3

Unsafe at Any Altitude

The Comparative Politics of No-Fly Lists in the United States and Canada

Colin J. Bennett

I know everybody's income and what
everybody earns,
And I carefully compare it with the
income-tax returns;
But to benefit humanity, however
much I plan,
Yet everybody says I'm such a
disagreeable man!
And I can't think why!

—King Gama in *Princess Ida*,
Gilbert and Sullivan

As some day it may happen that a
victim must be found,
I've got a little list—I've got a little list
Of society offenders who might well
be underground,
And who never would be missed—
who never would be missed! . . .
The task of filling up the blanks I'd
rather leave to you.
But it really doesn't matter whom
you put upon the list,
For they'd none of 'em be missed—
they'd none of 'em be missed!

—Koko in *The Mikado*,
Gilbert and Sullivan[1]

Gilbert and Sullivan would no doubt have found great satirical humor in the various attempts of governments to keep tabs on their citizens in the early twenty-first century. Each of these quotations implies an opposing theory about the motivations for surveillance. The chilling implications of the Lord High Executioner's "little list" is contrasted with the well-meaning attempts of King Gama to "benefit humanity" by correcting his "erring fellow creatures."[2] The arbitrariness of the former is contrasted with the meticulous and systematic approach of the latter. The motivations behind the "little lists" are justified to find scapegoats, whereas those of the King Gama are prompted by public purpose. One sees no need to justify his surveillance; whereas, the other, of course, does.

We supposedly now have more sophisticated models of surveillance that do not rely on assumptions about the arbitrary whims of tyrants or philanthropists. The little lists are now not so little, and they are generated by a variety of bureaucratic motives and technological imperatives. The comparison of data from different sources (such as earnings and income-tax returns) is now routinized, as we leave traces of personal information behind us when we engage in the normal transactions of modern society. Contemporary surveillance does not rely on the venal whims of a Lord High Executioner or the benign motives of the philanthropist, but even so, the collection and analysis of personal information is a structural condition of modernity.[3]

Even though the increasing securitization of airline travel is explained by trends and measures put in place well before the attacks of September 11, 2001, there is no question that those events have accelerated the development of a range of measures in different countries and different airports: new forms of biometric identification, secure cockpit doors, the increased sharing of advanced passenger-information data, trusted traveler programs, and so on. However, the success of many of these measures does, to a large extent, rely on the identification of a group of individuals (e.g., "terrorists") who pose a threat to airline safety and who should be the subject of extra precautionary measures before they are allowed to board an aircraft. The "lists" thus generated are the focus of this chapter.

It is commonly assumed that airlines have always held information on "problem travelers"—the person caught smoking in the toilet, the tedious alcoholic who harasses the flight attendant, the recalcitrant passenger who refuses to obey the seat belt signs, and so on. But practices have varied considerably, and the names were not necessarily centrally stored and disseminated as they are today. The generation of "no-fly lists" as a public-policy measure is a more recent development and needs to be understood in the context of larger systems for the prescreening of airline passengers, such as the Computer Assisted Passenger Profiling Systems (CAPPS), Secure Flight, and the Automated Targeting System (ATS) in the United States and Passenger Protect in Canada. This chapter begins with an overview and comparison of these programs and then analyzes what we do and do not know about how "no-fly lists" are generated and deployed in both countries, and how they have been resisted.

These lists should be regarded not only as tools of surveillance but as "policy instruments," as one, among many, "tools of government" that might be deployed to address a commonly perceived problem.[4] Prescreening airline passengers against a prior "list" is one of several instruments used to prosecute the "war on terror."[5] The extent, level, type, and distribution of surveillance practices are not only dependent on legal and regulatory measures, nor on high-level sociological theory about technology, bureaucracy, modernity, and so on, but rather on the "structural configurations of states," which structure policy outcomes in path-dependent ways.[6] This approach is rooted in political science rather than in law and sociology. It has been termed "neo-institutionalist" and can help us to understand different patterns of surveillance in similar jurisdictions.[7] This chapter concludes with an interrogation of no-fly lists as policy instruments, as well as with some critical commentary on surveillance studies.

Systems for Airline Passenger Prescreening

Ten years ago, little attention was paid to privacy issues in the airline industry or the airport environment, and it was difficult to find interested or

expert officials within the airlines, or their regulatory agencies, who could provide accurate descriptions of the personal-data processing practices of the industry. Since September 11, 2001, the interrelated questions of who travels by air, who gets to see who travels by air, and who gets to prevent people from traveling by air have been brought sharply into focus. These questions have become some of the most important in contemporary studies of privacy and surveillance.

Computer Assisted Passenger Profiling System (CAPPS)

On September 11, 2001, the nineteen hijackers were screened prior to boarding their flights against a Computer Assisted Passenger Profiling System (CAPPS), which had been in place since the early 1990s. More than half of them were identified for further inspection, but only their bags were inspected. At that time, the program was implemented in a decentralized fashion by the airlines themselves. Security concerns constrained the U.S. government from listing all potential terrorist suspects or delivering that list to the airlines.[8] This colossal security failure explains a great deal about subsequent responses in both the United States and Canada.

In January 2003, the Transportation Security Administration (TSA) published a *Federal Register* notice announcing CAPPS II and a new Aviation Security Screening Records (ASSR) database.[9] The *Federal Register* notice described a system that would allow the government access to "financial and transactional data" as well as virtually unlimited amounts of data from other proprietary and public sources. The TSA also indicated that many private and public entities might gain access to the personal information used in the ASSR database. This second-generation system was to be centrally coordinated through the TSA and to apply to all flights to, from, and within the United States.

The proposal was met with almost uniform criticism from a range of groups.[10] In response, TSA officials clarified that the basic elements of CAPPS II would be confined to the routine information collected at the time of reservation and included in the Passenger Name Record (PNR): a passenger's full name, home address, home telephone number, and date of birth, as well as that passenger's itinerary.[11] In an effort to verify the traveler's identity, that information would then be checked against credit information and other data held by various private corporations that maintain files on the commercial activities of most American citizens. CAPPS II would then conduct a check against government databases (including intelligence and law-enforcement databases) to assign a risk assessment score to each passenger: green for minimal, yellow to spark heightened security procedures, and red for those "high risk" passengers judged to pose an acute danger and who

should be referred to law enforcement. It was anticipated that the number of passengers so identified as high risk would be extremely small but critically significant in the context of homeland security.

