countries is extensive.

* The author would like to thank Robert Smith, Celiyana Rivera-Velazquez, Amy Hasinoff, Aisha Durham, Himika Bhattacharya, Helen Kang, Carolyn Randolph, Jillian Baez, Kent Ono, C. L. Cole, Paula Treichler, Ian Kerr, Jane Bailey, Daphne Gilbert, and the anonymous reviewers for their helpful suggestions.

1. U.S. Department of State, "Canada: Security Assistance," (2007), <http://www.state.gov/t/pm/65290.htm>.

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

This “special friendship” between the United States and Canada is not free of stress, nor has it been historically as issues of industrialization, social policy, natural resources, power, and pollution have taxed—and continue to tax—the relationship between the two countries. Disputes over the U.S.–Canada boundary were common in the nineteenth century. In particular, disagreements over boundaries within maritime regions gave rise to the War of 1812. Originally set along the 45th parallel, the U.S.–Canada border moved several times as a result of a series of nineteenth-century border disputes. In 1818, the Canada–U.S. boundary was reestablished at the 49th parallel.³ By the 1870s, relations between the two countries had become increasingly peaceable. In 1871, only four years after Canadian confederation, the Treaty of Washington officially recognized the borders of the Dominion of Canada,⁴ and relations between the two countries improved.⁵ All remaining boundaries between the two nations were settled nonviolently by 1903 when the Alaska boundary was resolved.⁶

In an attempt to avoid future border disputes repeating the near-conflicts that had occurred in the nineteenth century, Canada and the United States established the International Boundary Commission (IBC) in 1908, cementing a friendship through a bilateral border initiative. Initially designed to address boundary disputes between the two countries through the clarification of the boundary line between the United States and Canada, the IBC was made a permanent institution in 1925. Today, it is the IBC that maintains the 6-metre swath between the two countries, keeping the border clear of brush and vegetation, and maintaining the boundary markers and buoys that demarcate the U.S.–Canada border. Until recently, the IBC’s tasks have “been reasonably specific and technical in nature, a fact that kept its operation relatively free of controversy and public debate.”⁷

The IBC shares its boundary maintenance obligations with a second bilateral commission, the International Waterways Commission. The border between the United States and Canada is one-third water. Thus, determining the coordinates of the liquid boundary that traverses the Great Lakes and the St. Lawrence River is of paramount importance. This task was the responsibility of the International Waterways Commission, now the International Joint Commission (IJC).⁸ Although the relationship between the United States and Canada is not free from bilateral tensions, a boundary open to cross-border

3. John Herd Thompson and Steven Randall, *Canada and the United States: Ambivalent Allies* (Athens: University of Georgia Press, 1994).

4. Thompson and Randall, *Canada and the United States*, 40 (n. 3).

5. Norman Hillmer, Canada’s Relations with United States, *The Oxford Companion to Canadian History* (Oxford: Oxford University Press, 2004).

6. Thompson and Randall, *Canada and the United States*, 40 (n. 4).

7. *Ibid.*, 73.

8. *Ibid.*, 74.

trade has been the hallmark of the long and primarily friendly relationship between the two countries.⁹

II. THE POST-9/11 U.S.–CANADA BORDER

The events of September 11, 2001, prompted a significant change in U.S.–Canada border relations. Previously represented as the “longest undefended border in the world,” the border newly came to be understood instead as a reified line between the two countries, and openness was represented as a “luxury” that the United States could no longer afford.¹⁰ The United States ceased to understand Canada as its “friendly neighbor” and as the “Great White North.” Instead, U.S. understandings of Canada shifted to highlight the dangers to the United States of Canada’s “permissive” immigration and refugee policy. One incident in particular highlighted this transformation of Canada in the U.S. cultural imaginary: the persistence of the rumor that the 9/11 hijackers entered the United States from Canada.

III. RUMORS THAT THE 9/11 HIJACKERS CAME FROM CANADA

The shifting place of Canada in the U.S. national imaginary began immediately following the attacks on the World Trade Center and the Pentagon on September 11, 2001. Within days of the attacks, several major U.S. newspapers claimed that a number of the hijackers had entered the United States across the Canadian border. On September 13, 2001, an article in the *Boston Globe* suggested that investigators were “seeking evidence [. . .] that the hijackers responsible for Tuesday’s attacks had slipped into the United States from Canada.”¹¹ A day later, on September 14, the *Washington Post* asserted that two of the suspected

9. Of course, key differences between U.S. and Canadian national policies have historically and continue to tax their “special” relationship. One famous example is the tension between the two countries as a result of the Vietnam War, in which Canada repeatedly voiced concerns over U.S. military policy. Tensions between the two countries escalated over the course of the war when Canada accepted more than 50,000 draft resisters from the United States (Thompson and Randall, 2002: 230). More recently, Canadian resistance to American military policy surfaced in Canadian refusal to engage with the U.S. Star Wars plan for missile defense. Canada also refused to send troops to fight in Iraq, although Canada’s support for the war in Afghanistan makes it clear that the ambivalence that has historically plagued the relationship between the two countries remains.

