Transforming Travel and Border Controls: Checkpoints in the Open Society

Ian Hosein
Visiting Fellow, Department of Information Systems, The London School of Economics and Political Science
Senior Fellow, Privacy International

Abstract

Prior concerns regarding terrorism resulted in a rush to legislate. Now terrorism is not the only issue in the new security agenda, and we appear to have stopped rushing our legislative processes. Yet policies are still emerging with a lack of public discourse and legislative deliberation. This article reviews two such policies: access to personal information held by airlines, and new border practices that include the collection and processing of biometrics. By looking at the negotiations between the U.S. and the European Commission on passenger name records (PNR), the debates in Canada regarding the collection of passenger information, and the deployment of the US-VISIT system, we identify a number of policy dynamics. We can see within these dynamics of policy formation some essential ingredients for discourse and deliberation, which may inform future debates. In particular, this article argues that we may inform policy by looking at the international, regulatory, legal, and technological dynamics of policy.

Biographical Statement

Ian (Gus) Hosein is a Visiting Fellow in the Department of Information Systems at the London School of Economics. He is a Senior Fellow with Privacy International where he directs research on anti-terrorism policies, and co-ordinates a project on international policy dynamics. He is also an advisor to the American Civil Liberties Union on international technology policy issues. For more information please see http://personal.lse.ac.uk/hosein.

About this Research

Some of this research has been previously presented in publicly available reports and discussion documents. None of these give rise to any copyright issues, however, since they are all in the public domain, as published by Privacy International on its website. The analysis presented here is unique to this paper, however. As a result of this earlier public circulation, this work has benefited from reviews by colleagues in other organizations and scrutiny from presentations to public and private sector audiences. In particular I would like to acknowledge the advice and input of Ian Angell, David Banisar, Tony Bunyan, Simon Davies, Andreas Dietl, Edward Hasbrouck, Frank Land, Jay Stanley, Barry Steinhardt, Edgar Whitley, and Jean-Marie Willigens. I attest that all the work presented in this paper is my own. Components of this research were funded by the Open Society Institute Information Programme, the American Civil Liberties Union, and the Social Science Research Council.
Transforming Travel and Border Controls: Checkpoints in the Open Society

1 Introduction

In a sense, this paper follows a trip that I am currently taking. At the moment of writing these very words, I am at somewhere around 35,000 feet above the Atlantic Ocean, en route to New York City from London, via Montreal.

In traveling through three jurisdictions in seven hours, it is difficult to tell how many different laws apply, and how many institutions have access to my personal information. We aren’t all that shocked by this concept; after all this is the very legal confusion that globalization was promised to provide. As it becomes difficult to identify which regulatory regimes are at play at what point of the trip, it also becomes more difficult to identify the responsible authorities. The greatest challenge is to try to understand how we got here in such a short period of time.

On this trip, I am to go through a number of checkpoints. First my airline records additional information about me, and is now required to verify all this information against my passport. Often the carriers also look to see if I have a legitimate visa to travel to my destination, for fear of fines being levied against them. Some of this is due to combating terrorism, but there are other factors too: immigration control is increasingly on the public agenda. Airlines are facing increased scrutiny to transform their traditional role, conveyors of people, to deputies of a variety of states’ immigration and security policies.

The next checkpoint is in Canada. The Canadian Government is well-aware that we are on our way, as the carrier has already handed overall the reservation information of those on the flight, probably before the flight even left. Similarly, the next border point is likely to know of our impending arrival, as data is also made available to the U.S. Government. Decisions are constantly being made as to my legitimacy as a traveler.
When we move on to the next checkpoint, the United States immigration checkpoint in Canada, another novel event occurs. At this U.S. checkpoint, my companion’s fingerprints and facial image are collected, to be stored for up to 100 years. My companion's fingerprints are then compared to existing fingerprints on a wanted-list, her travel records will be analyzed with previous transactions and visa requirements, and this information will be made available to a multitude of departments, agencies, and institutions.

My British traveling companion will likely encounter a checkpoint as she leaves the U.S. where she'll have to again give her fingerprints. And upon return to the United Kingdom, Her Majesty’s Customs and Excise will also have access to the files in the carrier's database.

Access to all this data sounds quite reasonable. After all, this is the age of the 'new security agenda', in a post-September 11, -March 11, and –July 7 world. We expect that behind every scene, the national security and law enforcement authorities of a number of states are busy at work ascertaining whether travelers pose security threats, immigration problems, and other unrelated troubles.

But these rising checkpoints represent recognizable shifts in international and national policy environments. While changes have been introduced since September 2001 to deal with terrorism, increasingly these measures are not limited to combating terror. These measures necessarily involve the deputization of other non-state actors, notably carriers. The policies also apply to non-residents, who traditionally hold fewer rights – it is unlikely that these individuals will refuse to consent. These policies increase the collection of information and surveillance of individuals to an unprecedented level. These changes are generating tremors in the international landscape; creating obligations upon other countries to amend their own laws or otherwise face sanctions.

One would imagine that this vast collection of information, transformation of laws, restructuring of an industry’s information practices, and the fingerprinting of the masses would generate public controversy. Yet there is a remarkable silence surrounding these
shifts and the legislative processes leading to them. The European Union was forced into changing its privacy laws because of American anti-terrorism laws that demanded access to passenger data. Canada significantly amended its own privacy laws in order to gain access to passenger data, and is also demanding it from other jurisdictions. The U.S. is compiling vast dossiers on all visitors, including all ten fingerprints and travel patterns. Under normal circumstances, such changes in law would be quite controversial.

And so we are left with this conflict: it appears natural to demand more information, but these demands have resulted in significant shifts in policies at both the national and international levels. The goal of this article is to peer inside these policies to see how they were developed and implemented. Though there was limited public debate and legislative deliberation, we must look at the debates that (may have) occurred to understand the contentions and controversies. Looking through the policies outlined above, we may learn something about this ‘new security agenda’ that is both able to transform law and reduce controversy. By studying the dynamics of these limited debates, we may identify dimensions of modern policy-making, so as to inform future debate.

2 On Silent Discourses

When I speak at conferences outside of the U.S. on issues relating to anti-terrorism policy, the audience often wants me to focus on the United States. First they want me to speak ill of its unilateralism. Instead I remind them that the U.S. has been conducting the war on terrorism in very multilateral way, working through a number of international institutions, for better or for worse.¹

Audiences also want me to speak ill of its civil liberties record, of the USA-PATRIOT Act, of discrimination, of transgressions and so forth. My response is often disappointing and annoying, for those in the audience at least. First I note that the situation in the U.S. will improve, that there have been political and legal victories in areas where there have been civil liberties infringements. Second, the level of public discourse in the U.S. is high: there are media institutions raising awareness of abuses, independent inspectors investigating
transgressions, and non-governmental organizations drawing attention and appealing for recourse. Third I declare (exaggerating mildly) that the USA-PATRIOT Act is not the big bad law that everyone outside the U.S. thinks it is; in fact, most other countries already had many of the powers enshrined into law before September 2001. Also, there are many other more highly problematic U.S. laws that we should be focusing on.

I then ask the audience to raise their hands if they can name the law passed by their national legislatures in response to the events of September 11, 2001. On average only a quarter of the audience raises their hands. I conclude my talks, usually, by saying that I do not worry about the U.S. and U.S. law: American public policy discourse will resolve many of those problems, at least in the high profile cases. I worry about the lack of discourse and deliberation elsewhere. I worry that legislatures are not held accountable, that there is a lack of alternative voices with sufficient expertise, and there is a lack of media attention. In America, these institutions and dynamics will solve American problems whenever they apply to Americans, but who will solve everyone else's? We hardly notice the lack of discussion, debate, and deliberation.

Yet we do complain about the rush to legislate that occurred after September 11, and we were concerned about facing a barrage of policy following the subsequent attacks such as those in Bali, Madrid, and most recently in London. Whether it was the UK's Anti-Terrorism Crime and Security Act that received Royal Assent in December 2001, or the similarly timed Anti-Terrorism Act in Canada, we hear repeatedly from commentators of the 'post-September 11 rushed legislation'. It seems that we believe that some other, slower processes would have reduced the risks of bad policy.

I imagine that our concerns regarding these 'rushed' acts may be because we fell that this is inimical to our ideas of the Open Society. To this day one of my favorite quotations at the start of a book still comes from Popper's *Open Society and its Enemies Volume I*, from Pericles: "Although only a few may originate policy, we are all able to judge it." In an Open Society, social actors yearn for improving society, knowing that no one has perfect knowledge or control of the outcome of decisions - thus creating a space for further actors...
to join in and participate. It is taken for granted that actors are able to contribute, to participate, and to submit their ideas for consideration.

