V. When the Rubber Hits the Road

What Gallie had in mind when articulating the idea of essential contestability were comprehensive normative traditions and ideologies that range across the whole spectrum of social and political belief. His observations about social conceptualization might be applied equally to variations within the liberal tradition and, even more relevantly to our purposes in this inquiry, to differences in liberal cultural traditions. Indeed, what Rawls aspires to as an overlapping consensus is grounded in *liberal* diversity rather than the whole range of normative difference.

Although this study could have attempted to explore the wide range of differences among liberal polities – and it will indeed advert to a reasonably broad group of such polities, including those in Australia and India – it will most conveniently and manageably serve our purposes if it focuses primarily on differences that have come to notice in relations between the countries that form the EU and the US. Of course, even that is a simplification, because both the EU and the US embody a variety of traditions and understandings, and what we refer to as the views of each are but prominent and shifting expressions within each rather than an exhaustive characterization.

This has already been presaged in our brief comparative discussion of the roots of privacy in Europe and the US (Chapter III) and in our account of the regulatory traditions found in each (Chapter IV). The different constructions of privacy have played a large part in the ongoing debates between the EU and the US regarding digital technologies and the access to and use of digital data. In addition there are larger socio-political concerns that have informed their divergences.

Three cases will serve to illustrate the problems addressed by this study. They are: (A) the Passenger Name Record (PNR) controversy that has for several years dogged EU–US relations; (B) the US subpoenaing of SWIFT data; and (C) the National Identity (ID) card debate.

(A) The PNR Controversy

The PNR (Passenger Name Record) controversy began after 9/11 when the US began demanding certain personal information of passengers traveling to or from the United States, information that the EU considered to be private and therefore not appropriately demanded except under much narrower conditions than the US observed. Here we trace its main outlines.

Whenever a person books a flight from country A to country B,[1] a Passenger Name Record (PNR) is created. That record contains various *data*; it has a *location*; and it acquires a *history*.[2]

Data. The PNR will contain a lot of personal data that the traveler is asked to provide – formal data such as name, address, date of birth, credit card information, frequent flyer numbers and billing and approval codes (if relevant), as well as informal data concerning preferences such as meals or religious preferences, sleeping preferences if the traveler is also booking a hotel or even notes from the agent if they are thought pertinent.[3] There will also be various ancillary data about the agent who is making the booking or about some other person if that person is making the booking for the person who is traveling. All told, over thirty different fields are usually represented.

Location. This information is then stored – not usually on the airline or travel agent's computer system but in the centralized database of a Computerized Reservation System (CRS) or Global Distribution System (GDS) such as Sabre, Galileo/Apollo, Amadeus or Worldspan. These CRSs are owned by private- or publicly-traded companies. Amadeus, a Spanish corporation with its primary operations in Germany, is largely owned by the airlines that use it. The others are based in the US and are used but not owned by US-based airlines.

History. As travelers make changes or buy additional tickets, and even if they cancel, the information is updated and to some extent consolidated. An audit trail is created, and though data can be changed they are not expunged. An approximation of such a procedure is as follows:

> When a travel agent makes a reservation, they enter data on a CRS/GDS terminal, and create a PNR in that CRS/GDS. If the airline is hosted in a different CRS/GDS, information about the flight(s) on that airline is sent to the airline's host system, and a PNR is created in the airline's partition in that system as well. What information is sent between airlines, and how, is specified in the Airline Interline Message Procedures (AIRIMP) manual, although many airlines and CRS's/GDS's have their own direct connections and exceptions to the AIRIMP standards.
>
> If, for example, you make a reservation on United Airlines (which outsources the hosting of its reservations database to the Galileo CRS/GDS) through the Internet travel agency Travelocity.com (which is a division of Sabre, and uses the Sabre CRS/GDS), Travelocity.com creates

1 It need not be an international flight, but we are restricting the example to those.

2 See Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?" at: http://hasbrouck.org/articles/PNR.html.

3 Most airline bookings are made through travel agents and so PNRs will often contain other details concerning car hires, hotel rooms, companions, special requests etc.