10. Blas Nuñez-Neto, “Border Security: The role of the U.S. border patrol” (2005), <http://www.fas.org/sgp/crs/homsec/RL32562.pdf>.

11. Colin Nickerson and Ellen Barry, “Attack Aftermath/Looking for Answers to the Hunt: Seeking Trail of Suspects across Borders,” *Boston Globe* (September 13, 2001).

9/11 hijackers definitely had entered the United States across the northern boundary: “Two suspects in Tuesday’s terrorist attacks in the United States crossed the border from Canada with no known difficulty at a small, border entry in Coburn Gore, Maine, which is usually staffed by only one border inspection officer, a U.S. official said today.”¹² Although this claim quickly was disproved, it nonetheless continued to circulate.

Both immediately and over the next several years, the continuing persistence of this and other mistaken beliefs concerning Canada’s role in allowing terrorist access to the United States led the Canadian government to take steps to dispel a number of falsehoods about Canada’s connection to terrorism. In 2004, the government of Canada launched a website called CanadianAlly.com, designed specifically to reassure Americans that their neighbor to the north remains a friendly one. The website provided a number of facts about the relationship between the United States and Canada, including a “debunking the myths” section that roundly denounced original and persistent rumors that the 9/11 terrorists had entered the United States from Canada:

True or False: Some of the 9–11 Hi-jackers (sic) entered through Canada:

FALSE

This is simply not true. In fact, they had all been legally admitted to the United States, as has been confirmed by senior American officials.¹³

IV. THE RECONFIGURATION OF CANADA IN THE U.S. IMAGINARY: FROM FRIENDLY NEIGHBOR TO TERRORIST HAVEN

Despite these and other attempts by the Canadian government to dispel this mistaken belief, fears that Canada is a “terrorist haven” have continued to circulate. Since 2001, U.S. politicians ranging from Democratic Senator Hillary Clinton to Republican Senator Conrad Burns have repeated the story. Given that the mistaken claim that the 9/11 hijackers came from Canada was disproved almost immediately, why has this claim about Canada persisted?

Canada-as-terrorist-haven has served as a justification for U.S. attacks on Canadian immigration and refugee policy. Thus, U.S. congressional representatives repeatedly have “blasted Canada as an unwitting haven for a large number of terrorists, blaming soft immigration laws.”¹⁴ Shortly after 9/11,

12. DeNeen Brown and Ceci Connolly, “Suspects Entered Easily from Canada; Authorities Scrutinize Border Posts in Maine,” *Washington Post* (September 13, 2001).

13. Government of Canada, “Did you know? Facts about Canada and the US” (2007), <http://www.canadianally.com/ca/news-en.asp>.

14. Beth Gorham, “Wilson not worried about U.S. troops guarding border,” *Globe and Mail* (March 24, 2006).

U.S. members of the Foreign Service already were claiming that “Canada’s political asylum laws have helped make the country a ‘safe haven’ for foreign extremists.”¹⁵ Making clear that the perils of Canadian immigration were connected to the racialization of those crossing the border, a commentator in the *Los Angeles Times* argued that “security controls are famously lax in Canada because politically correct Canadians do not differentiate between 76 year old Madame Dupont coming to visit her grandchildren and bearded young men from Islamic countries.”¹⁶ Voicing the same problematic views about immigrant and refugee newcomers to Canada, Douglas Mackinnon, former press secretary to Bob Dole, argued that “the Canadian government not only willingly allows Islamic terrorists into their country, but does nothing to stop them from entering our nation [the United States].”¹⁷ Unpacking the durability of the myth of the 9/11 hijackers makes clear the ways that the border between the United States and Canada is undergoing transformation. After September 11, Canadian bodies are imagined to be newly suspect. This understanding of Canada underlies the need to make the U.S.–Canada border and unreliable Canadian bodies newly visible. Learning to see Canadian bodies as othered is a project to which biometric identification technologies are essential. Identifying what were problematically referred to as “homegrown” suspects is no easy task. Biometric technologies are represented as able to sharpen the edges of a border zone made soft by an historical understanding of the border as an unmilitarized zone separating special friends.

15. Brown and Connolly, “Suspects Entered Easily from Canada; Authorities Scrutinize Border Posts in Maine,” (n. 12).

16. Editorial cited in Peter Andreas, *The Rebordering of North America: Integration and Exclusion in a New Security Context* (New York: Routledge, 2003), 454.