I am therefore assuming that we are concerned that the rush to legislate has reduced our ability to question policy, to further deliberation, to improve our laws. Yet even as we have moved on from the post-September 11th period, well after the wake of other calamities, similar policies continue to emerge and the public discourse continues to be relatively quiet, and the deliberation remains minimal. We have broadened our agendas from a war on terrorism to what may be referred to as a 'new security agenda', incorporating other wars (e.g. narcotics) and agendas (e.g. immigration and people-trafficking). New policies are being introduced not merely in the name of combating terrorism. The stated purposes now stretch into disparate domains of the provision of more effective public services, combating fraud, managing immigration, amongst many others. Yet we continue to suffer from a lack of public discourse and careful deliberation on important policies emerging under this security agenda, as we unwittingly challenge the Open Society.

2.1 Identifying the Dynamics of Policy

Traditionally, policies are created through a deliberative process, involving policy discourse where we learn the implications and debate the benefits of policy change. We need to concentrate our analyses on policy discourse, and the dynamics that arise. Policy discourses are an ever-changing mosaic, a tapestry of varying forces and processes that are dynamic, fluid, and loosely joined, involving actors, arguments and mechanisms. To study policy, we need to focus on the negotiation and transformation of the policy and the surrounding institutions.

At the risk of a normative statement, deliberative discourse may lead to better policy, institutions, and technology. Using the example of safety mechanisms in nuclear reactors, Giandomenico Majone argued that its development in the West vs. in the Soviet Union was due to the public discourse that occurred, due to the deliberative processes of democratic governments. Open deliberation led to safer nuclear technology. Extending this logic, one
would hope that deliberation on travel and border policies would lead to better policy. To avoid further normative statements, I leave the evaluation of the constitution of 'better policy' to others to discuss, while I will limit my focus to the dynamics of policy formation, studying the discourse and the deliberation.

Looking at contemporary policies, it is possible to say that the new security agenda has transformed the process through which policy is established in a variety of ways. Policies are increasingly imported from other fora, decided outside of traditional bodies and legislatures, and approved with little debate. Many of the policies that are established through these processes are inattentive to privacy, civil liberties, and other legal rights. We altogether ignore some of these policies because they do not affect the citizenry directly. And the regulatory aspects of these policies are often ignored because of the coercive power of governments to impose sanctions, or unwillingness to consider costs and burdens. Lurking within all of these are the technological dynamics, the roles and effects of the technologies that are implicated by these policies. The technological dynamics are poorly attended to within what little discourse and deliberation that exist. These international, legal, regulatory and technological dynamics are not necessarily distinct forces, but instead they intermingle. We need not to identify and reify one over the other, but rather we may approach the policy process with the awareness of their existences.

If one were to imagine an ideal policy formation process, it would involve a multiplicity of actors, inside and outside of Government institutions, negotiating and comparing ideas in a public discourse, informing a deliberative process that is open and considered. The purpose of the discourse and deliberation is not necessarily consensus, nor the generation of perfect information and perfect policy, but rather to inform the policy-making process, providing feedback and allowing for change in the direction of the policy. If we are to inform policy discourse and deliberation within the new security agenda, we need to attend to the international, regulatory, legal, and technological dynamics.

These dynamics will be investigated in the situations below. First I will review the transfer and use of travel information to look at the non-state actors who are implicated, the legal
challenges and international conflicts, and how the nature of the information itself affects the other dynamics. I will also review the collection of information at border checkpoints, studying the assumptions regarding the technologies, the legal implications, the pressures emerging from non-state actors, and the international dynamics behind this practice. Together these cases will be used to promote the virtue of enlivened and enhanced policy discourse and deliberation by looking at various policy dynamics.

3 Transformation of Travel

Even before my boarding of the plane to travel to the United States, the U.S. Government was aware of my intent to travel. Even before my arrival in Canada, the Canadian authorities knew of my impending arrival. This information was made available to these Governments by my airline and will be retained by these Governments for future use.

The use of personal information for the purpose of travel has grown significantly in recent years. This is in part due to the progress of technology, but much of it can be attributed to policies arising after the events of September 11, 2001. Increasingly, detailed passenger information is being sent to governments by carriers. Governments intend to mine this information to better understand visitors and air passengers to assess the threat they may pose as terrorists, immigration violators, and criminals.

3.1 EU and U.S.

As I live in the United Kingdom, any personal information received by the U.S. Government from any carrier that travels from the European Union (EU) involves a ‘trans-border data flow’. That is, information is being transmitted from the legal jurisdiction of European law into the jurisdiction of U.S. law; and this flow is the matter of conflict.

For a number of years, there has been a significant conflict on the issue of the transfer of information about airline passengers between Europe and the United States. And it is not just a conflict between the U.S. Government and European Union institutions, as it is often painted. It may also be seen as a conflict of the institutions on both sides of the Atlantic,
between those who value privacy and the limits placed on governments’ intrusions, and
those who would like to create permanent infrastructures for the regular observation of
individuals’ travel patterns. Even this latter view is simplistic because in truth this is a
policy debate that implicates many more actors, and gives rise to technological, regulatory,
and legal complications beyond privacy.

The origin of the conflict is the decision by the U.S. Government to rely heavily on an
information-based approach to preventing terrorism. This was not merely a response to
September 11; under the Clinton Administration the Federal Government began a primitive
computer profiling system for passengers to measure their risk. After September 11 it was
felt that this approach was sound but a more sophisticated system was required and moved
to develop it. The U.S. Government also wanted advanced notice of those who were
coming to the country. As part of this strategy, the U.S. is seeking a sharp increase in the
amount of information that airlines must provide to U.S. authorities about their passengers
– a requirement that depends on the cooperation of other nations, including Europe, which
have strong privacy laws that must be reconciled with the U.S. request.

The origin of the passenger information conflict is one of the many pieces of legislation
passed by the U.S. Congress in the wake of September 11, the *Aviation and Transportation
Security Act 2001*. This law instituted a requirement that foreign carriers "shall make
passenger name record information available to the Customs Service upon request" (ATSA,
Section 115(c(3))), and provided for this information to be shared with other agencies
outside of the Transportation Security Administration. The availability of this information
was deemed necessary for purposes of "ensuring aviation safety and protecting national
security." It is important to note that U.S. carriers are not required to comply with this
demand; only foreign carriers.

Passenger name records, or PNR, are not defined in detail within the Act. This information
can include vast amounts of information, however, including:

- Identification data: name, first name, date of birth, telephone number;
• Transactional data: the dates of reservations, the travel agent where appropriate, the information displayed on the ticket, the itinerary;

• Financial data: credit card number, expiry date, invoicing address etc.;

• Flight information: flight number, seat number, etc.;

• Earlier PNR: may include not only journeys completed in the past but also religious or ethnic information (choice of meal etc.), affiliation to any particular group, data relating to the place of residence or means of contacting an individual (e-mail address, details of a friend, place of work etc.), medical data (any medical assistance required, oxygen, problems relating to sight, hearing or mobility or any other problem which must be made known to ensure a satisfactory flight) and other data linked, for example, with frequent flyer programs.

The European Commission estimates that although there are approximately 25 possible fields of PNR data, some of these fields include subsets of information expanding the total to approximately 60 fields and sub-fields.\textsuperscript{10}

The U.S. Government does not state how each type of information will be used. In fact, specificity is generally avoided. The Congressional requirement for PNR has been interpreted very widely by the Bush Administration. According to an interim rule of June 2002:\textsuperscript{11}

• All carriers must not just provide U.S. Customs with PNR data, but actually give the government direct electronic access to the airlines’ computer systems. Each airline was responsible for ensuring that its automated reservation system and/or departure control system could interface with the U.S. Customs Data Center so that U.S. customs agents could log-in and look through files.

• This data must be provided for all flights, not only those destined for the U.S. So long as a carrier is 'engaged in foreign air transportation' to the U.S., U.S. Customs may access PNR information on the carrier's database. (U.S. Customs claimed that it would not require PNR for non-US travel, but contends that "as a business decision,
the airlines opted not to build filters within their reservation systems to preclude access to travel with no US nexus”.

- Once transferred, this data may be shared with other federal agencies for the purpose of protecting national security or as otherwise authorized by law.
- According to the regulations on the passenger profiling system, this data could be stored by the U.S. Government for up to 50 years.

Failing to comply with the U.S. law could be disastrous. The U.S. authorities proposed to conduct 'secondary inspections' of arriving passengers in the U.S., impose fines for airlines, and even the loss of landing rights.

One of the larger impediments to the U.S. proposal was the EU’s legal regime of data protection. All member states of the European Union have laws that protect data privacy. These data protection laws are required in order to comply with a positive obligation under Article 8 of the European Convention on Human Rights 1950. Article 8 requires the protection of the private life of the individual, and any intrusions must be in accordance with law and necessary in a democratic society. Jurisprudence from the European Court of Human Rights indicates that Governments have an obligation to protect the right to privacy, and as such Governments have chosen to implement data protection laws. Because of the variety of data protection laws amongst member states, the EU in 1995 established the 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 to establish a standard practice for privacy within the internal market.

