4 Workshop on AGIS Programme, 'Police Information Technology Co-Operation in an enlarged European Union', Friday 21 May 2004.
5 Source: http://www.rcmp-grc.gc.ca/security/ibets_e.htm
6 Source: http://www.rcmp-grc.ca/security/insets_e.htm

References

Bales, K. (2004) *Disposable People: New Slavery in the Global Economy* (Los Angeles: University of California Press).

Convey, A. and Kupiszewski, M. (1995) 'Keeping up with Schengen: migration and policy in the European Union', *International Migration Review*, 29:4, pp. 939–64.

Dawson, A. and Fife, R. (2005) 'Don't Lose Fear of Terrorists, U.S. Envoy Cellucci Warns', *The Ottawa Citizen*, Monday 7 February 2005, p. A5.

European Report (2002) 'Justice and Home Affairs: Council Moves to Add Al-Qaeda Members to Schengen Information System', 26 June 2002, p. 481.

European Report (2004) 'Justice and Home Affairs: Data Exchanges with Europol Up by 39% in 2003', 7 July 2004, p. 408.

Evans, D. (1994) 'Bordering on the Ridiculous (development of Schengen Information System)', *Computer Weekly*, 24 March 1994, pp. 38–42.

Haggerty, K. and Ericson, R. (2000) 'The Surveillant Assemblage', *British Journal of Sociology*, 51:4, pp. 605–22.

Hier, S.P. (2003) 'Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes or social control', *Surveillance and Society*, 1:3, pp. 399–411.

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

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press).

Marx, G. (1988) 'Do Monitoring Technologies Threaten Employee Privacy Rights?' *Editorial Research Reports*, 2:12, p. 489.

Nelkin, D. and Andrews, L. (1999) 'DNA Identification and Surveillance Creep', *Sociology of Health and Illness*, 21:5, pp. 689–706.

Reiner, R. (2000) *The Politics of the Police* (Oxford: Oxford University Press).

Staples, W.G. (2000) *Everyday Surveillance: Vigilance and Visibility in Postmodern Life* (Lanham: Rowman and Littlefield Publishers).

Staples, W.G. (1997) *The Culture of Surveillance: Discipline and Social Control in the United States* (New York: St Martin's Press).

Warren, P. (1992) 'Continental Cop-out', *Computer Weekly*, 8 October 1992, pp. 26–8.

Zaccardelli, G. (2004) *Speech-Cooperation and Coordination in the New Security Environment*, Department of National Defence Network Enabled Operations: Ottawa). Available at: http://www.rcmp-grc.gc.ca/speeches/sp_new_security_e.htm

Chapter 8

What happens when you book an airline ticket? The collection and processing of passenger data post-9/11

Colin J. Bennett

In 1999 I wrote a paper with a similar title (Bennett 1999) based on a series of case studies for the European Commission on the collection, processing and dissemination of personal data by multi-national businesses, including the international airline industry (Raab *et al.* 1998). The paper traced the flows of data from the time of booking an airline ticket, through the check-in process, to the flight and the landing.[1] The case study examined the flows of data through an increasingly complex series of scenarios concerning the identity and tastes of the traveller, his 'frequent flyer status' and the nature of the ticketed route. The study allowed me to draw some tentative generalizations about the practices of typical international air carriers with regard to the processing of personal information, the characteristics of the larger surveillance network and the prospects for international regulation.

At the time of writing, little attention was paid to personal data protection issues by the airline industry. It was then difficult to find interested or expert officials within the major airlines who could provide accurate descriptions of the personal information processing practices of the industry. Few companies had appointed Chief Privacy Officers and few had explicit codes of practice. It was also difficult to find knowledgeable people from the community of outside activists and regulators who had paid much attention to the issue. There has, however, been a dramatic increase in the attention paid to the personal data processing activities of the airline industry since 11 September 2001. Passenger Name Record (PNR) data has been aggressively sought by US and international law-enforcement agencies as the basis of pilot projects for passenger profiling systems. This has caused a major transatlantic row between the Europeans and the US over the legality (under the EU's 1995 Data Protection Directive) of transferring such data to the US for processing, given the presumed 'inadequacy' of American privacy protection standards. In addition, the construction of Advanced Passenger Information (API) databases and the introduction of trusted traveller systems, often accompanied by biometric identifiers, have brought the question of the processing of travel data sharply into profile.

This paper attempts to update the earlier 1999 version in light of developments since 9/11.[2] Again, this paper eschews abstraction in favour of a very detailed empirical description of 'what happens when you do indeed book an airline ticket'. It describes two scenarios, both based on recent personal experience. The first outlines the relatively simple trip that I took to attend the conference at which the first draft of this article was presented: a flight via one airline (Air Canada) within one country (Canada, from Victoria, British Columbia to Toronto, Ontario, with onward flights to Kingston and Ottawa, Ontario). It outlines the personal information practices of the booking process, the check-in process, and the frequent flyer programme. At each stage, I have tried to discover what information about me is collected by whom, for how long it is retained, and who might have access to it. A second scenario takes the onward leg of my journey to New York rather than to Ottawa, and investigates how current and future changes in the rules of Canadian and US border control agencies have affected the flows of personal data about me.

Although the paper concludes with some reflections of a more theoretical nature, it is explicitly based on some firm assumptions about how we should be studying the 'everyday' nature and implications of personal surveillance systems (Lyon 2001). I am critical of some of the literature on the surveillance (or privacy) implications of information and communications systems and networks. The analysis of social or individual risk is often based on exaggerated claims about the potential for the linkage and communication of personal data, on extrapolations about surveillance potential from highly abnormal cases, and on hypotheses about what roles new technologies might perform in the abstract, with very little grounded analysis of its role in real, dysfunctional organizations within which fallible but mainly well-intentioned individuals make choices and decisions. 'Our physical bodies are being shadowed by an increasingly comprehensive data body', asserts Felix Stalder in his critique of privacy in the very first issues of *Surveillance and Society* (Stalder 2002). Perhaps, but is it possible to observe this body of data? Can one find one's 'digital persona' (Clarke 1994)? The common assumptions in the literature are that one's 'data shadow' is becoming more latent, comprehensive, integrated, finely tuned, and thus more pernicious. Through this very narrow, and hardly generalizable, case study based on the 'politics of personal experience' I wish to raise some searching questions about these and other assumptions within the surveillance literature.

Victoria–Toronto–Kingston–Toronto–Ottawa–Toronto–Victoria

The reservation

Airline flights can be reserved in one of four ways: first, directly from the airline's own reservation system (by phone or at its website); second, through a travel agent who will have access to international computerized reservation systems or global distribution systems (GDS);[3] third, if reward points are being used, through the toll-free number or website associated with the airline's frequent flyer programme; and fourth, over the Internet, through services such as www.travelocity.com, www.expedia.com or www.travelport.com.