17. Douglas MacKinnon, “Oh, no, Canada.” *Washington Times* (December 16, 2005). Although it is beyond the scope of this paper, it is important to note that the United States is not alone in its attacks on Canadian immigration and refugee policies. Canadians rushed to join the United States in blaming newcomers to Canada for terrorism. Regressive changes to Canadian immigration policies began pre 9/11; Sunera Thobani, “Nationalizing Canadians: Bordering Immigrant Women in the Late Twentieth Century,” *CJWL/RFD*, 12 (2000). However, connecting the 9/11 terrorists to immigrants and refugees expedited increasingly draconian reforms to Canada’s immigration policy. Thus, the bilateral *Smart Border Declaration*, signed in December 2001, included stipulations for a *Safe Third Country Agreement*, which would “harmonize” Canadian policies with those of their southern neighbor. This agreement, in prohibiting refugees who had filed a claim in the United States from filing in Canada, has succeeded in dramatically reducing refugee claims filed in Canada; Kent Roach, *September 11: Consequences for Canada* (Montréal: McGill-Queen’s University Press, 2003). Refugee claims from some countries, including many in Latin America, have been reduced even further. For example, refugees from Colombia have been reduced almost to zero since the *Safe Third Country Agreement* was signed.

V. MAKING THE U.S.–CANADA BORDER VISIBLE

The United States wants to better secure its border with Canada, but it might have trouble finding it in some areas, an official with the agency that maintains the border said. “If you can’t see the boundary, you can’t secure it.”

—Dennis Schornack, U.S. commissioner of the International Boundary Commission (IBC), the intergovernmental agency responsible for maintaining the U.S.–Canada border.¹⁸

Canada’s immigration and refugee policy was not the only part of the idea of the “Great White North” to come under post-9/11 US scrutiny. The U.S.–Canada border itself was the object of American anxiety with regard to the risks posed by Canada. Earlier, I noted the role of the International Boundary Commission in ensuring that the border between Canada and the United States be clearly defined as a recognizable “six-metre-wide swath” between the two countries. The IBC currently operates with a budget of \$1.4 million from the United States and \$2 million from Canada.¹⁹ This budget is extremely modest in comparison with the overall budget for border security. For example, Canada alone has earmarked \$368 million U.S. for border security in 2007–2008.²⁰ The goal of the IBC is to ensure that even those persons who accidentally stumble across the border cannot fail to note its existence—a challenge colloquially referred to by border officials as the “moron test.”²¹ Despite its identification as a simple undertaking, finding the U.S.–Canada border has proven to be no easy task.

The border is long. It runs through changing physical terrain, including territory that is remote and hard to access. In 2006, the *Ottawa Citizen* noted, “The United States is eager to install a battery of surveillance towers, motion sensors and infrared cameras to monitor the Canada–U.S. border. Now if only they can find it.”²² Old maps drawn in the 1930s and thorny vegetation up to four meters tall (12 feet) provide significant challenges to locating the border. Even those places that have been cleared on a regular basis quickly become

18. David Sharp, “U.S.–Canada Border Security Choked with Weeds,” *Dessert News* (October 1, 2006).

19. D. Bowermaster, “Blaine couple fight to retain backyard wall near Canada border,” *Seattle Times* (April 11, 2007). This budget is contentious, as the United States and Canada are supposed to share equally in IBC funding.

20. Stockwell Day, “Canada’s New Government invests over \$430M for smart, secure borders” (June 14, 2007), <http://www.cbsa-asfc.gc.ca/media/release-communique/2007/0112windsor-eng.html>.

21. Sheldon Alberts, “Where, Oh Where Has the Border Gone?” (April 27, 2006), <http://forum.blueline.ca/viewtopic.php?p=174897&sid=abb4abe8115ad391a8a22bfc3e4f18c7>.

22. *Ibid.*

overgrown with trees, brush, and snow, making the boundary hard to locate. In a 2006 article, the Associated Press documented that “The U.S. and Canada have fallen so far behind on basic maintenance of their shared border that law enforcement officials might have to search through overgrown vegetation for markers in some places.”²³ This inability to find the border causes serious consternation among the border officials of both countries.

Concerned border officers have expressed their apprehension about being charged with the difficult task of securing an invisible border. During his tenure with the IBC, Dennis Schornack, the former U.S. Commissioner of the International Boundary Commission, worried that the agency had not been able to physically locate the border in a number of places, asserting anxiously, “I can send you places where you just can’t find the border.”²⁴ As he said: “If you can’t see the boundary, then you can’t secure it.”²⁵ Schornack feared “real diplomatic dispute” between the two countries as a result of the border’s ambiguous location. Border officials responsible for guarding the boundary with renewed post-9/11 fervor found themselves playing a game of hide-and-seek—a game that highlights the tension over the paradoxical process of making the border visible.

The hard work of cutting down hedges to locate the border has failed to attract the attention and excitement of funders to the IBC in the face of sexier technological solutions. “I’ve talked and talked, and we don’t seem to be getting anywhere,” stated Schornack, additionally making reference to the fact that weed whackers no longer suffice in the manufacturing of the border. Schornack’s comments highlighted the tensions endemic to the process of making the U.S.–Canada border visible. New technologies have come to play a complicated role in this post-9/11 context. Deemed essential to the fraught process of uncovering the material edge between the United States and Canada, these technologies introduce poorly understood ideological issues.