Under the 1995 EU Data Protection Directive, EU member states must:

- restrict access to data collected or held within the territory
- limit the purposes for its use, as data may only be used for the purpose it is collected
- minimize the period of retention
• ensure that individuals have access to the data that is held on them
• ensure that individuals have legal recourse
• ensure that the data is protected adequately.

One of the Directive's primary goals was to ensure "not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."\(^{16}\)

This principle of free-flow between states with similar privacy laws provides the stumbling block to the transfer of this information from Europe to the American authorities. Article 25 of the EU Directive requires that if personal information is going to be sent to other jurisdictions that are not covered by EU laws, these other jurisdictions must have adequate privacy laws.\(^{17}\)

An adequacy assessment is required to establish an agreement with the U.S. to allow this transfer of data. According to the EU Directive,

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.\(^{18}\)

The conflict began when the European Commission Directorate General for the Internal Market, the directorate responsible for data protection at the time,\(^{19}\) realized that the United States does not come close to matching these requirements for "adequacy", and the U.S. Governments' demands were disproportionate. Federal privacy laws in the U.S. fall far short of these criteria, and in any case apply only to 'U.S. persons'. Also, as EU officials are aware, the PNR transfer is part of a much larger surveillance regime being established in the U.S. – a broader regulatory and technological framework that includes data mining and passenger profiling\(^{20}\), no-fly lists, and foreigner registration programs. There were also concerns that this information will be retained by the U.S. authorities for extensive periods,
in contravention with the EU requirements to delete personal information as soon as possible.

The European Commission Internal Market DG was also concerned that the PNR data will be used for an expansive set of purposes – not limited to national security but also for ‘other crimes’. Finally there were concerns that the PNR data may also be sold to private companies. The European Commission DG Internal Market felt that the U.S. legal regime would certainly not protect the personal data of EU citizens adequately, and as a result this information may not be transferred out of the EU to the U.S.

This view was confirmed by the privacy authorities in Europe. European Privacy Commissioners, the national regulators responsible for the enforcement of the data privacy laws, weighed in on the debate under the auspices of the European Commission’s ‘Article 29 Working Party’. This working party is responsible for certifying all transfers outside of the EU by deciding whether the protections are ‘adequate’ or not. Throughout the negotiations the Article 29 Working Party released a number of assessments of the proposed transfers. Repeatedly the Working Party argued that the transfer was incompatible with the EU Directive. In October 2002 the Working Party argued that “the need for the transfer is not proven and secondly it does not seem acceptable that a unilateral decision taken by a third country for reasons of its own public interest should lead to the routine and wholesale transfer of data protected under the directive.” The Working Party called for ‘a dialogue’ with the U.S. to resolve this impasse, provided that the U.S. could provide sufficient guarantees for the protection of the data.

This led to a tense set of negotiations between the two trading blocks, with a number of extended deadlines and changes in position. The European Commission DG Internal Market negotiated on behalf of the Europeans, and the U.S. Bureau of Customs and Border Protection and the U.S. Transportation Security Administration negotiated on behalf of the U.S. The Article 29 Working Party continually weighed in to assess interim agreements, or ‘undertakings’. In June 2003 they released another assessment of the transfers and again found them to be problematic. Apart from technical problems, the Working Party also
found that the transfers were disproportionate, granting the U.S. authorities greater access to data than currently granted to similar European judicial and policy authorities, that Europeans would lose their right of access to their own data for the purpose of rectification, and that the planned use of this data for profiling raised even greater concerns than previously considered. This last issue was particularly problematic because the uses of the data were not limited by the U.S. ‘undertaking’: the U.S. insisted that the data would be used to combat terrorism and other unspecified “serious criminal offences”. The Working Party was also concerned that access to the full set of PNR data was excessive, and thus not proportionate. This situation was exacerbated by the U.S. demands in the ‘undertaking’ to keep this data for 7-8 years.

Eventually the Americans further reduced the retention period to 3.5 years, minimized access to less than 40 data elements, and no longer required the ‘pull’ system of gaining access to each airline database but instead could demand carriers to submit, or ‘push’ the required information prior to travel. Also, the U.S. was compelled to reduce the purposes for which this information could be used. Previously the U.S. authorities proposed to use this information to combat crime as well as terrorism; after the negotiations the U.S. conceded that it would only use this information for combating terrorism and other serious crimes. In particular, the U.S. promised that the data would not be used for passenger profiling until a new and separate agreement was reached. The result of the negotiations is imperfect as there remain continued concerns as to how this information will be used, and whether sensitive information will be excluded, but the European Commission began to feel as though it had pushed for sufficient changes.

Regardless, pressure continued to emerge from the European Commission’s Article 29 Working Party. Following the updated ‘undertakings’ from the U.S. Government in January 2004, the Working Party released three more assessments of the agreement in 2004. The Working Party was satisfied with a number of the changes in the undertakings but was still concerned with the vague statement of purposes, arguing that in U.S. law ‘serious crimes’ was too broad. Also, though there was a reduced list of PNR items sought by the
Americans, the Working Party was concerned that the list still included "all of the 20 elements that the Working Party considered as disproportionate and problematic" in earlier assessments.\textsuperscript{26} The retention period was still too long for the Working Party: though it was reduced from 7-8 years to 3.5 years, the period was "considerably longer period than the 'weeks or months' called for by the Working Party" earlier.

The regulators were not alone in their opposition to the 'undertakings'. The European Parliament also continued to place pressure on the Commission, calling for significant changes to the agreement to protect privacy. A number of declarations were issued by Parliamentary Committees, a resolution rejecting the agreement, and the Parliament even threatened court action against the Commission on grounds of jurisdiction. Industry associations also weighed in, calling for less expensive solutions. The Association of British Travel Agents warned that it would cause lengthy check-in procedures.\textsuperscript{27} The Business Travel Coalition appealed to the U.S. Congress for "greater public policy debate regarding the tradeoffs, safeguards and remedies that such a comprehensive data collection program should require".\textsuperscript{28} The International Air Transport Association likened the situation to a 'tug of war': "The airline industry was always hopeful they would reach an agreement because we were faced with conflicting instructions."\textsuperscript{29} IATA went on to warn that data collection could cost tens of millions of dollars. And the public concern grew in response to news coverage of mass-transfers of data to law enforcement agencies.\textsuperscript{30} Some non-governmental organizations got involved, where some organized protests and co-ordinated complaints to national Data Protection authorities; some worked with Members of the European Parliament; and some briefed the media and wrote reports.

Despite this pressure from its own regulators, Parliament, and from within industry, and a growing amount of media coverage, the European Commission grew concerned that it could not continue its opposition to the U.S. plans. Apart from the threatened sanctions, it emerged that the European Commission’s DG Internal Market received countervailing instructions from other Directorates, including the Directorate on Transportation and the Directorate on Justice and Home Affairs. As the negotiations continued, it emerged that the
European Commission was also concerned with creating a policy similar to the U.S. policy on access to PNR. In fact, the Commission grew reluctant to refuse to the U.S. government access to the data on these very grounds. When negotiating with the U.S. to limit access to 'sensitive information' such as religious faith (as ascertained by the dietary choice, e.g. Halal or Kosher), the head of the DG Internal Market, Commissioner Bolkestein, informed the European Parliament that the EU must be careful what it refused to the U.S.

The EU cannot refuse to its ally in the fight against terrorism an arrangement that Member States would be free to make themselves.\(^{31}\)

Despite the initial 'worries' about the information that would be accessed by the U.S., however, the established agreement was considered adequate by the European Commission. Pressure arose from EU Member States, and from other sections of the European Commission. The final Communication from the Commission later stated that the agreement

with the US appears to be a sound basis for taking forward work on an EU approach (....). The list of data elements also seems broad enough to accommodate law enforcement needs in the EU. Nothing in the arrangements agreed with the US therefore seems to prejudice the development of an appropriate EU policy.\(^{32}\)

The Commission argued that it could not restrict U.S. access to information that would be collected for EU use. Put another way, the EU could not say that the U.S. had no right accessing sensitive data that the EU wished for itself for even more expansive purposes (see above). Put this way, the Commission was not only negotiating for the protection of privacy; it was also negotiating wiggle-room within an international agreement for the establishment of an EU-level policy on access to PNR.