The TSA would also delete all records of travel for U.S. citizens and lawful permanent-resident aliens no more than a certain number of days after the safe completion of their travel itineraries, though it gave no similar commitment about non-U.S. citizens. The assurances about more-limited data retention, as well as about procedures to challenge their own risk assessments, did little to quell the criticism of this program. As the Electronic Frontier Foundation (EFF) put it, "the good news is TSA does not plan to retain data on individuals. The bad news is that CAPPS II puts the riskiest element of the program—the determination of risk and the construction of rules for conducting background checks—into the realm of the more secretive intelligence and law enforcement programs and databases."[12]

This entire system relied, of course, on obtaining the PNR data from the airlines and the Global Distribution Systems (GDS), reservation systems such as Galileo and Sabre.[13] To this end, the TSA announced that it would conduct a pilot project with Delta Air Lines in three midsize airports in the spring of 2003. However, Delta Air Lines, after strong public opposition, decided not to provide its passengers' data. There was a more serious scandal over the revelation that JetBlue had provided five million passenger records to a defense contractor, in what was reported as an underhand transfer of data for the testing of the CAPPS II profiling system.[14] It was later revealed to the Senate Governmental Affairs Committee by Acting TSA administrator David Stone that Delta, Continental, America West, JetBlue, and Frontier Airlines, as well as the major GDSs, had all disclosed passenger records to the TSA's contractors in 2002 to test CAPPS II.[15]

Pressure also came from Congress. In September 2003, the conference committee responsible for reconciling the Department of Homeland Security (DHS) appropriations for the next fiscal year decided to put the program on hold until the U.S. Government Accountability Office (GAO) had an opportunity to report on the effectiveness and fairness of the system. Analysis by the GAO culminated in a report that indicated that the TSA had failed to address most of the originally identified issues of concern. It recommended a number of actions, including a "risk mitigation strategy."[16] The American Civil Liberties Union (ACLU) summed up seven reasons why the CAPPS II should be abandoned: (1)the secret nature of the risk analysis; (2) the absence of an increase in safety; (3) the possibility of mission creep; (4) the lack of notification, correction, or appeal; (5) the possibility of enabling the building of lifetime travel dossiers; (6) the unnecessary burden; and (7) the discriminatory impact.[17]

Under the weight of an enormous volume of criticism, Tom Ridge, the Secretary of Homeland Security, declared CAPPS II "dead" in July 2004, a statement that raised a series of further questions about what would happen to the millions of records already collected. At the same time, the Report of the 9/11 Commission strongly advocated a centrally coordinated screening system:

> Improved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by the TSA, and it should utilize the larger set of watchlists maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system.[18]

Shortly thereafter, Congress passed the Intelligence Reform and Terrorism Prevention Act, which directed the DHS to "commence testing of an advanced passenger pre-screening system that will allow the Department of Homeland Security to assume the performance of comparing passenger information . . . to the automatic selectee and no-fly lists."[19]

Secure Flight

In August 2004 the TSA announced that the successor would be named "Secure Flight" and published a federal register notice indicating that it was to set up a new system of records pursuant to the Privacy Act in order to create this program. It also issued an emergency notice ordering airlines to divulge by October 29, 2004, details of all passengers who had flown domestically during the month of June 2004. The airlines initially questioned the order because of concerns about privacy, but in the end all seventy-two airlines complied and the details of around forty-two thousand passengers were transferred. At a minimum, they were to divulge the passenger's name, reservation date, travel agent, itinerary information, form of payment, flight number, and seating information—in other words, the basic information on the PNR. At that time, it was unclear whether the GDSs were also expected to cooperate.

According to the TSA, Secure Flight was to meet the following goals: identifying, in advance of flight, passengers known or suspected of being engaged in terrorist activity; moving passengers through airport screening more quickly and reducing the number of individuals unnecessarily selected for secondary screening; and fully protecting passengers' privacy and civil liberties. This notice went on to explain that the PNR data was to

be compared against the existing Terrorist Screening Database, maintained by the Terrorist Screening Center. Secure Flight was to automate the watch-list comparisons and allow for more "consistent response provisions."[20] The tests were designed to verify that Secure Flight was able to match and authenticate information on air travelers with records stored in government databases and with data purchased from unspecified commercial data aggregators.

It appeared at the time that the major difference between Secure Flight and its predecessors was the abandonment of any predictive computer algorithms designed to profile travel behavior that might be linked to suspicions of terrorism (e.g., buying a one-way ticket in cash). Also, the new system was only to look for known or suspected terrorists, not other law-enforcement violators. In addition, it was to include a redress mechanism, where people could resolve questions if they believed that they had been unfairly or incorrectly selected for additional screening. It was reported that the CAPPS system (at least in 2004) screened about one out of every six air passengers. Secure Flight was supposed to cut the number down drastically.

In the 2005 Appropriations process for the DHS, Congress mandated the GAO to audit the program and in particular to assess the effectiveness of using commercial data for prescreening efforts. The GAO produced a series of reports in February, March, and July of 2005 and recommended a number of measures to reduce the risk of error and to improve procedures by which individuals could mount challenges. They also found that the TSA was less than forthcoming about the purposes of collection in its original Privacy Act Notice.[21] Critical reports were also issued by the "Secure Flight Working Group," the Department of Justice Office of the Inspector General, and the House Select Committee on Homeland Security.

While conceding that Secure Flight was an improvement on CAPPS or the proposed CAPPS II, groups such as the ACLU, the Electronic Privacy Information Center (EPIC), and the EFF also maintained consistent pressure, submitting evidence, making Freedom of Information Act (FOIA) requests for DHS documents as well as assisting individuals who had been wrongfully selected for screening. There was also use of the Privacy Act to obtain records sent to the TSA by the airlines during the testing phase. An initial request by four Alaskan citizens for any PNR data held by the TSA set in motion a lengthy process of stonewalling, confused messages about the destruction of the data, as well as an amendment to the original Privacy Act notice.[22] In August 2005 the EFF put out "an action alert" urging members of the public to request the information collected about themselves by the TSA under the Privacy and Freedom of Information Acts. The EFF asked inquirers to request that all commercial data be preserved from deletion for closer examination.[23] The TSA was thus flooded with requests. The agency

responded that they did not have the "capability to perform a simple computer based search to locate any responsive records."[24]

The Secure Flight program was originally planned to be implemented in September 2005. In February 2006 it was subjected to further criticisms from the GAO, which reported that the program fell short in protecting security and privacy, and that it was seriously in jeopardy of not meeting its stated goals.[25] At a subsequent set of hearings from the Senate Committee on Commerce, the head of the TSA, Kip Hawley, announced that the Secure Flight program would be suspended pending a comprehensive security audit: "We will move forward with the Secure Flight program as expeditiously as possible, but in view of our need to establish trust with all of our stakeholders on the security and privacy of our systems and data, my priority is to ensure that we do it right . . . not just that we do it quickly."[26] A year later it was reported that the implementation of Secure Flight would be delayed until 2010.[27]

The Automated Targeting System

By 2007, however, another system, the Automated Targeting System (ATS), arose to the attention of the media and civil-liberties advocates. The ATS is a system designed for the screening of cargo coming into the United States. Somewhere in the depths of the DHS, someone had the idea to use these existing screening programs and risk-assessment methodologies for passengers as well. We do not know when this screening started, or how many individuals have been affected. The only public acknowledgment of this system appeared in the routine Privacy Act Notice, published in November 2006, which stated the following:

> The risk assessment and links to information upon which the assessment is based, which are stored in the Automated Targeting System, are created from existing information in a number of sources including, but not limited to: the trade community through the Automated Commercial System or its successor; the Automated Commercial Environment system; the traveling public through information submitted by their carrier to the Advance Passenger Information System; persons crossing the United States land border by automobile or on foot; the Treasury Enforcement Communications System, or its successor; or law enforcement information maintained in other parts of the Treasury Enforcement Communications System that pertain to persons, goods, or conveyances. As part of the information it accesses for screening, Passenger Name Record (PNR) information, which is currently collected pursuant to an existing CBP regulation (19 CFR 122.49d) from both inbound and outbound travelers through the carrier upon which travel occurs, is stored in the Automated Targeting System.[28]

The notice went on to declare that "as noted above, this system of records notice does not identify or create any new collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems."[29] Subsequently, the DHS published a Privacy Impact Assessment (PIA), which described the extent of the planned system and confirmed that "every traveler and all shipments are processed through ATS, and are subject to a real-time rule based evaluation. ATS provides equitable treatment for all individuals in developing any individual's risk assessment score."[30] These risk assessments are to be maintained for up to forty years.