VI. BIOMETRICS AND BORDERING

In order to address both the physical difficulty of locating the border and the need to consider which bodies should be allowed and which denied access into the United States, innovative ways to make both Canada and Canadians newly visible needed to be identified. In this context, biometrics have risen to prominence in the post-9/11 spotlight. Biometric technologies have become an

23. Associated Press, “Canada–U.S. border obscure in places: Commission” (2006), http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060930/canada_us_border_060930?s_name=&no_ads=

24. Associated Press, “Canada–U.S. border obscure in places,” (n. 23).

25. Alberta, “Where, Oh Where Has the Border Gone?” (n. 21).

essential component of the identification and application of the U.S.–Canada border, represented as able to locate and enforce the border through the inspection and classification of individual bodies.

The first major indication that biometrics would become central to post-9/11 border management occurred shortly after the attacks in December 2001. At that time, the United States and Canada entered into the Smart Border Declaration and an accompanying 32-point Action Plan. Biometrics featured centrally in this post-9/11 border accord. The very first point of the Smart Border Declaration action plan concerned the use of biometric technologies:

#1 BIOMETRIC IDENTIFIERS

The United States and Canada have agreed to develop common standards for the biometrics that we use and have also agreed to adopt interoperable and compatible technology to read these biometrics. In the interest of having cards that could be used across different modes of travel, we have agreed to use cards that are capable of storing multiple biometrics.

The Smart Border Declaration has given rise to a number of subsequent border initiatives. Each of these initiatives has continued to feature biometrics as central to their security strategies. One example is the NEXUS-Air pass. The third point of the Smart Border Action Plan called for the development of a program designed to expedite “pre-approved, low-risk travelers” across the border.²⁶ NEXUS-Air was designed to allow precleared travelers to bypass scrutiny by customs agents so long as they agreed to have their identity verified by biometric iris scanners instead. The fourth point of the Smart Border Action Plan subsequently gave rise to a Statement of Mutual Understanding. This agreement harmonized the Canadian and U.S. processing of refugee and asylum claims. The “harmonization” is partially accomplished through the cross-border sharing of applicants’ biometric information, including both face- and fingerprints.²⁷

Biometric passports were also the subject of continuing discussion and development. Although the Smart Border Declaration had given rise to discussions concerning mandatory biometric travel documents for Canadians entering the United States, Canadian passport holders continued to be exempt from the 2004 U.S.-VISIT rules requiring biometric passports.²⁸ Changes resulting from the U.S.-sponsored Western Hemisphere Travel Initiative (WHTI) for the first time required both Canadians and Americans to present passports if they

26. Foreign Affairs and International Trade Canada, “Smart Border Action Plan Status Report,” (2004), <http://geo.international.gc.ca/can-am/main/border/status-en.asp>.

27. *Ibid.*

28. Passport Canada, “Biometrics in the International Travel Context” (2004), <http://www.pptc.gc.ca/newsroom/news.aspx?lang=e&page=/newsroom/20040201.aspx>.

wished to enter the United States, rather than other identifying documents such as driver's licenses. Further to the WHTI, those traveling by air or sea were required to present a passport by January 8, 2007, while those traveling across land borders were required to present a passport by December 31, 2007²⁹—a date that was deferred to June of 2009. It remains unclear when and how Canada will comply with the WHTI by developing biometric passports—although as early as 2005, Canada had commenced trials of biometric passports that contained digitized photos.

At the same time, the U.S. attempt to racialize risk through the biometric classification of Canadians can be noted in the advisory issued by Ottawa notifying Canadian residents born in Iran, Iraq, Libya, Sudan, and Syria that they must be biometrically fingerprinted at the U.S. border.³⁰ Although the United States retracted the decision to target these Canadians in particular, it reserved the right to interrogate Canadians depending on “where they had traveled and if they were traveling on another country's passport.”³¹

Given the number of border initiatives that rely on biometrics, their role in the reimagining of the post-9/11 U.S.–Canada border is significant. One example that well illustrates how biometric technologies facilitate the remaking of the northern boundary between the United States and Canada is their role in outsourcing the U.S.–Canada border away from the territorial edges of the state.

VII. OUTSOURCING THE BORDER

Biometrics are regularly identified as the most effective border technology. In large part, this is because Canada–U.S. border agreements discursively represent biometric technologies as able to fulfill one of the new features of a post-9/11 security environment—moving the border as far away from the edge of the nation-state as possible. In a 2005 report, the Canadian Senate Committee on National Security and Defense suggested that securing the border required that “threats” to Canadian security be identified as far away from North America as possible. This assertion was illustrated by the following diagram:

29. Krista Boa, “Biometric Passports: A response to the Western Hemisphere Travel Initiative?” (2006), http://www.anonequity.org/weblog/archives/2006/08/biometric_passports_a_response_1.php.