On 24 June 2004, I followed the instructions of the conference organizers and reserved return flights from Victoria to Kingston with onward connections to Ottawa through a local travel agency based in Kingston, Ontario. All Canadian travel agencies are now covered by either federal or provincial privacy legislation, and should be developing their own privacy policies and appointing privacy protection officers. It seems, however, that only the larger agencies, such as Thomas Cook, have taken these initiatives.[4] The Association of Canadian Travel Agencies (ACTA) also provides guidance concerning obligations under the new legislation, although the professional standards promulgated by ACTA have yet to incorporate privacy protection.[5] Thus, no agency should be revealing information in my customer profile to anybody else (without my consent) unless it is for the express purpose of reserving travel arrangements for me,[6] or is otherwise required by law.

Like many Canadian travel agents, this one used the Galileo reservation system to book my flight and collected my name, address, e-mail, credit card number and Aeroplan frequent flyer number. Travel agencies pay an annual fee to Galileo for access to this system, and for the presumed convenience, speed and possible cost savings to their clients. Galileo International, Inc. is one of the leading global distribution systems (GDS).

Their services connect approximately 44,000 travel agency locations to 470 airlines, 24 car rental companies, 56,000 hotel properties, 430 tour operators and all major cruise lines throughout the world. Located in Greenwood Village, near Denver, Colorado, Galileo's Data Center handles, on average, over 175 million requests for information per day. At peak times the company processes more than 2,915 messages per second.[7] GDSs like Galileo are the central repository for vast amounts of information related to an individual's travel. They are the central hubs which link all providers of travel services. They play a similar role to that played by the credit bureaus in relation to the financial industry (Hasbrouck 2004).

Thus, when a prospective traveller discloses air travel plans to a travel agent, the agent enters the data into the Galileo system, either via an encrypted Internet portal protected by SSL technology or by a direct communication link. The Galileo system then electronically contacts the airline(s) in question to ascertain whether the requested flight is available. If it is, the travel agent completes the reservation in the Galileo system. Galileo then transmits the reservation data to the travel suppliers involved in the booking – solely Air Canada in this case. If the airline is hosted on a different GDS, information about the flight(s) on that airline is sent to the airline's host system. The standards for information sharing between airlines are governed by the Airline Interline Message Procedures Manual (AIRIMP).

I was then e-mailed an electronic ticket, issued by Air Canada, which includes a ticket number, the name and place of the booking agent, the entire itinerary and the price for each leg (plus taxes). The electronic ticket includes the statement: 'Carriage and other services provided by the carrier are subject to conditions of carriage which are hereby incorporated by reference. These conditions may be obtained from the issuing carrier.'[8] It also states that 'this receipt may be required at check-in and must be presented to customs and immigration if requested.' My itinerary and e-ticket could also be viewed online by typing in the reservation locator number and my last name at www.viewtrip.com, a website operated by Galileo.[9]

At this point in the process, the travel agent's role is typically complete. Certain billing and scheduling issues may be raised after the completion of travel. For example, an airline might contest the quoted price of a fare because certain booking conditions were not met. As the travel information is no longer online (see below), the agency would have to retrieve a hard copy from Galileo. With these exceptions, the only records of travel that might be kept by an individual agency relate to the accounting information. The data-retention practices of travel agencies differ widely, however.

The record – the PNR

When my flight was booked, a Passenger Name Record (PNR) was created on Galileo's reservation system.[10] It is probable that my PNR simply included the five mandatory fields of data: the Passenger's Name, Itinerary or Routing Information, Recipient (reservation booking personnel), Phone Contact and Ticket Number. There are two supplementary categories contingent upon the construction of the PNR: a Special Service Request field and an Other Service Request field, into which information might be entered depending on the special needs and preferences of the traveller (seat assignment, meals, wheelchair needs and so on). Some of the materials contained within these fields are available to other carriers through an inter-operability mechanism, while others are exclusive to the carrier itself. A General Remarks Category is available to the operator as well. Some carriers will also 'overlay' their checkpoint information (seat numbers, baggage, frequent flyer) onto the PNR through their own systems at check-in. Some carriers (typically chartered carriers) do not enter formal PNR information, particularly where the carrier has an agreement with a 'Tour Operator', but are provided with a basic 'manifest' of passenger information by the operator with whom they have a contract.

A PNR may be amended by different agencies through different channels at different times. For complex travel arrangements, therefore, there may be several PNRs created and stored on different GDSs. An example of the possible complexities is given by Hasbrouck (2004):

> If, for example, you make a reservation on United Airlines (which outsources the hosting of its reservations database to the Galileo CRS/GDS) through the Internet travel agency Travelocity.com (which is a division of Sabre, and uses the Sabre CRS/GDS), Travelocity.com creates a PNR in Sabre. Sabre sends a message derived from portions of the Sabre PNR data to Galileo, using the AIRIMP (or another bilaterally-agreed format). Galileo in turn uses the data in the AIRIMP message to create a PNR in United's Galileo 'partition'.

Once a PNR is created, an audit trail logs each entry in the PNR history with the date, time, place, user ID and other information of the travel agent, airline staff person, automated system or any other person (such as a company secretary) who requested the entry or change. Each entry in each PNR, even for a solo traveller, may thus contain personally identifiable information on several people.

In my case, the profile is not that interesting. But it could also include the credit card information, alternative addresses, phone numbers and emergency contacts. It may contain notes about tastes and preferences, as well as personal notes intended for the use of the travel agency.[11] PNRs can therefore reveal an enormous amount about our travel preferences, and therefore our tastes and behaviours. They show:

> where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. … Through meeting codes used for convention and other discounts, PNRs reveal affiliations – even with organizations whose membership lists are closely-held secrets not required to be divulged to the government. Through special service codes, they reveal details of travelers' physical and medical conditions. Through special meal requests, they contain indications of travelers' religious practices – a category of information specially protected by many countries. (Hasbrouck 2004)[12]

Airlines also, of course, transport special categories of persons – deportees, unaccompanied minors, refugees, and so on.

The PNR created for my travel was collected in Canada, and is therefore subject to Canadian privacy legislation. A recently constructed privacy policy for Galileo Canada stipulates in greater detail how this information is collected, stored and disclosed. Galileo Canada discloses personal information to the extent necessary or related to successfully completing the reservation. Thus,

> personal information is disclosed to the travel agency and travel suppliers selected by the traveler and others involved in the transaction, such as the traveler's credit card company, insurance company, and otherwise as necessary on important public interest grounds or as required by law, court order, or as requested by a governmental or law enforcement authority or in the good faith belief that *disclosure is otherwise necessary or advisable.*

Certain ticketing information in the Galileo system is optionally available to the airlines. Personal information may also be disclosed in any other manner upon the consent of the traveller involved or to anyone who Galileo Canada reasonably believes is seeking the information as the agent of the traveller. They also reserve the right to disclose personal information in connection with the sale or transfer of all or substantially

all of the assets of Galileo Canada or Galileo International, Inc. to a third party.[13] The PNR data remains online for up to 72 hours after the completion of travel. After that it is archived for three years in the Galileo Data Center, after which it is destroyed.