These announcements raised suspicions that the ATS had been in existence for a number of years, without appropriate congressional approval, and that CAPPS and Secure Flight were perhaps distractions from the real surveillance that was going on. The response from civil liberties and privacy advocates was angry and swift. The EFF pointed out that the ATS

> will create and assign "risk assessments" to tens of millions of citizens as they enter and leave the country. Individuals will have no way to access information about their "risk assessment" scores or to correct any false information about them. But once the assessment is made, the government will retain the information for [forty] years—as well as make it available to untold numbers of federal, state, local, and foreign agencies in addition to contractors, grantees, consultants, and others.[31]

The EFF filed an FOIA suit against the DHS to extract more details on the program. The EPIC, writing on behalf of thirty organizations and sixteen experts, regarded the ATS as a secret government program in clear violation of the Privacy Act and another example of "mission creep."[32] The ACLU contended that the ATS "subverts the Fourth Amendment by allowing DHS to create a dossier on every American Traveler. In short, this program turns every American traveler into a criminal and terrorist suspect."[33] Security expert, Bruce Schneier, pronounced it a complete waste of money: "The idea of feeding a limited set of characteristics into a computer, which then somehow divines a person's terrorist leanings, is farcical. Uncovering terrorist plots requires intelligence and investigation, not large-scale processing of everyone."[34]

As of the summer of 2007 outsiders are hoping that the various congressional investigations, and mainly that of the Senate Judiciary Committee, will shed light on the operation of the ATS and determine its legality. The announcement also reignited a long-standing dispute with the European Union concerning the circumstances under which PNR data on European travelers could be stored in the United States and accessed by law-enforcement

agencies. In the absence of adequate privacy-protection laws in the United States, and of an equivalent supervisory authority, European data-protection officials have insisted on some degree of oversight in the processing of PNR data in the United States.

Passenger Protect

Canadian policy on airline and passenger security has been inextricably linked to that of the United States because a very large proportion of flights to and from Canadian destinations intrude upon U.S. airspace. Furthermore, the U.S. government has required all airlines flying over American soil either to turn over the names of all passengers on board within fifteen minutes of take-off or to check those names against U.S. government watch-lists in an effort to prevent terrorists from entering U.S. airspace. Both options, handing over passenger rosters or checking those names against the U.S. lists, were considered unacceptable to the Canadian government. Checking the names against a more precise and "Canadian-made" list was regarded as a more palatable alternative. That decision set in motion a series of policy events, which, as in the United States, are still in flux and still very controversial.

The legislative history begins with the Public Safety Act, 2002, which received Royal Assent on May 6, 2004. This law made changes to the Aeronautics Act, under which the Canadian government has the authority to request and evaluate information about airline passengers. Section 4.76 authorizes the prime minister to respond to immediate threats to aviation security. Section 4.81 authorizes the prime minister to require the submission of passenger information from air carriers for security purposes. Together these sections have been read as giving Transport Canada, Canada's federal transportation ministry, the authority to create a list of persons who may pose an "immediate threat to aviation security."[35] Section 4.82 of the Aeronautics Act authorizes Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS) officials to access air-passenger information and match it against information under their control in order to identify threats to transportation and national security.

Thus, Section 4.81 is seen as an initial step in passenger assessment that will establish a list of persons who pose an immediate threat to aviation security, against which airlines can check their passengers. Section 4.82 is intended to build on section 4.81 by allowing for a more-advanced technological approach to passenger assessment. Since the summer of 2005, the government has proceeded on a two-track approach to implement sections 4.81 and 4.82. The 2005 budget allocated $16 million over 5 years for the

assessment and development of systems to collect information about passengers to enhance transportation security.

The first official acknowledgment that a Canadian no-fly list was being developed came in August 2005:

> Beginning in August 2005, Transport Canada will consult with the Privacy Commissioner, airlines and other stakeholders on the implementation of a passenger assessment program, known as Passenger Protect. Under the program, the Government of Canada will create a list of individuals who pose an immediate threat to aviation security and who will be prevented from boarding aircraft. The program, targeted for implementation in 2006, will lay the foundation for future passenger assessment initiatives and allow airlines to provide information on individuals on this list to the federal government.[36]

Under section 4.82, Public Safety and Emergency Preparedness Canada (PSEPC) was also supposed to commission an independent feasibility study on the implementation of the "automated passenger assessment system."

In July 2006 Jennifer Stoddart, the Privacy Commissioner of Canada, sent a list of twenty-four questions to Transport Canada about the operation of this program.[37] In a press release two days after the announcement, she stated that the no-fly list "represents a serious incursion into the rights of travelers in Canada, rights of privacy and rights of freedom of movement." She complained that she had not received any in-depth briefing on the project nor any assurance that a Privacy Impact Assessment (PIA), addressing her questions, would be forthcoming.[38] The British Columbia Civil Liberties Association (BCCLA) also weighed in with complaints about the lack of consultation and a reminder of the many problems encountered with similar programs in the United States.[39]

Based on a leaked internal focus-group study, an article by Jim Bronskill reported that Canadians were much divided on the value of such lists, and that many reported difficulty in understanding how the prescreening process would work and how the list would be constructed according to what criteria. The study reported that the government was thinking very seriously about an appropriate redress mechanism for those mistakenly included on the list.[40] The same journalist also reported that Canadian Airlines had been using the larger and more cumbersome U.S. version, even though there was no requirement under Canadian law to do so. The result has been complaints from forty to fifty Canadians who were denied boarding on the basis of a match against the U.S. list.[41] A further development was the suspicion that the sharing of these lists with the U.S. government led to the wrongful apprehension of Maher Arar in New York and his subsequent

deportation to Syria.[42] Therefore, when the government eventually announced the no-fly list in late 2006, a good deal of skepticism was already in the air.