30. CBC News, “Some Canadians may be Photographed, Fingerprinted at U.S. Border” (October 30, 2002), <http://www.commondreams.org/headlines02/1031-08.htm>.

31. *Ibid.*

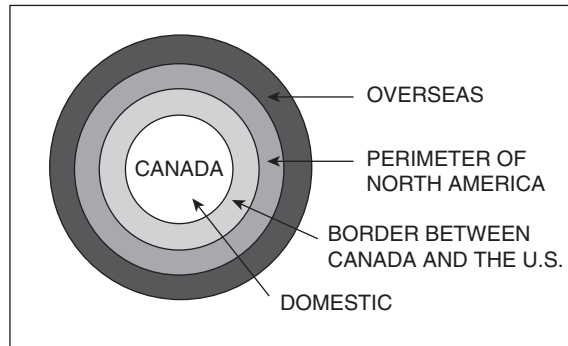


FIGURE 1. OUTSOURCING THE BORDER³²

The Senate Committee's recommendation and its recognition that, with the United States it securitize the broader entity of North America, is consistent with what Didier Bigo describes as state attempts to extend their spheres of control by delocalizing their borders.³³ Acting as a North American geopolitical entity, both Canada and the United States are attempting to "outsource" their borders. By "outsourcing the border," I am referring to specific techniques that a state may use to deterritorialize their boundaries. In the Statement of Mutual Understanding (2003) between the United States and Canada, the primary way to secure the state is described in the following way:

The best way to secure our borders is to identify and intercept persons posing security risks as early as possible, and as far away from our borders as possible.

Information sharing supports the Multiple Borders Strategy, which focuses control on measures overseas, where potential violators of citizenship or immigration laws are intercepted prior to their arrival to the United States or Canada.³⁴

Biometrics is one of the primary technologies used to achieve the out-sourcing of the border. This helps to explain the proliferation of biometrics programs used to test individuals before they leave their point of origin. As part of

32. Senate Committee on National Security and Defence, "Borderline Insecure: Canada's land border crossings are key to Canada security and prosperity. Why the lack of urgency to fix them? What will happen if we don't?" *An Interim Report by the Senate Committee on National Security and Defence* (June 2005).

33. Didier Bigo, "Security and Immigration: Toward a Critique of the Governmentality of Unease," *Alternatives* 27, no. 1 (2002).

34. Citizenship and Immigration Canada, "Statement of Mutual Understanding on Information Sharing" (2003), <http://www.cic.gc.ca/english/policy/smu/smu-ins-dos.html>.

Canada's \$3.5 million program to screen immigrants before they arrive on Canadian soil, the Canadian government is opening an office in Singapore to collect biometric information from immigration applicants. The biometric information will be used to determine "the identity of immigrants, although how this will be done is not clear."³⁵

Rather than continuing to understand the U.S.–Canada border as a one-dimensional dotted line along a surface, biometrics now are deployed discursively to represent the U.S.–Canada border in 3D, as "effective border management requires governments to treat the border as more than a single line at which threats can be intercepted."³⁶ In this way, the border is multiplied endlessly outward, replicating itself such that no one line may be identified. Thus, we understand that

Canada and the United States are pursuing a regional approach to migration based on the Multiple Borders Strategy. The Multiple Borders Strategy views the border not as a geo-political line but rather a continuum of checkpoints along a route of travel from the country of origin to Canada or the United States. At every checkpoint along the travel continuum—visa screening; airport check-in; points of embarkation; transit points; international airports and seaports; and the Canada–United States border—there is an opportunity for the participants to link the person and the document and any known intelligence.³⁷

This linking of "person and document" is facilitated through biometric inspection.

Moreover, the U.S.–Canada border is not only outsourced to other nation-states in order to prescreen "risky travelers." New technologies additionally are deployed to "insource" the U.S.–Canada boundary onto Canadian territory. The Smart Border Declaration declared that most major Canadian airports—including those in Vancouver, Edmonton, Calgary, Winnipeg, Toronto, Ottawa, and Montreal—would now have U.S. customs screening located in Canada rather than in the United States, precluding the admission of those deemed dangerous rather than requiring their expulsion.³⁸ As biometric passports are implemented, the screening of travelers to the United States will be outsourced to Canada so that the traveler's biometric identity will be determined before they cross the U.S. border.