The Galileo Canada privacy policy applies only to personal information collected in Canada. No general privacy protection policy appears on the parent site of Galileo.[14] As a global distribution system, however, this policy is not significantly different from that applied throughout the entire global operations and which has been driven principally by European rules.[15] A series of regulations on Computerized Reservation Systems (dating from 1989, 1993 and 1999) have governed the services between GDSs and suppliers, to ensure fair competition. These regulations also include bans on the transfer of personal data to third parties.[16] The 1995 EU Data Protection Directive reinforces these conditions. Thus, to all intents and purposes, the rules for personal data processing expressly defined under Canadian law would apply to Galileo's global operations.

It is commonly assumed that the PNR is a standard, while in fact they can vary in size and format. In the 1970s, the International Air Transport Association (IATA) tried to establish certain standards and inter-operability mechanisms. More recently, the International Civil Aviation Organization (ICAO) has been considering the development of an international standard to implement uniform practices.[17] The issue has really been brought to the fore by the request by the US Department of Homeland Security (DHS) for the PNR data and Advance Passenger Information (API) data from all international flights arriving in the US. This prompted questions from the European Union about what PNR data might actually be included. The DHS then came up with a list of 39 separate data elements, subsequently reduced to 34.[18]

In June 2004, the US Department of Homeland Security head Tom Ridge signed an agreement with the EU that would allow US Customs and Border Protection (CBP) to collect airline PNR data from flights between the US and EU. Once implemented, the agreement will be in effect for three and a half years, with re-negotiations to start within one year of its expiry date. Under the accord, data will be retained by CBP for three and a half years unless associated with an enforcement action. In addition, only the 34 PNR data elements will be accessed by CBP to the extent collected in the air carriers' reservation and departure control systems and CBP will filter and delete 'sensitive data' (on medical conditions, meal preferences, religious affiliations, etc.) as agreed by CBP and the European Commission. At writing, the entire agreement is under review by the European courts.

The departure: the departure control system

Typically, 24 hours before departure, relevant fields from the PNR are transferred to the airline's Departure Control System (DCS), and the check-in agents will 'edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated. When I check in for my flight at Victoria International, Air Canada check-in staff would enter my last name (or the locator code) on the DCS, but they would not necessarily have access to the complete PNR. They would add my seat allocation (if necessary) as well as the information on any checked baggage. Around five to ten minutes before departure, a complete list of passengers by seat number is printed (Passenger Information List) and given to the in-charge flight attendant. The records for each flight are purged from the DCS within 24 hours after the flight has landed, and then archived in Air Canada's headquarters in Montreal.[19] If there are special requests from third parties after the PNR has been archived, they would have to be made in writing and considered at Air Canada headquarters.

Air Canada's databases are password-protected for its own staff and check-in agents, with different levels of access depending on status in the organization. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the DCS. If a passenger is taking an ongoing flight with a domestic carrier, the onward flight appears as an Air Canada coded flight on the passenger's ticket. The details transferred would only be the relevant stage booking, the immediately prior connecting flight and any special needs. 'Second' carriers do not have direct access to the complete journey details, booking contacts or PNR history. Air Canada employees in Canada will have been made aware through training of the general policy about the disclosure of reservations information. In general, employees are told not to disclose information about a passenger, including via the telephone, unless the information is given to: a colleague/another airline or agent for the purpose of reservation booking or ticket issue; the passenger himself and you have taken the necessary steps to ensure that this person is the passenger; some other person, and the passenger has clearly consented to this and there is a record of this in the PNR; an appropriate person or organization in an emergency to prevent injury or damage to someone's health. Employees are also advised orally that requests from the police or law-enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department.

Airline personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. A greater variety of more urgent requests arise within the airport context from local law-enforcement authorities (who have jurisdiction over most airports), from the federal Royal Canadian Mounted Police (RCMP), or from customs and immigration officials. Working within a closer environment, personal contacts obviously develop between individuals from different authorities. Air Canada staff are also, of course, frequently asked to check whether Mr or Mrs X is on a particular flight. They should not give out such information; anecdotal evidence suggests, however, that they often do.[20]

Responsibility for the process or pre-board screening is now the responsibility of the Canadian Air Transport Safety Agency (CATSA), the main institutional response of the Government of Canada to the events of 11 September 2001. On 1 April 2002, CATSA assumed financial responsibility for pre-board screening by reimbursing airlines for the cost of the service. At Victoria International, the pre-board passenger screening is contracted to a company called Aeroguard, the main organization responsible for pre-board screening in Canadian airports.[21] On entering the screening area, I was welcomed by the sign: 'Security measures are being taken to observe and inspect passengers. No passengers are obliged to subject to a search of their persons and goods if they do not choose to board an aircraft.' There would, however, be very few circumstances under which Aeroguard personnel would seek passenger identification. Any attempt to take surreptitiously a prohibited object onboard would almost certainly be a matter for intervention by an official from Commissionaires Canada, the company contracted to provide general security services at the airport, and/or by the RCMP.

The Victoria Airport Authority (VAA) is obviously responsible for ensuring that security measures are strictly enforced, but they do not now supervise the passenger or baggage screening process. There would be very few circumstances, therefore, where the VAA would need to know any identifiable passenger information. The one exception would be the video-surveillance system. When I boarded my flight at Victoria, my image would probably be captured on three sets of digital cameras (at pre-boarding, the curb and the ramp). Those tapes would be retained by the VAA for a week before being destroyed.[22]

Collecting 'points'

I have been a member of Air Canada's Aeroplan for about 15 years, and am now a 'Prestige' member. My Aeroplan number appears on the PNR and on my boarding card. Aeroplan is a division of Air Canada, though it has a separate privacy policy and Chief Privacy Officer. I have a profile with Aeroplan which will have been collected over the years from me personally when I enrolled, from partners (hotels, credit card companies, car rental companies and other airlines) from whom I have earned miles, and from other companies who are not Aeroplan partners to whom I might have consented to the disclosure of my information. None of these partners, however, should be disclosing any details about the various transactions, beyond the aggregate miles accumulation. Aeroplan's Direct Marketing System Club Profile Database is located in Point-Claire, Quebec.

Controversy erupted in July of 2001 when, in an attempt to conform to the provisions of the Personal Information Protection and Electronic Documents Act (PIPEDA), Aeroplan released a brochure entitled 'All About Your Privacy', outlining the conditions under which Aeroplan collected, retained and disclosed the personal information of its members. The brochure was made available to approximately 60,000 of the nearly 6 million members of the Aeroplan programme. It identified the many situations in which Air Canada would disclose the personal information of Aeroplan members, including sending membership lists to Aeroplan partners, who send 'information of interest' to Aeroplan's members. Membership information was also disclosed to companies outside of the Aeroplan programme for similar purposes.