Nonflyers, Selectees, Specified Persons, and "Derogs"

So what are "no-fly" lists and how are these instruments being implemented in the United States and Canada? The first watch-lists in the United States go back at least as far as 1990. This mandate was provided under the Aviation Security Improvement Act of 1990 (P.L. 101-604), which required "the agencies of the intelligence community [to] . . . ensure that intelligence reports concerning international terrorism are made available . . . to . . . the Department of Transportation and the Federal Aviation Administration [FAA]." The agencies responsible for producing most of the intelligence on terrorism are the Central Intelligence Agency (CIA), the Department of State (DOS), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA). Between 1990 and 2001, the FAA issued several security directives and companion emergency amendments that identified persons whom carriers could not transport because they posed a threat to civil aviation. On September 11, 2001, only three of these directives were in effect.[43]

After 9/11 there have been several initiatives to try to coordinate the development, updating, and dissemination of these lists.[44] The broadest, and least exclusive, database of terrorist identities is called the Terrorist Identities Datamart Environment (TIDE). The TIDE database includes "all information the U.S. government possesses related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of purely domestic terrorism information."[45] Entries in the TIDE database might stem from a variety of sources within the federal government but are primarily the result of derogatory nominations ("derogs") submitted by the FBI, CIA, and the newly created Office of the Director of National Intelligence (ODNI).

These entries are then reviewed by the Terrorist Screening Center (TSC) at the FBI to determine whether they meet the criteria to be included within the Terrorist Screening Database (TSDB) described as follows:

> Under Homeland Security Presidential Directive (HSPD) 6, the TSC now provides "one-stop shopping" so that every government screener is using the same terrorist watchlist—whether it is an airport screener, an embassy official issuing visas overseas, or a state or local law enforcement officer on the street. The TSC allows government agencies to run name checks against the same comprehensive list with the most accurate, up-to-date information about known and suspected terrorists.[46]

The aforementioned presidential directive of September 16, 2003, stated,

> The heads of executive departments and agencies shall, to the extent permitted by law, provide to the Terrorist Threat Integration Center (TTIC) on an ongoing basis all appropriate Terrorist Information in their possession, custody, or control. The Attorney General, in coordination with the Secretary of State, the Secretary of Homeland Security, and the Director of Central Intelligence shall implement appropriate procedures and safeguards with respect to all such information about United States persons. The TTIC will provide the organization referenced in paragraph (1) with access to all appropriate information or intelligence in the TTIC's custody, possession, or control that the organization requires to perform its functions.[47]

Although, the name obviously changed from the TTIC to the TSDB, the inclusion of names is still driven by the secret "terrorist criteria" outlined pursuant to HSPD-6. We know that "only individuals who are known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism are included in the TSDB." We are also assured that "the purpose of the TSDB is not to hold information on individuals who have been convicted of a crime; however, an individual appropriately included in the TSDB may also have a criminal history. None of the information pertaining to the criminal history is contained or referenced in the TSDB."[48] The TSDB then supplies certain government users with more precise subsets of individuals who might be of interest to government agencies, including the selectee and no-fly lists, which would be made available to the DHS and its TSA.[49]

The no-fly lists are the most stringent lists kept, and the staff at the TSC regularly rejects nominations.[50] The criteria for inclusion in these subsets, however, are not published. A memo from the Acting Associate Under-Secretary in Transportation Security Intelligence, dated October 16, 2002, was obtained by the EPIC under the FOIA; it concedes that there are two primary principles that guide the placement on the lists, but these principles have been withheld.[51] What is also unclear is how the opaque ATS system interacts with the creation of these lists. The TSC does not, we are told, engage in profiling or providing risk-assessment scores,[52] but one must assume that nominations from this larger prescreening reach the TSC at some point.

Two lists are shared with the airlines and the TSA. A "no-fly" match requires the agent to call a law-enforcement officer to detain and question

the passenger. Someone on the "selectee," or "S," list has a special mark printed on their boarding pass, and the person then receives additional screening at security but presumably without any further intervention from law-enforcement officials. The FBI will neither confirm nor deny whether an individual is on these lists. How many names are on this list? The center's director, Donna A. Bucella, told Congress in March 2004 that the list was 120,000 names long. Other reports suggest that upward of 300,000 names would be a more accurate estimate. Since January 2005, the TSC has undergone a systematic scrub of all the information in the database. CBS News allegedly saw a list of 44,000 names in August 2006, not including a further 75,000 on the automatic selectee list.[53] By the time of this writing, in 2007, the numbers have probably become somewhat lower.

Increasing concerns about these lists, and about the lack of transparency and due process, has motivated a good deal of litigation. The most important suit was lodged by the ACLU. In April 2004, the National ACLU and the ACLU of Washington brought the first national lawsuit to challenge any aspect of the no-fly-list system. *Green et al. v. TSA* was brought on behalf of "false positive" passengers who had no method of resolving recurrent problems with being targeted by security even after they had been cleared for flight. The lawsuit and the related publicity led Congress in December 2004 to direct the TSA to maintain its lists in a manner that "will not produce a large number of false positives" and to create an appeal system for persons wrongly placed on the lists.

The overall public scrutiny forced government officials to admit there indeed were problems with these procedures and caused Congress to require the TSA to improve its processes for removing innocent people from the lists.[54] For those with names similar to those on the watch-lists, there is now a "TSA Passenger Identity Verification Form," through which individuals provide a range of personal information to allow the TSA to determine whether their check-in can be expedited. There is also an ombudsman in the TSA who is supposed to provide neutral and confidential services for employees and the public concerning TSA policies.[55] At the same time, there has been a more radical challenge to the very policy that airlines should require identification from airline travelers at all.[56]

Details of the Canadian government's implementation of the Passenger Protect program finally surfaced in the spring of 2007, when it published regulations on how the screening of people on the new "Specified Persons List" (SPL) would work. The lead agency is Transport Canada, which compiles the SPL based upon information received from the various Canadian security and intelligence agencies. It is assisted by a Passenger Protect Advisory Group, comprising senior officers from CSIS, RCMP, the Department of

Justice, and others to assess information on a case-by-case basis and make recommendations to the prime minister concerning the threat to aviation security. Under Transport Canada guidelines, a person will be added to the SPL if there is a determination the he poses an immediate threat to aviation security, including

> An individual who is or has been involved in a terrorist group, and who, it can reasonably be suspected, will endanger the security of any aircraft or aerodrome or the safety of the public, passengers or crew members; An individual who has been convicted of one or more serious and life-threatening crimes against aviation security; An individual who has been convicted or one or more serious and life-threatening offences and who may attack or harm an air carrier, passengers or crew members.[57]

It is clear that these criteria are not exclusive. In one sense they are narrower than those in the United States, because the list is meant to be confined to those who pose an "immediate threat" to aviation security. In another respect, the criteria are broader, because the list might also include many who have no connection to terrorism.