35. Canadian Biometric ID Documents Public Forum, "FAQ" (2006), <http://www.ferenbok.com/biometricIDforum/webcast.html>.

36. Government of Canada, "Securing an Open Society," 41 (n. 2).

37. Citizenship and Immigration Canada, "Statement of Mutual Understanding on Information Sharing," (n. 34).

38. Foreign Affairs and International Trade Canada, "Smart Border Action Plan Status Report," (n. 26).

Biometrics thus are central to the outsourcing of the U.S. border as they allow it to be exported. What formerly was understood to be just “a coastline, or a line on the ground between two nations” is now understood to be composed of the individual “bordered” bodies that make up the “line of information in a computer, telling us who is in this country, for how long, and for what reason.”³⁹

VIII. BIOMETRIC FAILURE

Despite the growth in reliance on biometric technologies in a climate of particular attention to race, ethnicity, and religious identification, biometrics often are described as technologies able to provide both “mechanical objectivity”⁴⁰ and race-neutrality. The claim that biometrics can automate inspection suggests that these technologies are able to replace the subjective eye of the customs inspector with the neutral eye of the scanner. In this way, biometric technologies are represented as able to circumvent racism—imagining the Canada–U.S. border as a race-neutral space. Biometric technologies are held up as bias-free technologies that will objectively and equally scan everyone’s bodily identity. The director of corporate communications for Visionics, a leading U.S. manufacturer of biometrics systems, asserted that the corporation’s newly patented iris scanning technology “is neutral to race and color, as it is based on facial features recognized by the software.”⁴¹ This understanding finds more than a little resonance in public opinion. In an online discussion surrounding the implementation of iris scanners at the U.S.–Canada border, one respondent claimed he would much prefer to present himself to “race-neutral” biometric technologies than to potentially racist customs border officials:

If I was a member of one of the oft-“profiled” minorities, I’d sign up for sure. Upside—you can walk right past the bonehead looking for the bomb under your shirt just because of your tan and beard . . . In short, I’d rather leave it up to a device that can distinguish my iris from a terrorist’s, than some bigoted lout who can’t distinguish my skin, clothing or accent from same.⁴²

Biometrics are being mustered in the fight to identify suspect Canadian bodies at the border, a deeply problematic task. It is not surprising, therefore,

39. Citizenship and Immigration Canada, “Statement of Mutual Understanding on Information Sharing,” (n. 34).

40. I take this phrase from Peter Daston and Lorraine Galison, “The Image of Objectivity,” *Representations* 40 (1992).

41. Zelazny cited in Saumya Roy, “Biometrics: Security Boon or Busting Privacy?” *PC World*, 32 no. 4 (2002).

42. “Airport Starts Using Iris Screener” (2005), <http://www.vivelecanada.ca/article.php/20050715193518919>.

that when biometric technologies are used to accomplish this task they fail easily and often. What is most interesting about biometric failures are the specific ways in which they do not work. As biometrics are deployed to make Canadian bodies visible, they regularly break down at the location of the intersection of the body's class, race, gender, and dis/abled identity. In this way, biometrics fail precisely at the task that they have been set—to identify newly othered bodies.

As biometric technologies are developed in a climate of increased anxiety concerning suspect bodies, stereotypes around “inscrutable” racialized bodies are technologized. That is, biometric technologies consistently are unable to distinguish the bodies of persons of color. For example, research on the use of biometric fingerprint scanners resulted in the conclusion that some “Asian women . . . had skin so fine it couldn't reliably be used to record or verify a fingerprint.”⁴³ Tests of biometric iris scanners also have revealed that they perform differently on racialized bodies. In some cases, it seemed as if W. E. B. Dubois's “color line” was being technologized: the darker the skin color, the greater the likelihood of technological failure.

Answering a question on whether it regarded the rates (of failure) as satisfactory, the Home Office replied: “It is true to say that at times in the past some difficulties have been experienced in successfully recording the iris images of people with very dark skin (on some iris systems). The difficulty lay in the ability of the system to successfully locate irises against a darker skin tone.”⁴⁴

John Daugman is the scientist who invented the mathematical algorithms upon which all iris scanning technologies depend. He consistently has found that these technologies perform differently on brown and black eyes than they do on blue, green, or hazel eyes—a problematic finding given the connection of eye color to racialization. These biometric failures result, in part, from their reliance on outdated and erroneous biological understandings of race. There are a multitude of biometric studies that assume that the faces of different “races” will give rise to clear and different (race specific) biometric scans. One example is the troublingly titled study “Facial Pose Estimation Based on the Mongolian Race's Feature Characteristic.”⁴⁵ The suggestion underlying this biometric identification technology—that race is a stable, biological entity that reliably yields common measurable characteristics—is deeply problematic. Such conclusions are repeated in a number of articles that claim to classify “faces on the basis of

43. W. Sturgeon, “Law & Policy Cheat Sheet: Biometrics” (2004), <http://management.silicon.com/government/0,39024677,39120120,00.htm>.

44. Kahlenet, “More Accurate on the Eye,” *The Register* (2006), http://www.theregister.co.uk/2006/04/05/iris_scan_tech_improving/.