Former Canadian Privacy Commissioner George Radwanski launched an investigation into the policies and practices of Aeroplan, to ensure that they were conforming with the provisions of PIPEDA. On 20 March 2002, Radwanski released his findings after a nine-month investigation and found that Aeroplan had 'not met its obligations under Principles 4.2.4, 4.3, 4.3.1, and 4.5 of Schedule 1 of the Act', concerning consent for the disclosure of personal information. He recommended that Air Canada should

> inform all Aeroplan members as to the collection, use, and disclosure of their personal information; explain to all Aeroplan members the purposes for the collection, use, and disclosure of their personal information. This is not done adequately in the current version of the 'All about your privacy' brochure; seek positive (i.e., opt-in) consent from all Aeroplan members regarding all information-sharing situations outlined in the brochure; establish appropriate procedures for obtaining positive consent; and execute appropriate agreements with all the direct-mailing houses it employs as agents to ensure that the personal information of Aeroplan members is protected in accordance with the Act.[23]

The Privacy Commissioner also found that, prior to the distribution of the brochure in July of 2001, received by fewer than 1 per cent of Aeroplan customers, Air Canada had made no attempt to obtain consent for the retention and disclosure of personal information. Radwanski also determined that the 'opt out' portion of the brochure constituted a 'negative option', wherein members were unwittingly providing consent unless they negated the possibility by virtue of a check mark. The Commissioner condemned the practice by ruling that 'negative or opt-out consent is not sufficient for any of the five situations described in the brochure'.

Aeroplan has subsequently amended its Privacy Policy to include a recognition of the 'importance of privacy for the Aeroplan Program', which includes a reference to the newly appointed Aeroplan Privacy Officer. The amended policy also addresses Aeroplan's commitment to privacy protection, which includes acceptance of responsibility for the personal information collected; a statement of justification for the collection of personal information; the limitations upon the collection, use, retention and disclosure of personal information; a statement concerning the importance of consent and accuracy; and a statement ensuring security, transparency, and a mechanism for addressing complaints.[24] It still, however, relies on the opt-out procedures for securing consent. On the website, and on brochures periodically sent to subscribers, customers are allowed to check a number of boxes if they do not want their personal information shared with other airlines, hotels, car rental companies, travel partners, financial partners, retail and entertainment services and telecommunication partners.[25]

Adding a border

Toronto–New York

At each leg of my journey from which I take departing flights with Air Canada (Victoria, Toronto, Kingston and Ottawa) my basic PNR is accessed and updated by Air Canada personnel. At each departing point, it is removed from the system within 72 hours of the completion of that leg of my travel. With this relatively simple trip within Canada, data on my flight arrangements obviously have appeared on the systems at these airports. But it is also held in Greenwood Village, Colorado and in Point-Claire, Quebec. Let us now analyse an onward flight to New York rather than to Ottawa, again with Air Canada. Let us 'add a border' to the scenario and trace my data shadow as I enter the United States and then return to Canada. Let us also say that I am attending a conference in New York, for which my hosts are paying my travel expenses and a modest honorarium.[26]

The North American Free Trade Agreement (NAFTA) allows certain 'Professionals' in 63 approved categories to enter the United States to carry out professional activities pursuant to a contract or an offer of employment, under the TN Classification. The visitor is advised that 'in addition to your proof of Canadian citizenship a letter from your prospective employer, or a signed contract may assist in your inspection by United States Immigration and Naturalization Service (USINS) officials.'[27] The letter or contract should include: job title and detailed summary of your duties; starting date and anticipated length of stay; arrangement for payment; proof that you have the necessary degree to work in the profession for which you are to be engaged; and professional-level qualifications (certified copies of your diploma/alternative credentials). The TN Visa also serves as a work permit and can be presented to the US Social Security Administration to receive a Social Security Number. The TN classification is generally issued for one year (with a $50 fee) and is renewable as long as you can demonstrate that your employment is temporary. If I were not performing any paid work, I would not require a visa and could travel between the US and Canada with one of the following documents: a Canadian passport; a Canadian government-issued birth certificate with government-issued photo ID; a Canadian Certificate of Naturalization, Canadian Certificate of Citizenship (laminated card) or Canadian driver's licence only when travelling from the US to Canada on the return portion of a roundtrip ticket.[28]

I would go through US Customs and Immigration Service (USCIS) at Toronto's Pearson International Airport. At that point, I would submit this documentation and fill in a USCIS Form I-94 (Arrival-Departure Record) with the VISA classification, the date I arrived in the United States and the 'Admitted Until' date, the date when my authorized period of stay expires. The USCIS inspector might ask me questions about the purpose of my trip, how long I would be in the United States, and my residence while in New York. The I-94 would be surrendered when I leave the United States.

There are, in fact, four separate inspections on entry to the United States: Public Health, Immigration, Customs and Agriculture. Most people would talk to one Immigration official, and one Customs official. For Customs purposes, I am also required to fill in a Customs Declaration Form (Form 6059B) which requires: name; birth date; number of family members travelling; US address; passport number; country of residence; countries visited on the trip prior to US arrival; airline number; primary purpose of trip; whether I am bringing in fruits, plants, food, insects, meats, animals, animal/wildlife products, disease agents, cell cultures, snails, soil from a farm, ranch, or pasture; whether I have been in close proximity to livestock; whether I am carrying more than $10,000 in currency or monetary instruments; whether I have commercial merchandise; and the total value of all articles that will remain in the US. The small print on the back of the form states ironically that the authority for collection is the 1995 Paperwork Reduction Act, that my response is mandatory and that the 'average burden associated with this collection of information is 4 minutes per respondent'.

All the information submitted through this application process on Forms I-94 and 6059B is theoretically protected by the US Privacy Act of 1974. USCIS could, however, reveal that information to an extensive list of federal, state or local agencies for law enforcement, public safety and other 'routine uses'. At this point in my travel, therefore, the list of US government agencies to which this information might potentially be revealed is extensive. Section 215 of the USA PATRIOT Act also authorizes the FBI to request an order 'requiring the production of any tangible things (including books, records, papers, documents, and other items)' relevant to an investigation of international terrorism or clandestine intelligence activities, without the traditional 'probable cause' test. This immigration data may, therefore, be disclosed, disseminated, matched or profiled within government with few restrictions. With the exception of the new USA PATRIOT Act requirements, this was also the case before September 11.