The Commission also argued that a 'push' system would be ideal, where the required data would be sent to the U.S., and all sensitive data would be filtered by the carriers. In early December the Commission then stated:

The Commission is also working with the airlines on switching from pull to push as regards the means of transferring the data and on the necessary filters. The airlines are interested in a centralised or grouped approach, which seems also to the Commission to offer advantages in terms of cost and efficiency.\(^{33}\)
In mid-December, the Vice President of the Commission, who is responsible for Transport, Loyola DePalacio, agreed that a centralized approach would save money for airlines, but would also assist in "adopting a community policy in the field of data processing with a view to control immigration".\(^{34}\)

Carriers do have natural concerns with any such policy because of the costs of providing real-time terminal access to the U.S. Government. If the EU begins implementing similar policy across the member states, however, this will also increase the costs to carriers and the burdens upon reservations systems. On this point the carriers appear to be in agreement: a centralized solution would be cheaper because of the costs of abiding by the regulations. While some of the carriers may object to the practice altogether, they are not in a position to prevent access to this information by U.S. or European officials.

The Justice and Home Affairs Commissioner went a step further.

As a matter of fact, I can even see that a centralized structure inside European Union will be able to provide the necessary guarantees on the liability aspects, the accuracy of the data on the security of transmitted data, the technological means and the filters that Vice-President De Palacio has just mentioned to you, on the supervision by adequate control mechanisms, above all the role of the giant supervisory board and for offering added value to similar initiatives conducted at national levels within the European Union.\(^{35}\)

This led to the carefully worded final Communication from the Commission. The logic for a centralized system was clearly stated.

It was also made clear (...) that implementation of a push system could not solve the problem alone. Filters would also need to be installed. These filters entail significant costs for the airlines, which mean that a legal obligation would be desirable to ensure that all airlines are subject to the same requirements. Airlines have also indicated a preference for a centralised system.\(^{36}\)

The agreement with the U.S. was thus seen as a precursor to a European policy on access to PNR. When the Commissioner for the Internal Market announced to the European Parliament the new agreement with the U.S., he was accompanied by the Commissioners for Justice and Home Affairs, Transport, and External Relations. At this session, the then-Commissioner for Justice and Home Affairs, Antonio Vitorino, commented that the EU is
confronted with the need to complement that agreement with the United States of America by the development of a European Union policy on the use of PNR and of traveller’s data more generally within the European Union. \(^{37}\)

At this very same session, the Transport Commissioner argued for "adopting a community policy in the field of data processing with a view to control immigration". It was then announced that in 2004 a policy would be developed for "our own EU approach to the use of traveler’s data for border and aviation security and other law enforcement proposals."

The EU policy, however, would not be restricted to combating serious crimes and terrorism, but could be used for any law enforcement purpose, including immigration. The European Commission had thus transformed from an institution that wished to limit the purposes for the processing of PNR by government agencies, into an institution that wished to ‘complement’ the U.S. call for data for combating terrorism and serious related crime through using this information for border security, immigration, and other law enforcement purposes. While the transfers continue to be opposed by the European Parliament and European Data Protection Regulators, these institutions were rendered relatively powerless on the issue of travel surveillance once it became an internal policy.

3.2 Canadian Deliberations

As my travel is on a Canadian airline, the airline is also subject to U.S. requirements to transmit the information to the Department of Homeland Security. The reservation information is thus being transferred by a Canadian company to the U.S., giving rise to similar legal problems as those that arose in the EU. An additional complication is that Canada is also a recipient of this information. Since 2001 Canada has been working on establishing a policy on access to PNR by Canadian authorities. This section will therefore cover the domestic debate on access to travel data.

The domestic policy landscape in Canada differs in significant ways from the previous case. In Canada the policy was not shaped so much by demands from the U.S. Rather, a domestic policy process began because of demands from Canadian Government agencies. Fewer non-governmental organizations participated in this process, mostly because Canada
does not have an active civil society on civil liberties and human rights issues to the same extent as in the U.S. or Europe. Also, the Canadian airline industry is much more simplified with far fewer carriers. Like in Europe, Canada has a comprehensive data protection regime, and as such, the Privacy Commissioner played a significant role in the policy process. In Canada, the legislature played a larger role because of the lack of public attention to the issue, with most of the debate arising in the Upper House, or the Senate.

In its policy deliberations, the Canadian Government encountered some original resistance to its own use of PNR, particularly on the scope of purposes for its use. Bill C-17, was introduced in October 2002 to replace another bill, C-55, that had died the previous month. C-55 was introduced to replace another bill, C-42 that was introduced in November 2001 and had received significant criticism, forcing the Government to abandon this early bill.38

Bill C-17 was to amend twenty-three other pieces of legislation. The key component of the bill was the treatment of passenger travel information, including the information regarding domestic travel. The bill proposed to grant real-time access to law enforcement and national security agencies to analyze the lists and information on travelers, and to hold this data for a period of time. The bill empowers the Minister to require certain passenger information from air carriers and operators of aviation reservation systems, for the purposes of transportation security. This information must be destroyed within seven days, notwithstanding any other Act of Parliament. The Commissioner of the Royal Canadian Mounted Police (RCMP), the Director of the Canadian Security Intelligence Services (CSIS) may require certain passenger information to be used and disclosed for the following purposes: transportation security, national security investigations relating to terrorism, situations of immediate threat to the life or safety of a person, the enforcement of arrest warrants for offences punishable by five years or more of imprisonment, and arrest warrants under immigration law and extradition treaties. This information may be combined with other information held by the RCMP, but only for the purpose of transportation security only (and not for outstanding warrants, as the Bill’s predecessor contained). CSIS could receive and analyze this information for the purpose of transportation security, or national
security investigations relating to terrorism. Finally, the bill also permitted the transfer of this information to other countries, on the condition that the flight is landing in that country.

The then-Privacy Commissioner of Canada protested continuously against these measures, particularly in the Parliamentary committee process. In particular, the Commissioner argued that "the police have no business using this extraordinary access to personal information to search for people wanted on warrants for any offences unrelated to terrorism." That is, the power to stop individuals who are wanted on warrants already exists in law. According to the Commissioner,

If the police become aware, without this provision, without anything, that there is an individual wanted on a warrant, they don't need this provision. They have a common law and a legislative right and duty as peace officers to take the appropriate measures to apprehend the individual, period. So there's no issue of that. If you drop this provision tomorrow, and that's what the government is trying to obscure, it will not create a circumstance where if the RCMP [Royal Canadian Mounted Police] becomes aware there is murderer on a plane, they can't arrest him. Where there could be a problem is if it were not incidental, if in fact a practice were made of looking in CPIC [the database that is a 'grab-bag of all information known to all police forces'] and checking everyone to see if they were wanted for something when the police had no business looking in CPIC because they should have been looking in the anti-terrorism database, SCIS [Secure criminal investigation system, a more specialized database], for example. If it's systematic, then they could be encountering issues where they are using legislation meant to protect aviation security for purposes of looking for people wanted on warrants totally unrelated.

In a later testimony, the Commissioner further articulated his concerns about expanding the purposes for using this information beyond terrorism.

As we go about our normal law-abiding business in Canada, unless we're carrying out a licensed activity, such as driving, we don't have to identify ourselves to the authorities, but if the police can check passenger lists to see who's wanted for an offence unrelated to terrorism on an airplane, why not when we take a train or a bus or rent a car or check into a hotel? Why, once the principle is accepted, should the police not be able to pull cars over and check the identity of all the passengers and look in the database to see if they're wanted for anything? It opens a door that should not and need not be opened and has nothing to do with the stated purposes of anti-terrorism. Bill C-17 eventually failed, in part due to parliamentary scheduling.
In February 2004, the Minister of Transport introduced Bill C-7, again entitled 'the Public Safety Bill'. According to its legislative summary, the provision of information must be for the purposes of transportation security and may pertain to the persons on board or expected to be on board a specific flight in respect of which there is an immediate threat, or to any particular person specified by the Minister. Transportation security is broadly defined.\textsuperscript{42}

In this bill, the purposes for access and processing of this information had changed mildly since C-17. They are now defined as:

- for transportation security purposes;
- national security investigations relating to terrorism;
- situations of immediate threat to the life or safety of a person;
- the enforcement of arrest warrants for offences punishable by five years or more of imprisonment and that are specified in the regulations;
- and arrest warrants under the Immigration and Refugee Protection Act and the Extradition Act.\textsuperscript{43}

Disclosure is recorded with care. A record must be kept of all disclosures, the information disclosed, the reasons, and the name of the person or body to whom the information was disclosed. Information must be deleted within seven days of its receipt, unless required for security purposes.