The SPL contains the name, date of birth, and gender of each person. The information for each specified person listed is reviewed at least once every thirty days. Under the Identity Screening Regulations,[58] airlines are required to compare each person's name as it appears on her government-issued ID against the specified-persons list before issuing a boarding pass, for any person who appears to be twelve years of age or older. The regulations take into account the various ways in which the boarding pass may be obtained, whether at a kiosk, off the Internet, or at an airport check-in counter. When the airline verifies that an individual matches in name, date of birth, and gender with someone on the list, the airline is required to inform Transport Canada to verify the person's identity. Once a match between a person wishing to board an aircraft and someone on the SPL is discovered by an air carrier, and subsequently confirmed by Transport Canada, that person will be denied boarding.[59]

Transport Canada has certainly taken steps to minimize the risk of false matches of persons with the same or similar name as someone on the list. Further an Office of Reconsideration provides an independent review mechanism for anyone with complaints or inquiries. Under the new procedures, this office will reevaluate cases, and if false positives are found, will "update the SPL with additional information to ensure the same individual will not be confused with a specified person in future."[60] It is not clear whether the individual's name will actually be removed. The SPL is expected to be more defined, limited, and hopefully effective than previous programs. Press reports suggest no more than two thousand names.

Although it is quite apparent that the government had tried to draw lessons from the mistakes made by the United States and is desperately trying to avoid the same embarrassments, this "made-in-Canada" program has not satisfied critics. Within two weeks of the program's beginning, there appeared a string of critical editorials and reports about false-positive cases.[61] Moreover, federal and provincial privacy commissioners passed a resolution in June 2007 calling for the referral of the program to parliament for review and scrutiny, the enactment of legislative criteria governing the use of no-fly lists (given that the Aeronautics Act clearly does not supply those criteria), the establishment of an independent oversight body to review the SPL, and the suspension of the program until the review had been completed. The commissioners were especially concerned that Transport Canada could not give assurances that the SPL would not be shared with foreign governments.[62] It is still not clear whether this smaller list would satisfy U.S. law-enforcement agencies, and if not, whether the airlines would continue to use the longer U.S. versions.

What Is Wrong with No-Fly Lists?

So what is wrong with trying to prevent those who pose threats to aviation security from boarding aircraft? The arguments against no-fly lists tend to group into four categories: effectiveness, due process, discrimination, and security. There are first a range of *effectiveness* questions. If the program cannot be demonstrably proven as effective, then why should civil liberties be put in the balance? With respect to Secure Flight, U.S. security expert Bruce Schneier states the issue as follows:

> Imagine for a minute that . . . we can ensure that no one can fly under a false identity, that the watch lists have perfect identity information, and that Secure Flight can perfectly determine if a passenger is on the watch list: no false positives and no false negatives. Even if we could do all that, Secure Flight wouldn't be worth it. Secure Flight is a passive system. It waits for the bad guys to buy an airplane ticket and try to board. If the bad guys don't fly, it's a waste of money. If the bad guys try to blow up shopping malls instead of airplanes, it's a waste of money.[63]

This leads him and others to conclude that the money spent on these passenger prescreening systems would be better spent on more proactive investigative measures or emergency-response systems. A more essential question asks whether one should really care whether somebody on an airplane has connections with terrorism, so long as he/she is not going to harm that particular flight. Behavior-based, rather than identity-based, screening is more appropriate.

Of course, any prescreening system embodies a range of *due process* concerns. The lists are secret. The criteria for appearing on lists are vague. There will always be false positives and false negatives. Therefore, many nondangerous passengers have either been mistakenly put on the lists or detained for having the same or similar name as someone on the list. Some have been subjected to stigma and detention with no meaningful opportunity to remedy these errors or appeal their status. Most notably, U.S. Senator Ted Kennedy told a Senate Judiciary Committee hearing on border security that he had been prevented from boarding flights because his name appeared on a watch-list; the problem was only corrected after a call from Senator Kennedy to Secretary Tom Ridge. Other journalists offered reports of babies, lawyers, academics, and famous pop-singers appearing on no-fly lists. A CBS *60 Minutes* in October 2006 reported that the list still contained fourteen of the nineteen dead 9/11 hijackers, François Genoud (was a Nazi sympathizer and has been dead for ten years) and Evo Morales, the president of Bolivia.[64] Further, anyone with the common name David Nelson risked intrusive screening and interrogation, prompting an ACLU supported lawsuit on behalf of someone with that name.[65]

A third and related problem of *discrimination* is also raised. Critics have noted the obvious issue of how socially constructed understandings of the kinds of people likely to engage in terrorism will inform the construction of watch-lists and the interpretation of behavior. We simply do not know the extent to which these prescreening programs rely on religious or racial profiling, or on the targeting of those with unsympathetic political beliefs. For example, plaintiffs in the 2004 American Civil Liberties Association constitutional challenge to no-fly lists included staff members of the ACLU and of the Nobel Peace Prize–winning pacifist organization the American Friends Service Committee.[66]

Finally, no comprehensive passenger prescreening program can be free of *security* problems. Individuals can purchase tickets and attempt to board with false identifications. Individuals may try to fly on someone else's ticket. There is also error that will naturally occur in the front-end verification match of thousands of airline transactions daily. The system of ID verification is always subject to human and computer error. And yet the risk to the individual is direct, immediate, and easily grasped.

No-Fly Lists and Theories of Surveillance

So what are no-fly lists and how can we better understand their development? It is readily apparent that the image of one discrete and bounded list in the hands of one authority is misguided. No-fly lists are dynamic, as they

are constantly being updated, expanded, and refined. Donna Bucella, the head of the TSC, has likened the process to painting a bridge; as soon as you finish one end, you have to start again at the other.[67] One FBI agent has described the initial screening process as a "massive data dump" of anybody with a connection to terrorism, which the TSC has been trying to clean up ever since.[68]

From the outside, the apparent costs of these systems far outweigh any benefits. For many surveillance practices, the countervailing interests are normally quite evident. The case for passenger prescreening programs against no-fly lists, however, has clearly not been convincingly made, either in the United States or Canada. So what, then, explains the persistence of this idea? What theories of surveillance can help us come to grips with the dogged manner in which passenger prescreening programs have been developed in the United States, and then later emulated in Canada in the face of constant criticism, and the obvious and embarrassing fact that these systems still cannot adequately distinguish between terrorists and famous politicians or babies. The deep contradictions within this concept have been best expressed by Schneier: "Remember what the no-fly list is. It's a list of people who are so dangerous that they can't be allowed to board an airplane under any circumstances, yet so innocent that they can't be arrested—even under the provisions of the Patriot Act."[69]

It is now commonplace to try to understand surveillance practices in terms of the structural conditions of postmodern society.[70] The "conditions of possibility" for no-fly lists are obviously complex organizations employing the latest technologies. Airports are sites of discipline, where passengers become passive subjects and bearers of the power relations that force compliance. The "war on terror" is a further extension of the normalizing gaze of the panopticon. No-fly lists are the manifestation of authorities' attempts to marginalize—to separate the suspicious and abnormal from the innocent and normal. Surveillance is also supposed to have changed in character and degree. New patterns of information-capture inform the procedures by which individual behaviors might be discovered and interrogated. One persistent theme is that surveillance is now "routine" or "everyday"; it is the by-product of routine engagement with modern institutions.[71]

Contemporary surveillance is not, therefore, characterized by centralized "Big Brother" or "panoptic" control. It is, rather, decentralized and disaggregated in the form of different computer networks within government, outside government, and most notably within the gray areas in between collecting information about identity and behavior. In this environment, we talk less of "databases." The dispersed and networked information environment has created a more diffuse and elusive "surveillant assemblage."[72] In

this model, surveillance operates by abstracting human bodies from their contexts and separating them into a series of discrete flows. These flows are then reassembled by different institutions in different locations to produce a series of "data-doubles" for each individual. Like a rhizome, our digital personae operate beneath the surface and then emerge in different forms for different institutional purposes and agendas. Thus, the surveillant assemblage transforms the hierarchies of surveillance and the nature of personal privacy.