To whom in the United States, however, might the API or PNR data be revealed? Several schemes require discussion in this regard. The first is the US/Canada Smart Border Initiative signed between the two countries in December 2001. This constitutes a large package of security measures, including agreements on inter-operable biometric standards, permanent resident cards, refugee asylum claims processing, and the NEXUS programme to expedite air, land and sea crossings for pre-approved low-risk travellers. Canada and the United States have also agreed to share API and PNR data on 'high-risk' travellers destined to either country. The automated Canada-US API/PNR data-sharing program was due to be in place in Spring 2003. The two countries have also agreed on the co-location of customs and immigration officers in Joint Passenger Analysis Units to more intensively cooperate in identifying potentially high-risk travellers.[29]

Beyond these bilateral initiatives, the US has proposed three more general schemes for the collection and analysis of airline passenger data. The first, and most controversial, was the Computer Assisted Passenger Profiling System (CAPPS), the second generation of an earlier measure. The CAPPS II version was designed to receive PNR data from a new integrated database, cleanse and format the data, perform a risk assessment and then assign a risk 'score' to individual passengers entering the United States. The second-generation system was to rely on experimental data-mining algorithms to find patterns in the government and commercial databases available on individuals. In January 2003, the Transportation Security Administration (TSA) published a federal register notice announcing the creation of a new system of record called the Aviation Security Screening Records (ASSR) database. The notice described a system that would allow the government access to unlimited amounts and kinds of data from other proprietary and public sources: Passenger Name Records (PNRs) and associated data; reservation and manifest information of passenger carriers and, in the case of individuals who are deemed to pose a possible risk to transportation security, record categories may include risk-assessment reports, financial and transactional data, public source information, proprietary data, and information from law-enforcement and intelligence sources.[30] As a result of an enormous volume of criticism from Congress, civil liberties groups and other interests, 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.

Secondly, and as a result of recommendations of the United States National Commission on Terrorist Attacks upon the United States (2004), a successor to the CAPPS system emerged in August 2004. Secure Flight is intended to be confined simply to terrorist-related activities. Under this proposal, airlines will still have to submit passenger data to the agency, which will use an expanded, unified watch list run by the Terrorist Screening Center to flag potential threats. Homeland Security officials hope law-enforcement and intelligence groups will add more data to the watch list if they are assured the information will not be provided to private companies. That matching process is currently being tested with millions of passenger records, which the Transportation Security Administration ordered airlines to turn over in November 2004. The TSA further wants to test whether the information passengers provide to airlines can be verified using massive commercial databases run by companies such as LexisNexis and Acxiom. The government has claimed that this system is very different from its CAPPS predecessor because

privacy considerations have been built in from the outset. Civil liberties groups remain sceptical. They point to the fact that the watch lists currently in use have already been shown to be inaccurate, as exemplified by the high-profile example of Senator Ted Kennedy repeatedly misidentified as a suspected terrorist. It remains unclear how individuals who are improperly flagged will be protected.

A third, and related, proposal is the US-VISIT programme. The programme is a response to the Enhanced Border Security Act of 2002, wherein Congress directed the DHS to initiate controls on entry and exit points into the United States. Proposals were received in January 2004 and a contract was awarded to Accenture LLP on 28 May 2004. According to DHS:

> US-VISIT is part of a continuum of security measures that begins overseas, when a person applies for a visa to travel to the United States, and continues on through entry and exit at US air and seaports and, eventually, at land border crossings. The US-VISIT program enhances the security of US citizens and visitors by verifying the identity of visitors with visas. At the same time, it facilitates legitimate travel and trade by leveraging technology and the evolving use of biometrics to expedite processing at our borders. US-VISIT is helping us demonstrate that we remain a welcoming nation and that we can keep America's doors open and our nation secure.[31]

At the end of 2004, US-VISIT entry procedures were in place at 115 airports (including the major Canadian airports) and 14 seaports. It is scheduled to be expanded to the 50 busiest land ports of entry and to all 165 land ports of entry by 31 December 2005. US-VISIT begins at the US consular offices issuing visas, where visitors' digital fingerscans and photographs are collected and checked against a database of known criminals and suspected terrorists. When the visitor arrives at the port of entry, the same biometrics are used to verify that the person at the port is the same person who received the visa. This programme does not apply to citizens of 27 countries that participate in the Visa Waiver Program, although such citizens will need to submit machine-readable passports (or a valid US Visa) as of October 2004. US-VISIT has also been subjected to considerable scrutiny from a privacy perspective. Information gathered from US-VISIT may be shared with the usual list of federal agencies plus 'appropriate federal, state, local or foreign government agencies when needed by these organizations to carry out their law enforcement responsibilities.'[32] Canadian citizens are not yet subject to these rules, even though Canada is not a party to the Visa Waiver Program. Thus, at the moment, given my Canadian citizenship, there would be nothing different about my entry into the United States under the circumstances outlined above, from what would have occurred pre-9/11. Returning to Canada, however, would be a different story.

New York–Toronto

On my return to Canada, I would, as traditionally, be required to fill in immigration landing cards, and would be required to provide the following information: name, permanent address, date and place of birth, nationality, passport number, flight number, purpose of visit and the value of all goods being brought back to Canada. On arrival, I would surrender this card to Canada Customs which, some weeks later, will be processed and entered into the Canada Customs information system. Airline personnel will not have access to the information provided on these cards, although it may be shared and matched with data from other federal agencies.[33]

The collection and retention of the personal information of airline passengers entering Canada is regulated by the *Customs Act* of 1985. Canadian law also now requires that all commercial carriers and charter carriers provide the newly created Canadian Border Services Agency (CBSA) with information about all passengers and crew destined for Canada. The legislative amendments necessary to implement this initiative were included in Bill C-11, the Immigration and Refugee Protection Act, which received Royal Assent on 1 November 2001, Section 269 of which outlines the obligations of the carriers:[34]

> On the request of an officer, a commercial transporter must provide on departure of their commercial vehicle from the last point of embarkation before arriving in Canada the following information in writing on each person carried:
>
> (*a*) their surname, first name and initial or initials of any middle names;
> (*b*) their date of birth;
> (*c*) the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;
> (*d*) their gender;
> (*e*) their passport number or, if they do not have a passport, the number on the travel document that identifies them; and
> (*f*) their reservation record locator or file number.

> ***Passenger reservation information***
> (2) At any time after a commercial transporter undertakes to carry a passenger to Canada, the commercial transporter must provide an officer access to its reservation system or, on the request of an officer, provide in writing all reservation information held by the commercial transporter on passengers to be carried to Canada.

These regulations require that commercial carriers, charter operators, travel agents and owners/operators of a reservation system who undertake to carry persons to Canada must, at the time of departure, provide the Minister of Citizenship and Immigration with access to specific information on all passengers and crewmembers en route to Canada. The API data is collected at check-in time, and is transmitted by the carrier or reservation system prior to the arrival of the conveyance. At present these regulations only apply to air travel. It is argued that obtaining passenger information in advance of the arrival of a commercial conveyance will provide immigration officials with additional time to assess the specific risk of individual passengers and focus their attention on the passengers who pose the highest risk before they arrive at the border.

In order to receive the API/PNR data from the databases of the concerned third parties, Canada Customs and Revenue Agency (CCRA) contracted with the Société Internationale de Transportation Aéronautique (SITA) to provide the technology to bring API/PNR to Canada. CCRA developed a new tool entitled PAXIS, which is the user-end application needed to access API/PNR data, and began collecting this information in October 2002.[35] That information is now stored in the new Advance Passenger Information/Passenger Name Record (API/PNR) database. In March 2003, the more precise PNR data from airlines' departure control systems came online, and more and more airlines are increasingly becoming compliant. To effectively carry out this initiative, Canada Customs has established combined CIC/CCRA passenger assessment units (PAUs) at the three main Canadian airports (Vancouver, Toronto and Montreal). The primary role of the PAUs is to identify those travellers who, based on the information obtained from API/PNR, should be referred for an immigration 'examination'.