> a PNR in Sabre. Sabre sends a message derived from portions of the Sabre PNR data to Galileo, using the AIRIMP (or another bilaterally-agreed format). Galileo in turn uses the data in the AIRIMP message to create a PNR in United's Galileo "partition."
>
> If a set of reservations includes flights on multiple airlines, each airline is sent the information pertaining to its flights. If information is added later by one of those airlines, it may or may not be transmitted back to the CRS/GDS in which the original reservation was made, and almost never will be sent to other airlines participating in the itinerary that are hosted in different CRS's/GDS's. So there can be many different PNR's, in different CRS's/GDS's, for the same set of reservations, none of them containing all the data included in all of the others.[4]

The relevance of this is that there is little control over the uses to which these private companies can put their data. They may make commitments about how they will use it and share it, but there is little effective oversight.[5]

In addition, as the US government's Secure Flight Program[6] (formerly CAPPS II) becomes operational, these PNRs will be accessed and fed into the Passenger and Aviation Security Screening Records (PASSR) database of the Transportation Security Agency (TSA), which is a division of the Department of Homeland Security (DHS). The information will be used by the US government (along with other information) to fill out passenger profiles, including "selectee" and "no-fly" watch lists, as well as to match passenger data with existing lists.[7] Although Secure Flight was expected to be operational in 2005, its full implementation was significantly delayed – partly for privacy-related reasons – until 2009, when

---

4 Hasbrouck, "What's in a Passenger Name Record (PNR)?", 3.

5 Recognizing these weaknesses, we have undertaken to provide a means by which the companies themselves, along with external oversight bodies, can query the state of accountability in a given organization and identify where shortcomings exist. The Surveillance Technology Accountability Assessment Tool (STAAT) in Chapter IX of this study allows those interested in exercising greater control over questions of data construction, data mining and data sharing a means for grounding their efforts to improve these and other areas of digital technology use. The application of this tool is available to any entity engaged in digital technology surveillance.

6 See http://www.tsa.gov/what_we_do/layers/secureflight/editorial_1716.shtm. CAPPS II (Computer Assisted Passenger Prescreening System) was to be the successor of CAPPS I, developed in 1997. Opposition to the proposed CAPPS II led to its "demise" and reconstitution as Secure Flight.

7 Security lists were first developed in 1990 (and were originally administered by the FBI) to keep an eye on people "determined to pose a direct threat to U.S. civil aviation", but they moved to center stage only after 9/11. Being on a "selectee" list will heighten the security that a person will be required to undergo; being on a "no fly" list will lead to a person's being prevented from flying. "No-fly" lists are also distributed to other agencies concerned with visas, border crossings and law enforcement. It is thought that well over 300,000 names are on the lists, though information is not readily available on either numbers or the criteria used to make determinations.

it began to be implemented in stages.[8] Until now, the airlines themselves have been charged with matching names to the existing lists (which have been drawn up using other data).[9]

There appears to be no legal barrier to the US government using PNR data for security purposes.[10] However, in the case of German citizens based in Europe who wish to fly to the US, the US does *not* have jurisdiction over them at that point and there may even be laws against some of that data being transmitted without authorization. Indeed, as we have already noted, the European Parliament has a directive that severely limits the circumstances under which such data may be shared and used.[11] After 9/11 an interim agreement between Europe and the US was reached regarding access to PNR data for security purposes. That agreement was subsequently determined to be incompatible with European law and work then proceeded on a new agreement that was supposed to be concluded by July 2007, when the sun set on an interim arrangement. Controversy continues, though temporary understandings have been in place, allowing EU–US traffic to continue.

The proposed agreement reduced the number of pieces of PNR data to which US authorities could get access to nineteen, though some of the reduction involved combining data that had otherwise been kept discrete. Data concerning ethnicity, however, could not be accessed. It was further proposed that the US could store the data "actively" for a period of seven years, with the possibility of "dormant storage" for a further eight years. Although this involved a significant extension of the storage period (from three years), it was argued that better safeguards had been put in place. Significantly, the July 2007 bombings in Glasgow and London prompted PNR data-gathering initiatives in Europe similar to those in the US.