The contemporary sociological literature on surveillance embodies many powerful insights into the ways modern institutions keep tabs on unsuspecting subjects. It does not, however, help us explain the patterns documented in this article. Indeed, it is interesting to reflect on how little this literature tends to talk about "lists." Watch-lists are as old as government, and no-fly lists are perhaps a throwback form of surveillance. They are definitely not routine and they are highly centralized. They also are not necessarily dependent upon sophisticated methods of information extraction and monitoring. "Lists" seem too discrete and too simple. They are also deeply and inescapably political. They evoke images of the most intrusive and discriminatory forms of government surveillance. No person would ever wish to be on a no-fly list. On the other hand, we have inherent interests in having our names on the electoral rolls, the banking systems, the credit-reporting agencies, and a host of other government systems. The problem with many contemporary information systems is how the information is used and disclosed *once collected*. If one's name is on a no-fly list, one has a problem, regardless of how it will be used and disseminated.

Paradoxically, these lists might also be easier to regulate, from the point of view of existing privacy regimes. The American and Canadian Privacy Acts date from 1974 and 1982 respectively. It is commonly agreed that both pieces of legislation are unequal to the depths and complexities of contemporary privacy challenges. Both, for example, rest on the outmoded concept of a "system of records," a bounded "list" of personal information, which could be more easily identified and regulated before the emergence of current models of computing architecture, based on dispersed networks. It is, however, instructive that the EPIC and the ACLU were able to get a handle on the CAPPS, Secure Flight, and ATS systems by invoking the statutory obligations within the Privacy Act to produce a notice in the *Federal Register* whenever a new "system of records" was being constructed. The TSA was even caught at one point violating Privacy Act requirements. These notices are, to be sure, vague and insufficient; however, they do provide a starting point for further litigation, for FOIA requests and for outside scrutiny. And in Canada, there has never been a more united, and forceful, opposition to any surveillance measure than that expressed against Passenger Protect.

Privacy is often faulted in the critical surveillance literature for its central reliance on the risks associated with individualized subjects rather than with the larger societal consequences. To be sure, the language and policy instruments of privacy are not the only antidote to curbing the effects of excessive surveillance.[73] They do, however, have an emotive appeal against the relatively crude construction of "lists." This conclusion also suggests that privacy legislation constitutes a necessary, if not sufficient, strategy to fight excessive surveillance.

If one is seeking an explanation for the development of no-fly lists, then perhaps the neo-institutionalist literature on policy instruments, referred to earlier, can assist. When faced with a common problem, governments possess a finite inventory of policy instruments, and they draw lessons from their counterparts. The "tools of government" have been a matter of academic inquiry and practical policy-analysis for about twenty years.[74] This approach eschews the old-fashioned and descriptive "institutionalism." It leads naturally to a range of fascinating comparative questions: Which tools appear in the "toolbox" of different societies? Why are some preferred over others? Is the correct tool being used? The metaphor should not be overdone. As we point out in *The Governance of Privacy*,

> In a toolbox, each instrument is suited to a different purpose and has a specific use. But most of the tools are used separately, not in conjunction with each other, and there is no overall single purpose for their use. Throw away the screwdriver, the drill and the saw, yet the hammer remains, still capable of doing its job and driving the nail home. But it cannot do what the other tools can do, and its efficacy as a nail-driver may depend, in part, on factors to do with the person who wields it. Among these is the ability to recognize what is a nail, and what is not.[75]

Christopher Hood makes a basic distinction between "effecting" tools (the means by which government can impact on the outside world) and "detecting" tools (the instruments that government uses for taking in information).[76] Government then uses its "nodality, treasure, authority, and organization to perform these roles" the distinctions are not clear-cut, but we are unmistakably analyzing "tools of detection" here: "government needs a set of tools for examination, inspection, monitoring, watching and detecting, tools which must be applicable to a wide range of objects."[77]

He further distinguishes between nodal receivers (information that government obtains simply by maintaining a passive presence at the center of the social network); rewards (where resources are used to obtain information); requisitions (where information is provided under threat of sanction for noncompliance); and ergonomic detectors (where government puts the emphasis on physical or mechanical devices for obtaining information involuntarily or without the cooperation of an informant).[78] Here then is a useful taxonomy of how government collects personal information. It may get it for free (when, for example, individuals call "hotlines"); it may pay for it (though rewards, information exchanges, or active propositions); it may demand it and impose a sanction if it is not provided (through obligations to notify, tax returns, interrogations, or inspections); it may set up fixed or mobile systems to observe all who pass (turnstiles, or mobile and hidden scanners).

How are nodality, treasure, authority, and organization deployed by governments to address the problem of airline security? In both Canada and the United States all of these tools have been used to develop passenger prescreening programs. Both use their "nodality" to assert a central coordinating role in the "war on terror," in response to the obvious failure of a more dispersed and fragmented system of prescreening. Both the DHS and Transport Canada use their organizational powers to coordinate and consult with relevant stakeholders. But economic power is perhaps used more in the United States, where it provides incentives to database companies to share proprietary data for identity verification; U.S. federal privacy laws do not generally prevent intelligence agencies from purchasing personal information from commercial data-aggregators.

In an era when policy making in advanced industrial-states is characterized by new governance arrangements, by innovative ways to use institutions in civil society to coregulate society, and by a conventional wisdom that many tools are necessary for the delivery of public goods, no-fly lists do stand out as a classic, authority-based model of government, based on command and sanction. In both countries, statutory authorizations are necessary conditions for the construction of lists (from other agencies) and the provision of mandates to airlines to prescreen against flight manifests and PNRs.