However sensible the above provisions sound within the vacuum of legislative language, the law enforcement authorities had stated clearly their intentions to interpret these provisions widely. According to a report from the Parliamentary Research Branch,

> When witnesses from the RCMP and CSIS appeared subsequently before the Committee, they stated that the intent of the provision was to enable them to receive a continuous electronic data feed from the airlines regarding all passengers for all flights where it was technologically possible to do so. Further, they stated that they interpreted the wording of the provisions to permit that and, in addition, felt that their interpretation was the only way the system could actually work and meet their needs.\textsuperscript{44}

Officials later admitted that this was the intention when they drafted the bill, and no amendments to this were made.
The bill was to amend existing privacy law. Existing immigration law permits government to make regulations to gain access to reservation systems and reservation information, upon request. This information can only be used for immigration purposes or to identify a person for whom a Canadian arrest warrant exists. In each case, however, the individuals must be given notice of the use of the information. C-7 enables additional collection, use, retention, and disclosure of this information. This required amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) to permit the collection and use of personal information by air carriers and other organizations without the knowledge or consent of the individual, for the purpose of making a disclosure for reasons of national security, the defense of Canada or the conduct of international affairs, or a disclosure required by law.

The Canadian Bar Association noted that this fourth version of the proposed Public Safety Act "moves a bit further along the path to a more tailored response" but that "tinkering at each stage has not assuaged our overall concerns." The CBA questioned how the interpretations of "terrorism" or "serious threat" could shift with the political climate, that the cross-referencing of passenger information for extended law enforcement purposes threatens privacy, and that the sharing of passenger information with foreign states is an unnecessary intrusion on privacy rights. In conclusion the CBA states that

The CBA is concerned about the insidious invasions of privacy and fundamental rights creeping into Canadian law over the past few years. Bill C-7 is but one such measure. Canadians are now beginning to see the negative impact on individual liberties of the various government measures intended to combat terrorism. A full and rigorous review of all security-focused legislation is needed, to assess its cumulative effect on privacy, individual rights and freedoms, and checks and balances on state powers.

The CBA ended its intervention by urging the Senate to not pass C-7.

In the time between Bill C-17 and the introduction of C-7, a new Privacy Commissioner was appointed. The new Commissioner had some substantially evolved, yet similar concerns to her predecessor. Regarding the amendments to PIPEDA, she stated that
The proposed amendment to PIPEDA, in effect, allows organizations to act as agents of the state by collecting personal information, without consent for the sole purpose of disclosing this information to government and law enforcement agencies. Under the existing provisions of PIPEDA, this information is collected with the knowledge and consent of the individual. This is fair. The proposed amendment that would allow collection without consent is not.46

As to the concerns regarding the sharing of passenger information with the RCMP and CSIS, she held similar concerns to her predecessor regarding function and scope creep.

These provisions dangerously blur the line between the private sector and the state by enlisting businesses, not only in the fight against terrorism, but in identifying individuals against whom there may be outstanding warrants for a wide variety of offences. This legislation establishes a new and troubling precedent. What's next? Are we going to start requiring car rental firms, couriers and telecommunication companies to collect information for the purpose of turning it over to law enforcement agencies?

She worried that the law was unnecessarily broad and as a precedent it would permit further data collection and transfer, transforming our norms and practices generally. The Commissioner went on to say that if the bill dealt only with anti-terrorism and transportation security, this would minimize her concerns. But as it is, it proposes to monitor even domestic flights for matches with a list of outstanding warrants that have no connection to national security. As the Commissioner notes, despite all the renditions of this bill, "[w]e have yet to hear any compelling reason why the warrant provisions are needed and how we will be safer as a result of these provisions."

Many other organizations advised the Parliament on the problems with the bill, including the Canadian Association for University Teachers, the Coalition of Muslim Organizations, and the International Civil Liberties Monitoring Group. The media attention, while significant, was not as remarkable as in other countries. Regardless, the bill was given Royal Assent in May 2004.

4 Transformation of Border Controls

When we arrived at the U.S. Customs and Immigration checkpoint in our travels, I was fortunate enough to be at the desk when my companion was subjected to fingerprinting and a photographing. For the first time in her life her fingerprints were taken. The Border
security official was most kind as he admitted that he had previously encountered some resistance to this measure. He told us a story of a prior visitor who spoke of how the last time she was fingerprinted it was in Germany in the late 1930s. When my companion asked why she needed to be fingerprinted, he responded that this all began in September 2004. In fact, it did not, but I don’t believe he was misleading us.

Since September 30 2004, all visitors to the United States are face-scanned and fingerprinted at the border. These measures are part of a vast integrated information storage, matching and profiling system. The legislative grounds for this do reside somewhat in the USA-PATRIOT Act, but also in other legislation. In 1996 Congress called on the Attorney General to develop an automated entry and exit monitoring system for foreigners. This was expanded significantly by the USA-PATRIOT Act in 2001, which suggested the use of biometrics. The Enhanced Border Security and Visa Entry Reform Act of 2002 took the USA-PATRIOT Act even further and called for the integration of the border monitoring system with other databases.

The U.S. Visitor & Immigration Status Indication Technology System (US-VISIT) collects and retains biographic, travel, and biometric information on all visitors, except Canadians and Mexicans. The purpose of this collection is to identify people who are believed to potentially pose a threat to the security of the U.S., are known or believed to have violated the terms of their admission to the U.S., or who are wanted in connection with a criminal act in the U.S. or elsewhere. This information will be shared with "other law enforcement agencies at the federal, state, local, foreign, or tribal level" who "need access to the information in order to carry out their law enforcement duties."47

Personal information collected by US-VISIT will be retained for 75 to 100 years. In a meeting with Department of Homeland Security officials when the program first began, they stated that this retention period was necessary for immigration purposes as there may be legitimate long term needs to verify citizenship status; but as for VISIT specifically, they said that time limits may be shorter but the policy had not yet been decided.48 One month earlier, however, the Department of Homeland Security filed notices in the Federal Register
stating that arrival and departure data would be kept for 100 years\textsuperscript{49} while biometric and biographic data would be kept for 75 years\textsuperscript{50} Tourist information is to be kept alongside data collected from nationals of countries that threaten to wage war, or are or were at war with the United States\textsuperscript{51}

This system is to be used for a plethora of purposes. These include national security, law enforcement, immigration control, and "other mission-related functions and to provide associated management reporting, planning and analysis." It will assist in:

identifying, investigating, apprehending, and/or removing aliens unlawfully entering or present in the United States; preventing the entry of inadmissible aliens into the United States; facilitating the legal entry of individuals into the United States; recording the departure of individuals leaving the United States; maintaining immigration control; preventing aliens from obtaining benefits to which they are not entitled; analyzing information gathered for the purpose of this and other DHS programs; or identifying, investigating, apprehending and prosecuting, or imposing sanctions, fines or civil penalties against individuals or entities who are in violation of the Immigration and Nationality Act (INA), or other governing orders, treaties or regulations and assisting other Federal agencies to protect national security and carry out other Federal missions\textsuperscript{52}

This information will then be shared with other government departments and used in other programs of surveillance. This includes:

- "to the appropriate agency/organization/task force, regardless of whether it is Federal, State, local, foreign, or tribal, charged with the enforcement (e.g., investigation and prosecution) of a law (criminal or civil), regulation, or treaty, of any record contained in this system of records which indicates either on its face, or in conjunction with other information, a violation or potential violation of that law, regulation, or treaty,"

- "to other Federal, State, tribal, and local government law enforcement and regulatory agencies and foreign governments, and individuals and organizations"

- during the course of an investigation or the processing of a matter, or during a proceeding within the purview of the immigration and nationality laws, to elicit information required by DHS to carry out its functions and statutory mandates
• "in response to its request, in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of such an employee, the letting a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency’s decision in the matter."

• "to assist such agencies in collecting the repayment or recovery of loans, benefits, grants, fines, bonds, civil penalties, judgments or other debts owed to them or to the United States Government, and/or to obtain information that may assist DHS in collecting debts owed to the United States government."

amongst many other recipients.⁵³

The U.S. Government has already made Visa information available to law enforcement officials across the country, including photographs of 20 million visa applicants. This 'sensitive' information will be shared with 100,000 investigators across the country who will have access to seven terabytes of data on foreigners.⁵⁴

Some may argued that the increased surveillance at borders poses significant challenges to civil liberties, to race relations and to the functioning of a free and open society. What is most alarming about the technologies and policies is how little discussion there has been. The little attention that these policies have received was either generated by groups and commentators objecting to the discriminatory aspects of the policies, or the Government Accountability Office (GAO)⁵⁵ calling for additional scrutiny. The concerns of the former group appear to have been heeded, while much more attention is needed to meet the concerns for the latter.

### 4.1 Efforts to Ensure Accountability and Privacy

Some systems garner public attention, others don’t. US-VISIT never really captured the public’s attention in the way that others have. We have already seen the political failure of the Computer Assisted Passenger Pre-Screening System (CAPPSS II) due to privacy and
technological challenges. Similarly, the Total Information Awareness program lost its funding when audits and legal assessments found that the money is best spent elsewhere because of fears regarding Governmental abuse of power.\textsuperscript{56} Both these systems received great public scrutiny, however, and in turn to significant Congressional scrutiny, and in turn to audits and further deliberation.