However, the proposed agreement ran into trouble with the European Parliament, with an overwhelming majority of its members determining that it was "substantively flawed". The main objections were that: (a) the agreement on

---

8 "Secure Flight was implemented in two phases. The program initially assumed the watch list matching responsibility for passengers on domestic flights from aircraft operators beginning early 2009. In a second stage of implementation, begun in late 2009, the Secure Flight program assumed, from Customs and Border Protection and the international air carriers, the watch list matching function for passengers on international flights." See "TSA to Assume Watch List Vetting with Secure Flight Program" http://www.tsa.gov/press/releases/2008/1022.shtm. The program has now been fully implemented.

9 If a "no fly" match occurs, the airline agent is required to call a law enforcement officer to detain and question the passenger. In the case of a "selectee", the boarding pass will be marked and the person given additional screening by security.

10 49 U.S.C. § 44909 (c) (3). However, there may be more than "actual passenger" data in a PNR, and the statute does not require the data in advance.

11 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. This led, in 2000, to an EU/US agreement on "safe harbor" privacy principles: http://www.epic.org/privacy/intl/EP_SH_resolution_0700.html.

the collection, use and storage of PNR data was constituted simply by the non-binding assurances contained in a letter (that could be unilaterally changed); (b) there were no assurances that the data would be used only for counter-terrorism (though allowance was made for its use by the US Government for "unspecified additional purposes"); (c) in exceptional cases, information on travelers' ethnicity, political opinions or sexual orientation could be accessed; (d) that the reduction of fields was "largely cosmetic due to the merging of data fields instead of actual deletion"; and (e) retention of data under the proposed agreement was inordinate and raised the possibility of massive profiling. At the same time, the Parliament raised concerns about the proposed European data-gathering initiative.[12]

Even so, an agreement was reached with the European Union on July 23, 2007,[13] followed by a Letter (July 26) explaining how the US Department of Homeland Security (DHS) intended to collect, use and store the data it gained.[14] A DHS Report released in December 2008 came to an irenic conclusion about DHS compliance with the Agreement. However, it was an internal report including no EU representatives and, according to some reviewers, had failed to be adequately responsive to requests by travelers to see data (or all the data) held concerning them.[15]

The PNR controversy raises a number of important ethical questions, some specific and some general. The most general question relevant to the focus of this study is whether it is possible to develop standards for personal data collection, use and management that can be accepted by all the parties. Although we are concerned fairly specifically here with the EU and the US, the question can be cast to range over liberal democratic polities generally. More specifically, there are issues raised by the PNR controversy narrowly but which are also transferable to other contexts in which data are gathered. Here is a sample:

- Ever since "selectee" and "no-fly" watch lists have been compiled, errors have occurred and innocent passengers have been inconvenienced, sometimes quite seriously. It has not proven easy to rectify such errors.

---

12 However, the European Commission introduced such a plan – very similar to that which was so roundly criticized in the European Parliament – on November 6, 2007.

13 See: *Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)*, http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf.

14 Appended to *A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.

15 See *EDRI-gram* January 14, 2009, http://www.edri.org/edri-gram/number7.1. By June, 2010, provisional agreement appeared to have been reached, pending further negotiations. However, as of June 30, 2011, a further draft agreement was criticized for many of the same reasons as previously – not being limited to terrorism and serious crime, unnecessarily long data retention, lack of judicial redress for data subjects and an absence of any guarantees of independent oversight. See "EU-US PNR Agreement Found Incompatible with Human Rights", *EDRI-gram*, 9, no. 3 (June 29, 2011), available at: http://www.edri.org/edrigram/number9.13.

- Especially from the side of the EU, there has been a concern about personal data being collected for one reason – to combat terrorism – and then being used or being available to be used for other reasons (say, tax evasion or money laundering). Apart from such data being used for purposes to which consent has not been given, there are serious issues of disproportionality in collecting personal data for less serious social concerns.
- There is very little transparency with national security data collection. For example, it is not known or disclosed how many people are on watch lists. There is secrecy about the numbers of people on watch lists, or whether the personal data of some citizens is as likely to be surveilled as that of others.
- The lack of transparency extends to information about who is responsible for the compilation, protection and correction of watch lists.
- The lack of transparency further extends to the criteria used to compile watch lists and to disclosures concerning their effectiveness. For example, is Secure Flight really needed or will it simply add to the amount of information that government may amass about individuals? Transparency is an important liberal democratic value, and though it is recognized that security interests may sometimes require secrecy of data and strategies, the limits to such secrecy ought to be determined in the light of public debate.[16]
- Although transparency is typically a necessary condition for accountability it is not sufficient. So what oversight and accountability mechanisms are in place to ensure regulatory and ethical compliance?