No-fly lists are one reflection of the resurgence of the state's attempt to reassert its sovereignty and perhaps a reversal of the transnational, complex, and multilevel aspects of policy making that characterized the political science and international relations of the 1990s.[79] At the same time, both the Canadian and U.S. governments cannot implement this policy without the willing cooperation of a variety of civil-society actors, especially airlines. The tendency to download costs and responsibilities to nongovernmental actors is definitely a feature of the contemporary form of governance, characterized by coregulatory activity rather than "do-it-alone" government.[80] These patterns are also consistent with theories of governmentality, in which devolution of governmental responsibility is enacted through a number of policy instruments or technologies to manage risk.[81]

However, if one is seeking a robust explanation for these policy developments in both countries, then one needs to look no further than September 11 and the obvious failure to apprehend any of the perpetrators before they boarded the planes, even though it is reported that half of them were already flagged on the watch-lists of the day. That experience creates a powerful legacy for newly created bureaucratic agencies with a need to justify their existence and budgets. The particular dynamics of policy development produce bureaucratic and technological legacies. No-fly lists are, therefore, path dependent. They are explained neither by the arbitrary whims of the sovereign with his "little list" nor by the protective motivations of the benign philanthropist. Rather, the pattern is better explained by an overwhelming motivation to "be on the safe side" within contemporary risk societies and by the fact that the range of policy instruments available to contemporary policy makers is inherently limited.[82]

Notes

1. Both quotations are from the Gilbert and Sullivan archive, http://math.boisestate.edu/GaS/index.html.
2. "If you give me your attention, I will tell you what I am:
   I'm a genuine philanthropist—all other kinds are sham.
   Each little fault of temper and each social defect
   In my erring fellow-creatures, I endeavour to correct"
   (King Gama in *Princess Ida*, Gilbert and Sullivan).
3. Anthony Giddens, *The Consequences of Modernity* (Cambridge: Polity Press, 1990); David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001).
4. Christopher Hood, *The Tools of Government: Public Policy and Politics* (Chatham, N.J.: Chatham House, 1983); Michael Howlett and M. Ramesh, *Studying Public Policy: Policy Cycles and Policy* (Oxford: Oxford University Press, 2003).
5. Philip B. Heyman, *Terrorism, Freedom and Security: Winning without War* (Cambridge, Mass.: MIT Press, 2003).
6. Theda Skocpol, "Bringing the State Back In: Strategies of Analysis in Current Research," in *Bringing the State Back In*, ed. Peter Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambridge University Press, 1985), 3–42.
7. James G. March and Johan P. Olsen, "The New Institutionalism: Organizational Factors in Political Life," *American Political Science Review* 78, no. 3 (1984): 734–49; Colin J. Bennett, "The Public Surveillance of Personal Data: A Cross-national Analysis," in *Computers, Surveillance, and Privacy*, ed. David Lyon and Elia Zureik (Minneapolis: University of Minnesota Press, 1996), 237–59.
8. The 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton, 2004), 392.

9. *Federal Register* 68, no. 10 (January 15, 2003): 2101–3.
10. See, for example, the comments of the Electronic Privacy Information Center, *Air Travel Privacy*, http://www.epic.org/privacy/airtravel/ (accessed April 11, 2008).
11. *Federal Register* 68, no. 148 (July 31, 2003): 45265–69.
12. http://www.eff.org/Privacy/TIA/20030324_capps_letter.php (accessed April 11, 2008).
13. The travel industry is served by four main "reservation-system" service providers—"Global Distribution Systems." Two companies have emerged as giants of the industry: Sabre, the larger of the two companies and pioneer of the service, and Galileo. Both offer computerized reservation systems to airlines, travel agencies, rental companies, and hotel chains. The others are Worldspan and Amadeus.
14. Ryan Singel, "JetBlue Shared Passenger Data," *Wired Magazine*, September 18, 2003, http://www.wired.com/news/politics/privacy/0,60489-0.html (accessed April 11, 2008). See also Gallya Lahav's chapter in this volume.
15. http://www.epic.org/privacy/airtravel/stone_answers.pdf (accessed April 11, 2008).
16. Government Accountability Office, "Computer Assisted Passenger PreScreening System Faces Significant Implementation Challenges," GAO Report No. 04-385 (February 2004), http://www.gao.gov/htext/d04385.html (accessed April 11, 2008).
17. American Civil Liberties Union, "The Seven Problems with CAPPS II," April 6, 2004, http://www.aclu.org/privacy/spying/15258res20040406.html (accessed April 11, 2008.
18. The 9/11 Commission, *Final Report*, 393.
19. Intelligence Reform and Terrorism Prevention Act Public Law, 108-458 (2004).
20. Federal Register, "TSA, Reports, Forms and Record Keeping Requirements: Agency Information Collection Activity under OMB Review, Docket No. TSA: 2004-19160," *Federal Register* 29 (September 24, 2004): 65619–27.
21. These General Accounting Office (GAO) reports are all linked from the EPIC Secure flight page, http://www.epic.org/privacy/airtravel/secureflight.html (accessed April 11, 2008).
22. See http://www.alaskafreedom.com (accessed April 11, 2008).
23. https://secure.eff.org/site/SPageServer?pagename=ADV_secureflight&JServSessionIdr006=sevnmibej1.app6a (accessed April 11, 2008).
24. http://www.tsa.gov/research/privacy/faqs.shtm (accessed April 11, 2008).
25. General Accounting Office, "Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program," GAO-06-374T (February 9, 2006), http://www.gao.gov/new.items/d06374t.pdf (accessed April 11, 2008).
26. Hawley, Kip, "Testimony by Kip Hawley," February 9, 2006, http://www.tsa.gov/press/speeches/speech_1002.shtm (accessed April 11, 2008).
27. http://www.epic.org/privacy/airtravel/secureflight.html (accessed April 11, 2008).

28. *Federal Register* 71, no. 212 (November 2, 2006): 64543–46, http://edocket.access.gpo.gov/2006/06-9026.htm (accessed April 11, 2008).
29. Ibid.
30. Department of Homeland Security, "Automated Targeting System Privacy Impact Assessment," November 22, 2006, p. 2, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf (accessed April 11, 2008).
31. Electronic Frontier Foundation, "American Travelers to Get Secret 'Risk Assessment' Scores," November 30, 2006, http://www.eff.org/news/archives/2006_11.php (accessed April 11, 2008).
32. http://www.epic.org/privacy/pdf/ats_comments.pdf (accessed April 11, 2008).
33. American Civil Liberties Union, "ACLU Backgrounder on ATS," January 10, 2007, http://www.aclu.org/privacy/gen/27928pub20070110.html (accessed April 11, 2008).
34. Bruce Schneier, "Automated Targeting System," December 22, 2006, http://www.schneier.com/blog/archives/2006/12/automated_targe.html (accessed April 11, 2008).
35. Section 4.81 states:
    The Minister, or any officer of the Department of Transport authorized by the Minister for the purposes of this section, may, for the purposes of transportation security, require any air carrier or operator of an aviation reservation system to provide the Minister or officer, as the case may be, within the time and in the manner specified by the Minister or officer, with information set out in the schedule
    a) that is in the air carrier's or operator's control concerning the persons on board or expected to be on board an aircraft for any flight specified by the Minister or officer if the Minister or officer is of the opinion that there is an immediate threat to that flight; or
    b) that is in the air carrier's or operator's control, or that comes into their control within 30 days after the requirement is imposed on them, concerning any particular person specified by the Minister or officer.
36. Transport Canada, "Government of Canada Moving Forward on Air Passenger Assessment," August 5, 2005, http://www.tc.gc.ca/mediaroom/releases/nat/2005/05-gc009e.htm (accessed April 11, 2008).
37. Office of the Privacy Commissioner of Canada, "Questions Submitted to Transport Canada, Regarding Plans for a 'No-fly List,'" August, 9, 2005, http://www.privcom.gc.ca/media/nr-c/2005/ques_050809_e.asp (accessed April 11, 2008).
38. The author made an access-to-information request for this Privacy Impact Assessment (PIA). A version, conducted by Deloittes and dated December 16, 2005 was released with several significant redactions in September 2007.
39. British Columbia Civil Liberties Union, "Letter to Ms. McLellan and Mr. Lapierre, Re: Opposition to Proposed 'No-fly' List," June 10, 2005, http://www.bccla.org/othercontent/05nofly.html (accessed April 11, 2008).
40. Jim Bronskill, "No-Fly List May Not Fly, Federal Study Warns," *Globe and Mail*, March 17, 2006.
41. Jim Bronskill, "U.S. No-Fly List Mistakenly Snagging Dozens of Canadians," *Edmonton Journal*, July 18, 2006.