45. Yadong Li, Ardeshir Goshtasby, and Oscar Garcia. “Detecting and Tracking Human Faces in Videos,” *IEEE* (2000): 807–810.

high-level attributes, such as sex, ‘race’ and expression.”⁴⁶ Although the scare quotes around the word “race” would suggest that the authors acknowledge that race is not biological, they still proceed to program the computer to identify both gender and race as if it were so. This task is accomplished by scanning a facial image, and then identifying the gender and race identity of the image for the purposes of programming the computer, until they claim the computer is able to classify the faces itself. Not surprisingly, error rates remain high. Neither gender nor race is a stable category that consistently may be identified by the human eye, nor by computer imaging processes. Thus, much of the scientific research underlying biometrics serves as a disturbing reminder of the racial science that provided the foundations of earlier identification technologies including the passbook system used under apartheid in South Africa.⁴⁷

These assumptions concerning the dependence of biometric performance on racial and ethnic identity can also be noted in the locational differences in hypotheses around race and biometrics that are specific to the site of several of the studies. In the United States, biometric technologies failed to distinguish “Asian” bodies. In the United Kingdom, biometric technologies had difficulty distinguishing “black” bodies. In Japan, one study posited that it would be most difficult for biometrics to identify “non-Japanese” faces, beginning with the premise that race is biological and that there may be an “other race effect”: “[M]ost people report finding it difficult to recognize the faces of people of other races.” Asserting that there were few mixed-race individuals in Japan, the author concluded that facial recognition technology could distinguish more reliably between “Japanese” faces than between “non-Japanese” faces.⁴⁸

Nor does the technological fallibility of biometrics end with hi-tech racism. Biometric technologies consistently were unable to identify those who deviated from the “norm” of the young, able-bodied male. In general, studies showed that “one-size-fits-all” biometrics technologies did not work. For example, biometric facial recognition technology was shown to work poorly with elderly persons and failed more than half the time in identifying those

46. Michael J. Lyons, Julien Budynek, Andre Plante, and Shigeru Akamatsum, “Classifying Facial Attributes using a 2-D Gabor Wavelet Representation and Discriminant Analysis,” *Fourth IEEE International Conference on Automatic Face and Gesture Recognition* (2000).

47. In their book *Sorting Things Out* (1999), Leigh Star and Geoff Bowker document the impossibility of classifying race given its socially constructed nature through their analysis of the race-based passbook system in South Africa.

48. Kenichi Tanaka, Kazuyuki Machida, Shingo Matsuura, and Shigeru Akamatsu, “Comparison of Racial Effect in Face Identification Systems based on Eigenface and Gaborjet,” *SICE Annual Conference in Sapporo* (2004).

who were disabled.⁴⁹ Other studies on biometric iris scanners showed that the technologies were particularly bad at identifying those with visual impairments and those who are wheelchair users.⁵⁰ New demands for biometric forms of identification served to manipulate and extend the definition of disability. Thus, those who had rare skin diseases such that they did not have fingerprints became the newly disabled. In California, an individual teacher was unable to work because he could not be fingerprinted.⁵¹

Class also became a factor. Those persons with occupations within the categories “clerical, manual, [and] maintenance” were found to be difficult to biometrically fingerprint.⁵² Biometric iris scanners failed to work with very tall persons,⁵³ and biometric fingerprint scanners could not identify 20% of those who have nonnormative fingers: “One out of five people failed the fingerprint test because the scanner was ‘too small to scan a sufficient area of fingerprint from participants with large fingers.’”⁵⁴ Any kind of bodily breakdown could give rise to biometric failure. “Worn down or sticky fingertips for fingerprints, medicine intake in iris identification (atropine), hoarseness in voice recognition, or a broken arm for signature” all gave rise to temporary biometric failures while “[w]ell-known permanent failures are, for example, cataracts, which makes retina identification impossible or [as we saw] rare skin diseases, which permanently destroy a fingerprint.”⁵⁵

Moreover, in addition to having technologized problematic assumptions around the comprehensibility of difference, biometric technologies discursively are deployed in ways that continued to target specific demographics of suspect bodies. For example, biometric facial recognition technology requires Muslim women who wear the hijab to remove it in order to receive new forms of ID cards, where older forms of identification such as the photos on driver’s licenses only required their partial removal.⁵⁶ In this way, biometric technologies are

49. “Black Eye for ID Cards,” (2005), <http://www.blink.org.uk/pdescription.asp?key=7477&grp=21&cat=99>; BBC News, “ID cards scheme dubbed ‘a farce’” (October 17, 2005).

50. Karen Gomm, “U.K. Agency: Iris recognition needs work,” News.com, (October 20, 2005).

51. David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (New York: Routledge, 2003).

52. UK Biometrics Working Group, “Biometrics for Identification and Authentication - Advice on Product Selection” (2001), <http://www.idsysgroup.com/ftp/Biometrics%20Advice.pdf>.

53. Gomm, “U.K. Agency: Iris recognition needs work” (October 20, 2005).

54. “Black Eye’ for ID Cards,” (n. 49).

55. Bioidentification, “Biometrics: Frequently asked questions,” (2007), <http://www.bromba.com/faq/biofaq.htm>.

56. “ID Card and You” (2004), <http://www.idcardandyou.co.uk/racism.html>.

literally deployed to further the invasion by the state of the bodily privacy of Muslim women.