The construction of this database was the subject of a very high-profile conflict between the Canadian government and the former Privacy Commissioner, George Radwanski, the result of which were certain constraints on how this information might be used. Advance Passenger Information (API) – which consists only of passport information such as name and date of birth and does not include any specific travel information – will continue to be stored for six years and can be widely shared under Section 107 of the Customs Act. The much more detailed Passenger Name Record (PNR) will immediately be purged by the CCRA of all meal and health information.

PNR data will still be held for six years, but use and access will vary by length of retention. For the first 72 hours, it will be used by customs and immigration officers to assess risk. From 72 hours to two years, the information will be depersonalized and used, without names attached, only by intelligence officers and analysts. The information can be re-identified with the traveller's name only when necessary for customs purposes. During this two-year period, information will only be shared with other agencies or departments for non-customs purposes if a warrant has been obtained, including for tax-evasion purposes. From two years to six years, the information can only be used to fulfill the CCRA's mandate regarding the security of Canada, rather than all customs purposes. It will be used on a depersonalized basis unless the Commissioner of the CCRA personally approves re-personalizing it based on reason to suspect that the name or other identifying elements are necessary to deal with a high-risk person. During this final period, information can only be shared with agencies that have a national security mandate, where there are reasonable grounds to believe that the information relates to a real or apprehended threat. Commissioner Radwanski hailed this compromise as a great victory for the privacy rights of Canadians.[36] Others were more sceptical.[37]

Conclusions

The literature on privacy, surveillance and all the attendant issues surrounding the processing of personal information is replete with images and metaphors about how each individual has a 'data shadow' (Stalder 2002) or perhaps a 'digital persona' (Clarke 1994). The new networked society (Castells 1996) produces a proliferation of remotely captured and stored personal data that may or may not correspond with an individual's actual personality or behaviour. These fragments of personal data supposedly exist in a non-transparent, mystical and complex world over which the individual has little knowledge and no control. In the theoretical literature of post-modernity, this condition supports wider arguments about the dissolution of the 'subject' and of traditional borders between individual and society, public and private, self and other, and so on (e.g. Poster 1990).

Whether in its more sophisticated and theoretical version, or its more rhetorical or polemical variant, this theme is rarely supported by detailed empirical investigation into the nature of databases and the flows of information between them. We are left with a range of often insightful conclusions about the nature of the surveillance society, none of which have been, or indeed can be, subjected to rigorous empirical scrutiny. That empiricism is necessary if analysts and advocates are to understand the fundamentally contingent or 'Janus-faced' nature of contemporary surveillance practices (Lyon 2001), and also to comprehend how their worst effects might be remedied.

Certainly the endeavour of tracing my data shadow with respect to the flights described in this paper resonates with some important themes in the contemporary literature. The collection of personal information is largely characterized by a process of automatic 'data capture' (Agre 1994), rather than visual monitoring. Unawares, I left behind a 'data trail' (Cavoukian and Tapscott 1997). Most of these transactions have taken place at a distance, reinforcing Lyon's point about 'disappearing bodies' (2001: 16–27). To the extent that 'my' data, even concerning a simple flight within Canada, have ended up in the United States, supports larger points about globalization and especially about the 'de-localized' border (Lyon 2003: 110); I did not have to cross a geographical or national border for 'my' data to do so.

If one confines the analysis for the moment to the travel *within* Canada, certain conclusions can be reached about my abilities as a data subject to access my information and to control its circulation. The following organizations have had access to the basic information about my flight plans: the local travel agency, Galileo, Air Canada and Aeroplan. The Victoria and Toronto Airport Authorities would also have access to my images captured at various stages in both airports. Each of these institutions is regulated by federal privacy protection legislation and should therefore be abiding by the standard fair information practices.[38] With the exception of the travel agent, each institution has developed a tailored code of practice for the benefit of consumers and employees. From my brief interviews with representatives from these organizations, I became convinced that the protection of the personal information of travellers was something that each took very seriously. There are of course important differences between rules and practices, and I have already noted how informal networks develop in an airport environment which can facilitate the unwarranted sharing of personal information.

Thus, for anyone with a little time and energy, it is possible to discover who has what information, when about a particular flight itinerary. These institutions rarely receive requests for personal information, but they are all obligated to provide it – even Galileo Canada, which claims that it is not. The prevailing assumption in much of the literature that surveillance is removed, invisible, non-transparent, mystical, complex and so on, is therefore overdrawn. It is difficult to trace one's 'digital persona', but it is not impossible. While it is common in the surveillance literature to critique the concept and policies of privacy protection, it is also true that those very policies oblige organizations to be far more forthcoming about what data they collect and store. Transparency of 'systems of records' is one of the unrecognized values of information privacy and data protection policy. Privacy is not *the* antidote to surveillance (Stalder 2002), but it is the only conceptual and legal framework available to achieve some organizational accountability and transparency.

Have I been the subject of surveillance or, more precisely, 'dataveillance' (Clarke 1989)? Again, the literature would suggest that any capture of personal information (however benign) constitutes a surveillance process. Surveillance, Lyon contends, is 'any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered.' It is simply the outcome of the 'complex ways in which we structure our political and economic relationships' (2001: 2). Marx (1988) has also argued that there is a 'new surveillance' – routine, everyday, invisible and pre-emptive. Linked to this broad definition is the power of classification and sorting. It is a powerful means of creating and reinforcing social identities and divisions (Gandy 1993; Lyon 2003).

Without dissenting from these judgements, two insights suggest themselves as a result of the case studies above. First, my personal data (so far as I know) has not been processed for any purpose beyond that of ensuring that I am a valid passenger on the days and flights reserved. It has not been analysed, subjected to any investigation, manipulated or used to make any judgement about me. No doubt, a certain amount of data mining of de-identified information occurs within the industry to analyse general travel patterns and demands. No doubt, had I not opted out under the Aeroplan privacy policy, my data might have ended up with a variety of Aeroplan's partners, and I might have received related, and unrelated, promotional materials.

It seems, however, that there is a fundamental difference between the routine capture, collection and storage of this kind of personal information, and any subsequent analysis of that information from which decisions (benign or otherwise) might be made about me. The new process for API/PNR analysis serves to highlight the distinction. As a passenger, when I return to Canada, that information is automatically transferred ahead of my arrival to the CCRA's Passenger Assessment Unit at the Canadian airport, and it is systematically analysed. Anybody within a 'high-risk' category is then subject to further investigation. The crucial process, therefore, is not the capture and transmission of the information, but the prior procedures, and the assumptions that underpin them, about who is or is not a high-risk traveller. Surveillance might be 'any collection and processing of personal data, whether identifiable or not.' If we are to use such a broad definition, however, we need to find another concept to describe the active intervention of human agents who then monitor that data to make decisions about individuals. 'Surveillance' conflates a number of distinct processes. To describe what has happened to me as surveillance perhaps serves to trivialize the real surveillance to which some individuals, perhaps with 'risky' surnames and meal preferences, can be subjected during air travel.