Another parallel system is the Student and Exchange Visa Information Service (SEVIS), which compels schools across the country to submit information on foreign students (of which there are over 500,000). Like US-VISIT, this system is also based on a law from 1996 but was later amended by the USA PATRIOT Act. The purpose of SEVIS was to keep track of addresses of students, their enrolment status, whether they have a reduced course load, and monitoring 'optional practical training';\textsuperscript{57} on an Internet-based system.\textsuperscript{58} Despite assurances that SEVIS was not complex, expensive or burdensome and that it would provide accurate, unambiguous and current information, the opposite has resulted. In one situation, 1450 student files were stolen by malicious hackers from the University of Kansas.\textsuperscript{59} The Immigration and Naturalization Service (INS) also had to extend the deadline for implementing the system due to complaints from schools that the system was too cumbersome and was neither responding properly,\textsuperscript{60} nor designed adequately.\textsuperscript{61} There have been additional complaints regarding data integrity and data security.\textsuperscript{62} Others have complained of unfair processes and students being wrongly thrown out of the country.\textsuperscript{63}

Similarly, the visa regime in the U.S. has transformed in recent years with the inclusion of biometrics and tighter interview requirements, and this has given rise to concern as well. According to one report\textsuperscript{64} these new visa processes, are said to be causing delays in granting visas, and have cost U.S. firms at least 30 billion dollars since July 2002. According to some critics these burdens to entering borders are hurting the economy.\textsuperscript{65}

What is remarkable is that CAPPS II, TIA, SEVIS and the new visa regime generated quite a public discourse, while US-VISIT has not, in the U.S. at least. Universities have been vocal in their objections to SEVIS because of the regulatory implications; industry and academic organizations have been vocal on visa costs and hurdles. Civil liberties organizations and
the media were vocal on CAPPS II and TIA. US-VISIT has not elicited the same reaction, discourse, and deliberation. Rather, much of the oversight has been provided by the U.S. Government as a matter of course. The Government Accountability Office has overseen many of these government projects to assess its costs, complexity, and progress. Its reports are often critical to the success or failure of a program, as the reports inform and shape congressional outcomes.

The GAO assessed US-VISIT in March 2004 and declared that it is "inherently risky because it is to perform a critical, multifaceted mission, its scope is large and complex, it must meet a demanding implementation schedule, and its potential cost is enormous."66 Pointing to other data collection and mining initiatives, the GAO warned that the project is 'increasingly risky'.

The project is also quite costly, particularly as it grows larger and more complex. The U.S. Government has commissioned a $15 billion contract to fully develop US-VISIT into a system that creates detailed dossiers on all visitors to the U.S. (even though DHS had originally budgeted $7.2 billion)67. The project began with the collection of two fingerprints, and already it has been expanded to collect all ten fingerprints.68 The system is likely to include additional biometrics in the future; according to the contract winner, Accenture: "Part of our approach is to continually assess technology innovations. For a 10-year contract that's a generation or two of technology, and biometrics is a very hot area."69

The Department of Homeland Security (DHS) has always contended that VISIT actually protects the privacy of foreigners, accordance with its privacy policy, in its privacy impact assessment. When VISIT first began, there were no rights of redress for individuals who faced any sort of adverse consequences, however.70 Following a review by the GAO (and some outcry by legal and civil rights advocates) there is now a limited appeal process, including a human review of the fingerprint matching process, and provision for some correction of faulty information.
A further assessment by the GAO occurred in February 2005. The GAO found that a security risk assessment has not yet taken place, and that the privacy impact assessment was lacking. The problems arose particularly because US-VISIT is made up of various pre-existing systems, operated differently by different DHS organizational components. The GAO found conflicting protections under the Privacy Act for information that came from differing sources, arising from the fact that VISIT is an amalgamation of a number of different data sources. The GAO found that while access to travel information was limited to authorized users, the data stores for fingerprints and face-scans "do not consider privacy at all". This was considered to be symptomatic of the general problems with US-VISIT, including rising costs and the lack of reliable cost estimates, management problems, and capacity issues. The GAO even concluded that the DHS should reassess plans for deploying an exit-capability.

Similarly, the normal scrutiny of technological decisions that applies in many of the above-mentioned countries when a domestic project is implemented has yet to arise. The inevitable problem facing large biometric systems is that biometric prints are often unstable and fallible. Some people cannot for physiological reasons be enrolled in a biometrics system. The physical characteristics and circumstances of numerous people means the biometric will change over time. This means there must be a margin of error in biometric registration and verification. And as the system grows in size, so must the margin. There are three distinct problems that can result from deployment of a large biometric system. The first is described as the Failure To Enrol Rate (FTER). This occurs when a person’s biometric is either unrecognizable, or when it is not of a sufficiently high standard for the machine to make a judgment. The second crucial indicator is the False Non-Match Rate (FNMR) that occurs when a subsequent reading does not properly match the properly enrolled biometric relating to that individual. The third problem is where there are so many biometric identities in a system – or where the margins are set so tightly – that people are falsely identified as someone else. This is known as a False Match.
Another GAO report makes the point that the FNMR for fingerprinting can be extremely high – up to 36 percent. With 300 million visitors to the U.S. every year, the potential for mass error increases. Yet there has been little attention to these issues.

### 4.2 Efforts to Reduce Discrimination

A great deal of attention has been raised regarding any chance of the U.S. Government devising a policy that may be construed as discriminatory. VISIT was developed after previous programs were abandoned, for the most part due to claims of discrimination. After September 11 the U.S. began a number of programs that involved the 'registration' of Muslim and Arab immigrants, and others deemed to be of interest. After the terrorist attacks, the Immigration Services identified 7602 individuals who shared similar 'characteristics' to the 19 hijackers, and aimed to interview them. These interviews were said to be 'voluntary', though few believed this to be true. Law enforcement officials interviewed 3,000 Muslim and Arab immigrants in the U.S. Even at this time, however, the government list of individuals it intended to question contained many duplicate names and data entry errors. The practice was considered to have an adverse effect on relationships with these communities, and generated some negative media coverage; yet the response of the U.S. Government was to emphasize the usefulness of this project.

Next came the 'Special Registration Procedures for Certain Non-immigrants'. This involved the forced registration, interviewing and fingerprinting of individuals. The program originally focused on nationals of Iran, Iraq, Libya, Sudan and Syria, but also "any other non-immigrant identified by INS officers at airports, seaports and land ports of entry", based on criteria designated by the Secretary of Homeland Security. The program was later extended to include individuals from Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates and Yemen.
Of the 82,000 men who were registered, more than 13,000 were found to be living in the U.S. illegally, and were to be deported.\textsuperscript{78} The program was later shut down in November 2003, one month before US-VISIT went live.\textsuperscript{79}

Another system was the National Security Entry-Exit Registration System, targeting individuals specifically at the border. Ironically, registration was justified on the grounds that the European authorities have registered visitors for some years. According to a statement from the then-Attorney General John Ashcroft,

\begin{quote}
Our European allies have had similar registration systems in place for decades and know the value of ensuring that foreign visitors are doing what they said they would do and living where they said they would live. The NSEERS system takes the European model and combines it with a modern intranet system so that files may be updated in real time at any INS office in the country.\textsuperscript{80}
\end{quote}

Under NSEERS, these individuals would be 'fingerprinted and processed'. Unlike the other systems and policies, it was not limited to 'terrorist nations', however. According to the Attorney General,

\begin{quote}
So far, [Immigration and Naturalization Services] has fingerprinted and registered individuals from 112 different countries. From the Baltic to the Balkans and from the Cape of Good Hope to the Rock of Gibraltar, visitors who may present elevated national security concerns will be included. No country is exempt. In the war against terrorism, we cannot afford to have tunnel vision.\textsuperscript{81}
\end{quote}

The general response to this practice was negative. After considerable pressure from foreign governments\textsuperscript{82} and civil liberties advocates, the program was claimed to be shut down.

In April 2003 NSEERS was renamed as the US-VISIT program. Although the US-VISIT program would end the domestic special registration, it would register all visa-holders to the U.S., though was later extended to all visitors to the U.S. This would circumvent prior concerns from civil liberties advocates and lawyers that the earlier programs were discriminatory. In turn, there has been a relative silence in the public discourse regarding VISIT, with a small number of articles and debates. So long as it does not discriminate, much of the controversy dies. Even the New York Times claims that "[t]he government has wisely decided that [all visitors to the U.S.] will be included in [VISIT], which checks
photographs and fingerprints against watch lists... it is hardly an onerous burden\. This was considered to be a reasonable, non-discriminatory step forward.

### 4.3 The Spread of VISIT

The VISIT methodology is now going international, which is in a sense the next logical step forward. Brazil retaliated against US-VISIT by fingerprinting U.S. visitors to Brazil, which led to a complaint from Secretary of State Colin Powell because it was felt that Brazil was discriminating against U.S. citizens.\(^{84}\) Greek, Swiss, and Chinese officials, amongst many others have complained about the forced registration of their nationals, whilst other governments have been conspicuously silent.