Given the specific anxieties that biometric technologies are discursively represented as able to allay, their failure rates are not surprising. Significant failures of the technology have occurred in Virginia Beach and Tampa, Florida.⁵⁷ In Florida, the biometrics system was eventually abandoned altogether due to its failure to identify even one person correctly.⁵⁸ In a test of facial recognition technology at Logan Airport in Boston, biometric technology worked only 50% of the time in situations of compromised lighting.⁵⁹ As it is unlikely that terrorists would stop to pose for well-lit photographs, this is a serious failing. The ease with which hi-tech biometric technologies can be hacked also calls their security into question. Researchers at Yokohama National University revealed that biometric fingerprint readers can easily be deceived by artificial gelatin fingers onto which a real print from either an actual finger or from another surface such as glass had been dusted.⁶⁰ This ease of falsely replicating fingerprints was confirmed by Marie Sandström in her 2004 Master's thesis in which she tested nine different fingerprint recognition systems and found that all could be deceived by an artificial gelatin imprint. In Germany, a community of hackers called the Chaos Communication Camp gathered to figure out how to hack the new technologies. The many ways in which they were able to hack biometric information further emphasized biometric fallibility. In a 2007 presentation at a biometric industry conference, Samir Nanavati of the International Biometrics Group asserted that spoofs of biometric technologies generally have been ignored, and then proceeded to demonstrate a number of techniques that continue to work to violate the security of biometric identification technologies.

The inaccuracies, misplaced and racist assumptions, and easy penetrability of biometric technologies seriously calls into question their use in the definition of the U.S.–Canada border, as well as their reliability in distinguishing and identifying those bodies entitled to pass through the border from those threatening or otherwise inappropriate bodies who must be excluded. Biometric technologies are being used to discursively construct new categories based on

57. Kelly Gates, "Our Biometric Future: The social construction of an emerging information technology," PhD Thesis, Institute of Communications Research, Urbana-Champaign, University of Illinois at Urbana-Champaign (2004).

58. *Ibid.*

59. ACLU, "Three Cities Offer Latest Proof That Face Recognition Doesn't Work, ACLU Says" (2003), <http://www.aclu.org/privacy/spying/14872prs20030902.html>.

60. T. Matsumoto and H. Matsumoto, "Impact of Artificial Gummy Fingers on Fingerprint Systems," *Proceedings of SPIE - Optical Security and Counterfeit Deterrence Techniques IV* (2002).

biometricability—categories that have significant consequences for personal mobility, and ones that mimic imaginary racial categories.

IX. CONCLUSION

As previously noted, the boundary separating Canada from the United States is regularly described as the longest, undefended border in the world. However, the relationship between the two countries historically has not been free from stress. Moreover, although the border between Canada and the United States was described as separating “special friends” in the years leading up to September 11, 2001, this friendship underwent a shift after the attacks on the Pentagon and World Trade Center. In particular, the persistence of the rumor that the hijackers responsible for the attacks came from Canada made evident the post-9/11 shift to representing this border as newly porous—leaking suspect threats from north to south. Through the inaccurate connection between terrorist threats and Canada’s supposedly “permissive” immigration and refugee policy, Canadian bodies were rendered newly dangerous. As a result, technologies able to visualize these threats and to distinguish them from the bodies of Americans were needed.

Biometric technologies drew increased attention in the post-9/11 political environment. Represented as able to identify newly threatening bodies and thus to allow for their exclusion, biometrics were identified as the leading border technology in all of the border accords signed after September 11, 2001. Biometric technologies also were represented as able to meet new needs to move the border away from the material edge of the United States—to “outsource” the border. In doing so, biometrics were deemed central to the process of identifying Canadians, as they were imagined to be able to visualize newly suspect Canadian bodies. In this way, biometric technologies are key to contemporary projects of identification—a bureaucratic process central to the modern state. As both Canada and the United States try to determine who belongs to the state and who must be expelled, biometric technologies are mustered as one of the tools allowing the state to make bodies legible to state institutions. In this way, the biometric inspection becomes a ritual of identification key to contemporary rationalities of governing.

The use of biometric identification technologies at the U.S.–Canada border has been shaped by a discourse of technological neutrality and efficiency. This narrative of efficiency and security needs to be interrogated given the ways in which it allows for and encourages the scrutiny of certain bodies, particularly immigrants and refugees, at the same time as it eases the passage of others. Although the biometric industry claims that these new technological tools are identity-neutral, we must call these claims into question

as biometric technologies depend upon the classification of race, class, and gender identities in order to function. Given the reliance of biometric technologies on outdated, biological understandings of race, the objectivity and race-neutrality of biometrics must be interrogated and their widespread use at the U.S.–Canada border reconsidered. A new narrative is needed that works to identify the border in ways that are not based on principles of exclusion or claims to “mechanical objectivity.” Rather, we need policies based on principles of inclusiveness and which facilitate substantive claims to equality at the U.S.–Canada border.