42. See http://www.ararcommission.ca (April 11, 2008).
43. TSA Watchlists Memo, http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html (accessed April 11, 2008).
44. I am very grateful for the insights provided by Lyn Rahily, Privacy Officer of the Terrorist Screening Center, and Tim Edgar, Deputy Civil Liberties Director at the Office of the Director of National Intelligence on the panel on "No-fly Lists in Canada and the United States" at the Computer, Freedom, Privacy (CFP) Conference, Montreal, May 3, 2007.
45. The National Counterterrorism Center, "Terrorist Identities Datamart Environment" (TIDE), http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf (accessed April 11, 2008).
46. http://www.fbi.gov/terrorinfo/counterrorism/faqs.htm (accessed April 11, 2008).
47. Office of the Press Secretary, White House, "Homeland Security Presidential Directive/Hspd-6," September 16, 2003, http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html (accessed April 11, 2008).
48. Ibid.
49. See FAQs, http://www.tsa.gov/research/privacy/faqs.shtm#0 (accessed April 11, 2008).
50. Comments by Lyn Rahily, Privacy Officer at the Terrorist Screening Center, Computer Freedom Privacy (CFP) conference, May 3, 2007.
51. TSA Watchlists Memo, http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html (accessed April 11, 2008).
52. Lyn Rahily, CFP conference, May 3, 2007.
53. CBS News, "Unlikely Terrorists on No-Fly List," *Sixty Minutes*, October 8, 2006.
54. American Civil Liberties Union, "Grounding the No-fly List," August 12, 2005, http://www.aclu-wa.org/inthecourts/detail.cfm?id=252 (accessed April 11, 2008).
55. http://www.tsa.gov/join/benefits/careers_benefits_ombudsman.shtm (accessed April 11, 2008).
56. In *Gilmore v. Gonzales*, the court found that there was no inherent constitutional right to travel anonymously. They did uphold the airline's policy that one either presents identification or opts to be treated as a "selectee" and undergo more intensive screening. The entire story is told at http://www.papersplease.org/gilmore/index.html (accessed April 11, 2008).
57. Transport Canada, "Passenger Protect Program," June 8, 2007, http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm (accessed April 11, 2008).
58. Aeronautics Act, Identity Screening Regulations P.C. 2007-602, April 26, 2007, http://canadagazette.gc.ca/partII/2007/20070516/html/sor82-e.html (accessed April 11, 2008).
59. Transport Canada, "Specified Persons List," June 6, 2007, http://www.passengerprotect.gc.ca/specified.html (accessed April 11, 2008).
60. Transport Canada, "Office of Reconsideration," June 7, 2007, http://www.tc.gc.ca/reconsideration/menu.htm (accessed April 11, 2008).
61. For example, "Boy on No-Fly List Advised to Change Name," *The Ottawa Citizen*, June 29, 2007.

62. Office of the Privacy Commissioner of Canada, "Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials. Passenger Protect Program—Canada's Aviation No-Fly List," June 28, 2007, http://www.privcom.gc.ca/nfl/res_20070628_e.asp (accessed April 11, 2008).
63. Bruce Schneier, "TSA's Secure Flight," January 31, 2005, http://www.schneier.com/blog/archives/2005/01/tsas_secure_fli.html (accessed April 11, 2008).
64. CBS News, "Unlikely Terrorists on No-Fly List."
65. American Civil Liberties Union, "Statement of David C. Nelson," April 6, 2004, http://www.aclu.org/safefree/resources/17468res20040406.html (accessed April 11, 2008).
66. British Columbia Civil Liberties Union, "Letter to Ms. McLellan."
67. Quoted in CBS News, "Unlikely Terrorists on No-Fly List."
68. Jack Cloonan, quoted in ibid.
69. Bruce Schneier, "Schneier on Security: Definition of No-Fly," September 26, 2005, http://www.schneier.com/blog/archives/2005/09/secure_flight_n_1.html (accessed April 11, 2008).
70. See chapters by David Lyon, Benjamin J. Muller, and Peter Adey in this volume.
71. Lyon, *Surveillance Society*.
72. Kevin D. Haggerty and Richard V. Ericson, "The Surveillant Assemblage," *British Journal of Sociology* 51, no. 4 (2000): 605–20; see Mark B. Salter's chapter in this volume.
73. Lyon, *Surveillance Society*, 119; Felix Stalder, "Privacy Is Not the Antidote to Surveillance," *Surveillance and Society* 1, no. 1 (2002): 120–24.
74. Howlett and Ramesh, *Studying Public Policy*.
75. Colin J. Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in the Twenty-First Century* (Toronto: University of Toronto Press, 2003), 164.
76. Hood, *The Tools of Government*, 3.
77. Ibid., 91.
78. Ibid., 91–105.
79. Edgar Grande and L. Pauly, *Complex Sovereignty: Reconstituting Political Authority in the Twenty-First Century* (Toronto: University of Toronto Press, 2005).
80. Jan Kooiman, *Governing as Governance* (London: Sage, 2003).
81. Nicholas Rose, "Governing 'Advanced' Liberal Democracies," in *Foucault and Political Reason: Liberalism, Neo-liberalism and Rationalities of Government*, ed. Andrew Barry, Thomas Osborne, and Nicholas Rose (Chicago: University of Chicago Press, 1996), 37–64.
82. Ulrich Beck, *World Risk Society* (Cambridge: Polity Press, 1999).

4

Mobility and Border Security

The U.S. Aviation System, the State, and the Rise of Public–Private Partnerships

Gallya Lahav

Immediately following the terrorist attacks of September 11, 2001, the United States shut down its air-traffic system for several days, and rerouted an estimated forty-five thousand passengers to Canada. The creation of Operation Yellow Ribbon by Canada's Department of Transport marked the first time in history that Canada shut down its own airspace.[1] Beyond lending testament to spectacular international cooperation, these dramatic events revealed the expansive and interdependent nature of contemporary border control, now including foreign states, and other nonstate and private actors such as airlines. Moreover, the implications of the presence of foreigners in the terrorist attacks reflected the dramatic realization of new global threats emanating from private, nonstate actors, in groups as diverse as terrorists, drug traffickers, human smugglers, migrants, and foreign students. They visibly exposed the changing nature of threat, while masking some of the dramatic qualitative changes that have occurred since September 11.

The subsequent surge of policy instruments and public–private partnerships brought to light the link between security and mobility in a global