Behind these more specific questions about the collection of PNR data there stand some more general ethical questions. For example:

- What privacy, if any, do we have a right to, and why? What are the limits to such a right?
- What security do we have a right to, and how should it best (ethically and practically) be enabled/protected?
- What is the appropriate role of government in ensuring security and what constraints should be placed on its security activities?
- To what extent may one government legitimately make demands of another government or on those under the jurisdiction of another?

16 These issues of practical policy implementation have led us to consider recommending that an internal body be developed within law enforcement and intelligence organizations that would be responsible for aiding surveillance practitioners in sorting out such problems. The creation of Techno-ethics Boards, discussed in Chapter IX, offers one means to build capacity within government agencies engaged in surveillance operations of this and other types (see Peter Mameli, "Tracking the Beast: Techno-Ethics Boards and Government Surveillance Programs", *Critical Issues in Justice and Politics* 1, no. 1 (2008): 31–56).

These are large questions – perhaps too large to be adequately resolved within the framework of the present study. Yet they cannot be wholly sidestepped. We will take some steps toward addressing them in later chapters.

(B) The Terrorist Finance Tracking Program and SWIFT Controversy

The events related to this second controversy came to light with a *New York Times* article on June 23, 2006, in which it was revealed that not long after 9/11 the CIA, through the US Treasury Department, secretly put (via administrative subpoena[17]) pressure on a Belgian cooperative – SWIFT – that routes over 11 million international financial transactions per day (amounting to US$6 trillion) to give it access to its records.[18] The US Government claimed that the emergency powers granted by Congress soon after 9/11 allowed it to do so and that it was not prevented from doing so by "American laws restricting government access to private financial records because the cooperative was considered a messaging service, not a bank or financial institution."[19]

Exactly what was looked at is not known, though US authorities have naturally argued that the data reviewed were limited and that they focused on terrorism, not tax fraud or drug trafficking. It appears that the primary tool used on the subpoenaed data was "link analysis", whereby those who had suspected ties then had all wired financial transfers tracked in which they were involved. It was claimed that the analyses had yielded positive results (though this has been disputed).[20]

When the US actions were made public (initially by a whistle blower), the Belgian Government immediately protested and a European Parliament resolution (July 7, 2006) alleged that "the SWIFT transfers were undertaken without regard to legal process . . . and . . . without any legal basis or authority." Although the

---

17 Unlike other subpoenas, administrative subpoenas do not have to be reviewed by judges or juries. They are issued under the International Emergency Economic Powers Act 1977. For discussion, see Charles Doyle, *Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations* (Congressional Research Service, 2005), http://www.fas.org/sgp/crs/natsec/RL32880.pdf.

18 Eric Lichtblau and James Risen, "Bank Data is Sifted by U.S. in Secret to Block Terror," *The New York Times*, June 23, 2006, A1. Other articles appeared in the *Wall Street Journal* and *Los Angeles Times* on the same day. SWIFT is an acronym for the Society for Worldwide Interbank Financial Telecommunication: "SWIFT is the industry-owned co-operative supplying secure, standardised messaging services and interface software to nearly 8,100 financial institutions in 207 countries and territories." It was founded in 1973. http://www.swift.com/index.cfm?item_id=43232.

19 Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, US Treasury. This was backed up by reference to *US v. Miller*, 425 US 435 (1976).

20 The claim is that it was helpful in the tracking of Hambali, the Indonesian leader of the al-Qaeda-related terrorist organization, Jemaah Islamiyah. Other suggestions about its usefulness were reported in the original *New York Times* and *Wall Street Journal* articles.