Surveillance is, therefore, highly contingent. If social scientists are to get beyond totalizing metaphors and broad abstractions, it is absolutely necessary to understand these contingencies. Social and individual risk is governed by a complicated set of organizational, cultural, technological, political and legal factors. The crucial questions are therefore distributional ones: Why do some people get more 'surveillance' than others (Bennett and Raab 1997, 2003)? But to address those questions, it is crucial to conduct the kind of finely tuned empirical studies such as the one attempted above.

These case studies have revealed something about the information flows when a fairly typical traveller books an airline ticket. In this context, the nature and extent of the surveillance, and thus of individual risk, is highly dependent on methods of booking, on local practices, on legal rules, on networks and interfaces, and on the behaviours and preferences of the individual. Students of surveillance have a responsibility to study these processes in far greater detail. We must try to trace the information flows, and thus interrogate Castells' major hypothesis about the 'space of flows' within the network society, in which 'dominant functions are organised in networks pertaining to a space of flows that links them up around the world, while fragmenting subordinate functions, and people in the multiple space of places, made of locales increasingly segregated from one another' (Castells 1996: 476). 'What happens when you book an airline ticket' is a complex question, but it is not unfathomable. My tentative answers certainly reveal a dominant network, represented by Galileo and other global distribution systems, as well as a number of segregated locales, at which localized data capture, but hardly pernicious surveillance, has occurred.

Notes

[1] Available at: http://web.uvic.ca/polisci/bennett/index.htm#online

[2] My thanks to Dean Murdock for the diligent and careful research assistance upon which this paper is based.

[3] 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 offer computerized reservation systems to airlines, travel agencies, rental companies and hotel chains. The others are Worldspan and Amadeus.

[4] http://www.thomascook.ca/About/PrivacySecurityOnline.aspx
My customer profile includes the following: name, designation, contact information, preferred language, nationality, date of birth, membership numbers (for frequent flyer points), credit card numbers, passport number, e-mail address, my flying preferences (seat, meals, etc.) and my beneficiary (for insurance purposes).

[5] Source: http://www.acta.ca

[6] Typical pressures arise when a travel agent is asked whether a third party is on a particular flight; when client profiles are transferred from one agency to another; and when client data have to be communicated in cases of emergency.

[7] Source: http://www.galileo.com

[8] Nothing in the Air Canada conditions of carriage statements (that appear on the reverse of paper tickets) mentions the collection and disclosure of personal information. Air Canada's privacy policy is available at: http://www.aircanada.com/en/about/legal/privacy/policy.html

[9] See the critique of the security of these web portals by Edward Hasbrouck, 'Who's Watching you While you Travel?' Available at: http://www.hasbrouck.org/articles/watching.html

[10] There are no indications on the Galileo system that a passenger can access his or her PNR from Galileo. Indeed, the Galileo Canada website expressly indicates that 'as a processor of data, Galileo Canada does not conduct business directly with individual travelers. Upon request, individual travelers may have access to their own data held by the Galileo system by contacting the travel agent involved in the booking' (Source: http://www.galileocanada.ca/privacy/2/). I asked the travel agency for my PNR and was told that it was not their practice to disclose this information as they were only accessing the remote network. Although I did not press the issue, the travel agency would legally be responsible for providing access.

[11] Hasbrouck (2004) suggests the following: 'prefers king bed', 'prefers room on low floor in hotels', 'always requests halal meal', 'won't fly on the Jewish sabbath', 'uses wheelchair, can't control bowels and bladder', 'prefers not to fly Delta Airlines'. Travel agents might add information like 'difficult customer – always changing his mind'.

[12] Air Canada provides the following meal choices: Asian vegetarian, bland/ulcer, child, diabetic, fruit platter, gluten-free, Hindu non-vegetarian, kosher, low calorie, low cholesterol, low salt, Muslim vegetarian, non-lactose, oriental, regular, vegetarian (lacto-ovo), and vegetarian. It provides the following Special Needs options: assistance climbing steps, assistance when on plane, blind, hearing impaired, wheelchair in terminal.

[13] Galileo Canada Privacy Policy available at http://www.galileocanada.ca (my emphasis).

[14] There is just a policy that applies to the collection of information through the website itself.

[15] Telephone conversation with Thomas de May, Chief Privacy Officer, Galileo, 5 August 2004.

[16] See: European Parliament, Directorate General for Research, *Working Paper on The Rights of Airline Passengers* (1999). Available at: http://www.europarl.eu.int/workingpapers/tran/105/default_en.htm

[17] FAL/12-WP/74, 153/04, 'Airline Reservation System and Passenger Name Record Access by States'. ICAO Facilitation Division – Twelfth Session, Cairo, Egypt, 22 March to 2 April 2004. Available at: http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp074_en.pdf

[18] PNR Data Elements Required from Air Carriers and Global Distribution Systems (GDS) Federal Register / Vol. 69, No. 131/Friday, July 9, 2004. 1) The PNR record locator code. 2) Date of reservation. 3) Date(s) of intended travel. 4) Name. 5) Other names on PNR. 6) Address. 7) All forms of payment information. 8) Billing address. 9) Contact telephone numbers. 10) All travel itinerary for specific PNR. 11) Frequent flyer information. 12) Travel agency. 13) Travel agent. 14) Code share PNR information. 15) Travel status of passenger. 16) Split/Divided PNR information. 17) E-mail address. 18) Ticketing field information. 19) General remarks. 20) Ticket number. 21) Seat number. 22) Date of ticket issuance. 23) No show history. 24) Bag tag numbers. 25) Go show information. 26) OSI information. 27) SSI/SSR information. 28) Received from information. 29) All historical changes to the PNR. 30) Number of travelers on PNR. 31) Seat information. 32) One-way tickets. 33) Any collected APIS information. 34) ATFQ fields.

[19] Telephone interview with Gail Paul, Air Canada manager, Victoria International Airport.

[20] I am indebted on this point to a paper written by a former student, who had worked as a customs agent at Vancouver International Airport. Khushwant Dhillon, 'Profiling by Canada Customs at Vancouver International Airport'. (Admn 548, April 2002).

[21] Source: http://www.aeroguard.ca/index.html

[22] Interview with Bruce MacRae, Victoria International Airport Authority, 3 August 2004.

[23] News Release on 20 March 2002, from the Office of the Privacy Commissioner of Canada. Available at: http://www.privcom.gc.ca/media/nr-c/02_05_b_020320_e.asp

[24] Aeroplan 'Privacy Policy'. Source: https://www.aeroplan.com/en/about/privacy.jsp The new policy reads:

> 1. We will only collect the personal information necessary to administer the Aeroplan Loyalty Program and to offer our members rewards, benefits, products, goods and services under the Program.