The U.S. has been calling for international co-operation on this scheme. According to then-Secretary of Homeland Security Tom Ridge,

> I think it's critical that we move this along as quickly as possible, and the best way of facilitating that is not simply on a bilateral-by-bilateral basis, but to get as much multilateral buy-in as soon and as quickly as possible.\(^{85}\)

When warned of retaliatory measures by other countries against US-VISIT by fingerprinting Americans, the then-Department of Homeland Security undersecretary, Asa Hutchinson, declared that:

> We welcome other countries moving to this kind of system. We fully expect that other countries will adopt similar procedures.\(^{86}\)

Another U.S. official declared that the U.S. has no problems if similar requirements are imposed elsewhere.

> We are in favour of these border measures generally. If there was such a requirement we would inform our citizens and it would be up to the traveller to decide.\(^{87}\)

Indeed, these systems are traveling elsewhere.

Canada is moving towards fingerprinting and face scanning, as part of its 'Smartborders' program.\(^{88}\) Japan has set up a working group to look into possible biometric solutions,\(^{89}\) and Russia is planning a CIS-VISIT system.\(^{90}\) Britain is planning a similar system under
Project Semaphore in order to deal with asylum seekers, possibly using iris scanning. The UK recently announced its ‘E-borders programme’ that will collect fingerprints and iris scans and PNR on all visitors and residents, for the purpose of combating terrorism and to support general policing, and to enable a profiling system that would identify suspect passengers or patterns of travel behaviour.

All these systems are likely to go beyond the US-VISIT program by collecting the fingerprints and travel habits of all, not just non-citizens. No legal analysis has been done on this though, partly because US-VISIT has applied only to foreigners. When outgoing Secretary of Homeland Security, Tom Ridge called for fingerprints to be included in U.S. passports, it sounded as though the Federal Government was considering including citizens in biometric border checks. When the EU begins fingerprinting all nationals of its member states to provide biometric border checks and passports, as it intends to do within the next two years, perhaps questions may then arise. It is entirely possible, however, that it may be too late to ask such questions, or we may not even fathom to ask them because we have grown so accustomed to the system in the U.S.

5 Transforming Checkpoints: The Dynamics of Discourse and Deliberation

I arrived safely to the U.S., and have since traveled back. No terrorist attack occurred, and delays arose only due to weather, which is the way it should always be. It is entirely possible that my trip was enabled by the protection offered by Governments who now have access to sufficient information regarding those who fly and those who pass borders. No respectable academic could deny such a conclusion; but equally, no respectable academic would accept that as a fait accompli, the end of the debate.

In fact, this should only be the beginning. Just because a system may appear to work does not make the system acceptable. In one of the audits that killed off the controversial Total Awareness Program in the U.S. that would apply to U.S. citizens, the Inspector General of the Department of Defense concluded that:
A review of the TIA program (...) showed that although the TIA technology could prove valuable in combating terrorism, DARPA [Defense Advanced Research Project Agency] could have better addressed the sensitivity of the technology to minimize the possibility of any Governmental abuse of power and could have assisted in the successful transition of the technology into the operational environment. As a result, DoD risks spending funds to develop systems that may be neither deployable nor used to their fullest potential without costly revisions and retrofits.\textsuperscript{94}

Of course that audit was not what stopped the program. Rather it was the heated public discourse, and the added deliberation by the legislative arm of the U.S. Government. Similarly, the controversial CAPPS II system had received more than $40 million, but faced significant public concern and eventually the Department of Homeland Security killed it off.\textsuperscript{95}

In an Open Society, we question policy, even after it is created, funded, and deployed. We regret the rush to legislate after September 11 2001 because we worry that we did not fully consider the policies. This article has pointed to other policies that we also did not fully consider, and this is not merely the fault of legislators and officials. In the policies outlined above, they are not the result of rushed processes. Rather, an inattentive society has allowed these policies to pass without adequate discourse and deliberation. Few questioned US-VISIT when it was no longer discriminatory; Canadian civil liberties groups are few and far between and did not engage much and relied on the efforts of the privacy regulator; and in Europe the regulators and parliamentarians played what role they could in a policy that was shaped equally by international affairs and self-interest.

\textbf{5.1 The Dynamics of Discourse and Deliberation}

What began with a war on terrorism has now transferred to a new security agenda. What began with increasing powers for Government agencies to combat terrorism has resulted in the increasing of Government powers generally.

In this new environment, all forms of criminality are now investigated with powers originally foreseen to combat terror. This is not necessarily Government merely over-reaching. There may be legitimate reasons for including ‘serious crimes’ as a purpose to process PNR or fingerprints from US-VISIT, since terrorists may also be involved in serious
crimes. Similarly, the general populace has grown even more concerned with illegal immigration in recent years, and so policies like access to PNR or biometric border controls may be seen as legitimate policies to deal with these troubles, which is exactly what we are seeing in the United Kingdom. In this new environment, it is often claimed that we must balance civil liberties with other concerns within society, particularly when some of these concerns may involve the destruction of society.

Such reasoning may be convenient, but it is lacking in rigor and detail. This article does not try to contest the policies. Rather, it calls for adequate discussion of these policies so that contestation may follow. In what little discourse and deliberation that did arise, we may find strains of interesting debate. The European Commission and Privacy Commissioners debated with the U.S. on the usefulness of PNR and the importance of privacy protection. The Canadian Privacy Commissioners and the Canadian Bar Association devised interesting arguments against the collection and processing of passenger information. The Government Accountability Office raised essential questions regarding the usefulness of the technologies in US-VISIT and the costs and efficiency of the process. These acts are qualities of the Open Society.

When we analyze these interventions, we can see within the dynamics of policy formation some essential ingredients for discourse and deliberation. The dynamics identified in this article are international, regulatory, technological, and legal in nature. There may indeed be more.

**International Dynamics.** Understanding access to passenger information is enhanced when we look at the conflict between the U.S. and the European Commission. These negotiations raised valid points about the conflict of jurisdictions, and the differences in legal protections; which may be used to inform future discourse in the U.S. if/and when U.S. carriers are compelled to provide information to the Department of Homeland Security. For border controls, it is important to note the response from other countries to the U.S. policies. The U.S. Government has even promoted this policy in other countries, and with the likely rise of CIS-VISIT, Canada-VISIT, Japan-VISIT, and UK-VISIT we may
inform policy-makers of likely challenges if we understand well the controversies that arose in the US-VISIT program.

**Regulatory Dynamics.** The policies discussed in this paper are not limited to Government-and-citizen interaction. Non-state actors such as industry (associations, carriers, tourism) have roles to play in each, and this gives rise to further issues such as costs and regulatory burdens. Airlines were concerned with the costs of providing 'pull', i.e. terminal access to governments, which in turn led the European Commission to promote a 'push' system where carriers could merely send the required information to authorities. This had the negative effect of promoting the idea of a centralized EU institution that would receive all this information before sending onwards to the U.S. in order to reduce costs for industry, while also benefiting EU Member States since they could also gain access to this information. The Canadian Privacy Commissioners asked why it was so important to verify domestic air travel, as they feared that if we started with the airline industry then it will surely spread to other sectors. In the case of US-VISIT, scrutiny by the GAO has shown that significant challenges have arisen in the deployment of the system, in particular with managing the contracts and the extraordinary cost of the contract which has already doubled in size. In these cases, a public discourse that included non-state actors could possibly inform deliberation to minimize these problems, though not necessarily.

**Legal Dynamics.** Within each of these policies, legal requirements became modalities of contention. The conflict in laws between the EU member states and the U.S. led to an informative discourse and debate regarding the treatment of data. The contributions from a variety of non-state actors, or non-governmental organizations provided insight into the legality and constitutionality of these proposed practices. At the same time, the lack of consideration of the legal implications of these policies is also quite telling: due to the trans-national nature of these policies, those who are affected are not included within the process of deliberation. The access to PNR by the U.S. Government and US-VISIT do not implicate U.S. citizens and as such did not generate much discussion in the U.S. Similarly, the European Commission was compelled to act because U.S. law affected EU law; and
even still, when it did act, the European Commission acted not only to protect privacy interests but also managed to serve and protect the national interests of its member states. In Canada where access to PNR did involve data on Canadian citizens, the discourse and debate was richer, and this did affect deliberation as it delayed the passing of the Public Safety Bill, though did not prevent it.

**Technological Dynamics.** By looking at the technological components of the policies discussed above we become more informed. When we finally look at the constitution of PNR we come to understand why it may be controversial (particularly when we realize that some of this data may include political, financial, and religious information). The differences in ‘push’ and ‘pull’ systems result in different costs structures and even policies, and this requires further attention. Similarly, the GAO raised valid questions regarding the technological effectiveness of the biometrics selected for the US-VISIT system, and the arising risks and costs of the system due to technological constraints. The increase from a two-finger to a ten-finger system deserves further attention as well. Understanding the role technologies play in sustaining, preventing, or changing political strategies may significantly inform future deliberation.