2. We do not collect, use or disclose personal information about a member without the consent of the member, except where required by law.
3. From time to time we may transfer personal information to our agents for processing in order to determine which members may be most interested in rewards, benefits, products, goods and services offered by Aeroplan or its Partners. We use contractual and other means to protect your information while it is being processed by our agents.
4. To increase opportunities for members to accumulate miles under the Program, to facilitate the redemption of miles under the Program, or to obtain special benefits for members, Aeroplan® may temporarily share personal information with a Partner. Use by the Partner for any purpose other than the Aeroplan Loyalty Program is strictly prohibited.
5. We will provide our members with a detailed explanation, when they enroll and periodically thereafter, of how they can have their name deleted from the lists we share with our Partners. Our members may contact us at any time at the address below to have their names deleted from the lists.
6. We maintain the security and confidentiality of the information furnished by our members according to the strictest standards. Compliance with these standards is constantly verified and revised as needed.
7. In the administration of the Aeroplan Loyalty Program, if we communicate information to our Partners, agents, or representatives, we assume the responsibility arising from these communications and take actions to ensure that the commitments and rules set forth in this Policy are observed by our Partners, agents, or representatives.
8. We require every organization that provides us with administrative or information processing support services to comply with this Policy and with the privacy protection rules it contains.
9. Our members are entitled to examine the information we hold regarding them, subject to the restrictions provided by law, and may request rectification of inaccurate or incomplete information. If applicable, we will disclose this information to the person concerned or rectify it promptly.

[25] Source: https://www.aeroplan.com/en/about/removal.pdf Aeroplan 'Opt-Out request form'. I have 'opted-out'.

[26] Many of the relevant rules have been derived from the website: http://www.foreignborn.com

[27] Source: http://www.dfait-maeci.gc.ca/nafta-alena/temp_entry-en.asp

[28] Canadian permanent residents and landed immigrants now require government-issued photo ID (The Maple Leaf card) when travelling to the United States.

[29] Department of Foreign Affairs and International Trade, Smart Border Action Plan Status Report. Available at: http://www.dfait-maeci.gc.ca/can-am/menu-en.asp?act=v&mid=1&cat=1&did=2465

[30] Federal Register: 15 January, 2003 (Volume 68, Number 10)][Notices] [Page 2101-2103] at: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-827.htm

[31] Source: http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml

[32] Source: http://www.dhs.gov/interweb/assetlibrary/USVISITPrivacyPolicy.pdf

[33] In 1999, the Federal Privacy Commissioner challenged the constitutionality under the search and seizure provisions of the Canadian Charter of Rights and Freedoms of a data matching arrangement between Canada Customs and Human Resources Development Canada (HRDC) for the comparison of these customs data with unemployment insurance records. At issue is HRDC's practice of collecting data from the Customs declarations of every returning traveller to identify employment insurance claimants (supposedly available for work) who were out of the country while receiving benefits.

[34] The Public Safety Act also regulates access to API/PNR data. See: http://www.tc.gc.ca/mediaroom/releases/nat/2002/02_gc004e.htm

[35] Customs Act, Section 107 (1) reads: 'The Minister may, under prescribed circumstances and conditions, require any prescribed person or prescribed class of persons to provide, or provide access to, prescribed information about any person on board a conveyance in advance of the arrival of the conveyance in Canada or within a reasonable time after that arrival.'

[36] Source: http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp

[37] See, for example, the analysis of the Canadian Civil Liberties Association at: http://www.ccla.org/privacy/api-pnr.shtml

[38] Ironically, the only institution that bears no legal responsibility for data protection is Queen's University; Ontario universities still are not regulated under Ontario's Freedom of Information and Protection of Privacy Act.

References

Agre, P. (1994) 'Surveillance and Capture: two models of privacy', *The Information Society*, 10, pp. 101–27.

Bennett, C. (1999) 'What Happens When you Buy an Airline Ticket? Surveillance, globalization and the regulation of international communications networks', paper presented to annual meeting of Canadian Political Science Association, Sherbrooke, Quebec, at: http://web.uvic.ca/~polisci/bennett/index.htm#online

Bennett, C. and Raab, C. (1997) 'The Distribution of Privacy Risks: who needs protection?', *The Information Society*, 14, pp. 263–74.

Bennett, C. and Raab, C. (2003) *The Governance of Privacy: Policy Instruments in Global Perspective* (Aldershot, UK: Ashgate Press).

Castells, M. (1996) *The Rise of the Network Society Vol. 1* (Oxford: Blackwells Press).

Cavoukian, A. and Tapscott, D. (1997) *Who Knows? Safeguarding your Privacy in a Networked World* (New York: McGraw-Hill).

Clarke, R. (1989) 'Information Technology and Dataveillance', *Communications of the ACM*, 31, pp. 498–512.

Clarke, R. (1994) 'The Digital Persona and its Application to Data Surveillance', *The Information Society*, 10 (2); also at: http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html

European Union (1995) *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (Brussels: OJ No. L281, 24 October 1995).

Gandy, O. (1993) *The Panoptic Sort* (Boulder: Westview Press).

Hasbrouck, E. (2004) 'Travel Privacy', in *Privacy and Human Rights Yearbook 2004* (Washington, DC: Electronic Privacy Information Center).

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press).

Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy Risk and Digital Discrimination* (London: Routledge).

Marx, G. (1988) *Undercover: Police Surveillance in America* (Berkeley: University of California Press).

Poster, M. (1990) *The Mode of Information* (New York: Polity Press).

Raab, C., Bennett, C., Gellman, R. and Waters, N. (1998) *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer* (Luxembourg: Office for Official Publications of the European Commission, at: http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/adequat.htm).

Stalder, F. (2002) 'Privacy is not the Antidote to Surveillance', *Surveillance and Society*, 1:1, at: http://www.surveillance-and-society.org/journalv1i1.htm

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

Chapter 9

Potential threats and potential criminals: data collection in the national security entry-exit registration system[1]

Jonathan Finn

On 5 June 2002 United States Attorney General John Ashcroft announced the National Security Entry-Exit Registration System (NSEERS). The initiative captures and archives biographic data and images of the faces and fingerprints of select foreign nationals visiting or residing in the United States on temporary visas. Because all of the 19 individuals involved in the 11 September 2001 hijackings entered the United States on valid temporary visas, NSEERS was promoted as a program to prevent future terrorist attacks and enhance border security through rigorous documenting and monitoring of visitors to the United States.

The registration system is based in a 1996 Congressional mandate, entitled the Illegal Immigration and Immigrant Responsibility Act, that the United States develop a comprehensive entry-exit registration system to record nearly all of the country's 35,000,000 annual visitors. On 5 January 2004 the United States Visitor and Immigrant Status Indicator Technology program (US-VISIT) was implemented to fulfill this mandate and to succeed NSEERS. Both programs collect detailed biographic information along with fingerprint scans and full-face, frontal photographs (hereafter referred to as photographs) from persons entering the United States. In over a year of operation, NSEERS had compiled data on 177,260 individuals (USDHS 2003). By comparison, in just three months of operation, US-VISIT had processed 3,002,872 individuals (USDHS 2004).