These dynamics intermingle with one another, providing interesting questions and challenges that, if raised, may heighten policy discourse and deliberation. It will not necessarily lead to better laws, but at least the process is something that we have all consented to, as it is the process of an open system of governance.

**6 The Fate of the Open Society**

When successive Privacy Commissioners in Canada questioned the collection and processing of passenger information, they were not questioning the use of this information for combating terrorism. Rather they questioned why it needed to be used for situations apart from terrorism. All proponents of privacy and civil liberties realize that when it comes to combating terrorism the scales have tipped in the direction of national security. These proponents do not accept that this has to be the case for everything. So the Privacy
Commissioners asked why did this have to amount to such a change in the way that Canadian society conducted itself: would this lead to road-checkpoints looking at the manifests of cars, checkpoints at bus stations and ferry ports? If we accept these checkpoints at airports and borders, the Commissioners asked rhetorically, and then are we willing to accept them everywhere else?

The Commissioners were merely pointing out that people would probably be concerned if the Government proposed road checkpoints, so if they were properly informed, they would also oppose checkpoints at airports for non-terrorism purposes. But there is a dangerous inverse to this equation, however, that worries me even more so. If we have accepted checkpoints at airports, won't we be more willing to accept checkpoints on roads? Similarly for the US-VISIT program: because we have accepted fingerprinting as the obligatory passage point for getting to our holidays in Florida or for that weekend in New York, won't we be more willing to submit to fingerprinting to get access to ferries and buses, or schools and libraries?

A society protects rights and liberties because it deems these rights and liberties important to protect. Certainly there are laws that protect privacy, but these laws, even constitutional rights, require public support. The European Commission transformed European privacy law that prevented the transfer of information to other countries without adequate protections, allowing the transfer to the U.S. while few were looking, while also granting access to themselves. Information on the travel habits of all Canadians is now accessed by law enforcement agencies, though few Canadians are aware of this practice and its ramifications. All visitors to the U.S. are fingerprinted, and if they refuse, they are returned home. All these practices in one way or the other corrodes our conceptualizations of rights and liberty.

Societies may passively choose to no longer protect rights. In American jurisprudence, the right to privacy relies on society deeming it reasonable that someone has that right in the circumstances in which she claims to expect it. If fingerprinting starts occurring at every border, society may be less willing to consider it unconstitutional when we fingerprint
people arbitrarily on streets. If people lose their expectations of privacy and stop valuing rights, then a lot of the essential questions that need to be raised will not even occur to many. Similarly, under the European Convention on Human Rights, invasions into our private lives may occur so long as they are proportionate and necessary in a democratic society. What is ‘proportionate’ may vary with time, and what we deem ‘necessary’ to combat terrorism has apparently also leaked over into the new security agenda.

At this point I am going to offer the most controversial point in this article. I would argue that maybe we must see discourse and deliberation as a good in itself. Perhaps the various actors need to have their varying interests and contentions voiced. This is after all the point of the open society. Governments can not by some magical nature have perfect information and thus can not be immediately trusted to develop the ‘best’ policies. Others may be able to judge these policies, and to make them better through presenting other information and considerations. Industry representatives certainly informed the debate on the value of PNR, just as privacy commissioners and experts provided information on the privacy issues at stake, and the GAO’s studies informed us on the risks of large-scale border systems. These are essential parts of the policy process not only because it can result in better policy, but also it enlivens and enriches the public debate. This is how we fuel the marketplace of ideas from which we develop our laws and policies.

This view of some inherent value of discourse and deliberation may even extend to those on the fringe of the debates, to those with the more extreme views. The New York Times was busy sounding ‘reasonable’ when the fingerprinting of visitors began, and many were worried about sounding unreasonable regarding travel data when this could be used to prevent future terrorist attacks. Only the more radical would be willing to stand up and not be reasonable and argue that it is unacceptable to collect vast amounts of information on people without a stated purpose that is legitimate, proportionate, and necessary. An interesting research paper can be shown how individuals who were unreasonable and ‘on the fringe’ were responsible for the eventual establishment of many of our political rights.
They may also be the individuals who can defend them within political discourse and deliberation.

Admittedly, even when there is an open political debate on a policy the outcome is not always ‘ideal’. This is often the case particularly when we speak of protecting rights, where polls show support for incursions upon fundamental rights such as free expression. At this point we are entering the domain of political theory with controversies regarding representation, and the domain of jurisprudence with controversies over the purpose of constitutions. But this certainly merits further research to investigate how the liveliness and richness of the debate may even serve to protect rights and liberties. For instance, when identity cards were considered in both Australia and the United Kingdom, initially public support was as high as 80%. As time went on and citizens learned more about the proposals, as debates took place, and as further information entered into the fray, support began to ebb away. Open discourse and deliberation does not necessarily or inherently lead to either conservative or progressive choices.

I will end with the final anecdote regarding my travels to the U.S. When my traveling partner was being fingerprinted, the DHS official and I entered into an extended conversation regarding each others' practices. When he discovered that I worked with organizations that usually opposed his Department’s strategies and positions, the tone of the discussion transformed radically. He did not grow more confrontational, in fact the conversation became more intimate, as we shared in each others' concerns. The conversation continued for a few minutes, to the distress of those in the queue behind me (and to my traveling companion looking to move on). Almost simultaneously we both said to each other: "Keep up the great work.” I agreed that his contribution was important to the protection of our society, and he in turn recognized the value of my colleagues’ contributions.

The Open Society relies on a diversity of views, people willing to question policy. Even though the DHS official and I are on the opposite ends of the debate table, he and I both recognized that it is important that the debate table exists. In a number of policy instances
since September 11, 2001, we didn’t only need to slow down our legislative processes; we
needed to recall the principles of open debate. As such, I am not calling for deliberation for
the hope of coming to a consensus through some political process; I am calling for
deliberation for the sake of deliberation. We need opposing views, not only because it may
lead to better policy, but because it leads to public discourse. And the lack of public
discourse was the first and greatest casualty in this new security environment.

---

2 Baumgartner, Frank R., Bryan D. Jones, and John D. Wilkerson. “Studying policy
dynamics”. In Policy dynamics, edited by F. R. Baumgartner and B. D. Jones. Chicago:
3 Kingdon, John W. Agendas, alternatives, and public policies. 2nd ed. New York:
4 Braithwaite, John, and Peter Drahos. Global business regulation. Cambridge: Cambridge
6 Majone, Giandomenico. Evidence, argument, and persuasion in the policy process. New
8 Federal Register. “Interim Rule Passenger Name Record Information Required for
passengers on Flights in Foreign Air Transportation to or From the United States.”
Washington: Department of the Treasury Customs Service, 19 CFR Part 122, June 25,
2002.
Manifest Information and other data from Airlines to the United States.” Brussels: European
Commission, 24 October, 2002. Available from
10 European Commission. “Airline passenger data transfers from the EU to the United States
(Passenger Name Record) frequently asked questions.” Brussels, MEMO/03/53. March 12,
2003.
11 Federal Register. “Interim Rule Passenger Name Record Information Required for
passengers on Flights in Foreign Air Transportation to or From the United States.”
Washington: Department of the Treasury Customs Service, 19 CFR Part 122, June 25,
2002.
12 U.S. Customs. “Presentation to European Parliament Hearings on Customs Border
system of records.” Washington: Department of Transportation. Volume 68, Number 10.
14 Bolkestein, F. “Speaking notes for European Parliament LIBE Committee.” Brussels:
16 ibid., preamble para 3.
17 “The transfer of personal data to a third country which does not ensure an adequate level
of protection must be prohibited.” Ibid., preamble paragraphs 56-57.
18 Ibid. Article 25.2.
The responsibility has since shifted to the European Commission's Directorate on Justice, Freedom, and Liberty.

The "Computer Assisted Passenger Pre-Screening System" (CAPPS II) appears to be defunct at this time, but at the time of the negotiations, it was a pressing topic.


Though the data would be excluded from the CAPPS II program until a new agreement was reached, the data could be used to test the prospective system.


Ibid.

Ibid.

Ibid.


Ibid., p.10

43 Ibid.
44 Ibid.
45 Canadian Bar Association. "Letter to Senator Joan Fraser, Chair of the Senate Committee on Transport and Communications." Ottawa, 2004.
52 Ibid.
53 Ibid.
55 Previously called the General Accounting Office.


Ibid. p.119.

Ibid. p.71.


Ibid., p.16.


Ibid.


This even included the Secretary imitating a stabbing in the heart during a press conference to declare how dead it was.