Belgian Privacy Protection Commission sympathized with the US's concern about terrorism and security, it argued that the requests were not focused on individuals suspected of terrorist activities and involved the transfer of massive amounts of data. Moreover, SWIFT was not a mere "messenger" but a "controller" in the processing of personal data. It concluded that European law concerning personal data was more stringent than US law with respect to "the principle of proportionality, the limited retention period, the principle of transparency, the requirement for independent control and an adequate protection level."[21] SWIFT had, furthermore, failed to get assurances that were required under European law concerning data of the kind involved.[22] Talks subsequently commenced to try to work out a common framework for the sharing of data.

US authorities argued that disclosure of the SWIFT actions had been very damaging to the fight against terrorism. In addition there was a back story about pressure that was placed on the *New York Times* to refrain from publishing the results of its journalistic investigation.

Here, too, a whole series of questions emerged, some specific and others more general. The specific questions focused on:

- the degree of specificity that desired disclosures of private financial information ought to have;
- whether those whose financial transactions were disclosed to US authorities ought to have been informed;
- whether SWIFT ought to have informed European authorities about its actions;
- whether the differences between European law and US law were significant and, if so, why;
- whether the privacy invasions had, in fact, yielded any information of significance, assuming that it would have been of justificatory value;
- whether a measure that might have been justified in emergency terms could still be justified five years later (since the gathering of such data had been ongoing);
- what controls US authorities placed on the program and the data it received, and whether those controls were enforced;

21 "Summary of the Opinion on the Transfer of Personal Data by SCRL SWIFT Following the UST (OFAC) Subpoenas", http://www.privacycommission.be/communiqu%E9s/summary_opinion_Swift_%2028_09_2006.pdf. A non-official translation of the whole opinion can be found at: http://www.privacycommission.be/communiqu%C3%A9s/opinion_37_2006.pdf. See also Dan Bilefsky, "Data Transfer Broke Rules, Report Says", *The New York Times*, September 28, 2006.

22 Embarrassed, SWIFT tried to wriggle out of the rebuke by claiming that because it had offices in the US it was required to obey the subpoenas.

- whether the newspapers that published the articles revealing the program were justified in doing so (in the face of US Administration opposition); and
- whether the whistleblower who disclosed what was going on was justified in doing so.[23]

No doubt there are other questions. As with the PNR data controversy, the SWIFT one generated similar broad questions concerning the scope of privacy, what constitutes private data, what kinds of actions compromise privacy, the ethical demands that appeals to security can make, issues of efficacy and probability and the trade-off between security and privacy.

In the follow up to the SWIFT controversy there were, as in the case of PNR data, further negotiations between the EU and the US regarding European financial transactions operated through SWIFT, with an agreement reached on June 28–29, 2007.[24] The US committed itself to using SWIFT data exclusively for counterterrorism purposes and to retaining the data for no longer than five years. For its part, SWIFT was to observe privacy requirements according to EU principles promulgated in 2000. Banks using SWIFT were to inform their customers about any transfers of data to US authorities. Moreover, the EU gained a right to inspect US investigators' use of European data, given that US laws regarding the use of data are not as stringent as those of the EU.

But even these concessions have not stilled the controversy and there has been continuing debate within the EU over their adequacy. An agreement signed on November 30, 2009, was possible only because of a politically necessary German abstention.[25]

(C) The Controversy over National Identity (ID) Cards[26]

One might infer, from an examination of the PNR and SWIFT debates, that the European Union has a much stronger and better developed concern for privacy than the US. That inference would seem to be justified. However,

---

23 As with the PNR, we believe that by forcing deeper consideration of the accountability questions at hand prior to action being taken the utilization of both STAAT and Techno-ethics Boards could aid in mitigating abuses in the areas that we noted when discussing the SWIFT case.

24 Reported in *EDRI-gram* (biweekly newsletter about digital civil rights in Europe), Number 5.13, 4 July 2007. See also: http://www.statewatch.org/news/2007/jul/eu-usa-pnr-agreement-2007.pdf.

25 See text of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program (30.10.2009), at: http://eur-lex.europa/LexUriServ/LexUriServ.do?uri=OJ:L:2010:008:0010:0016:EN:PDF. For further follow-up see *EDRI-gram* Newsletter 8, 3 (Feb 10), 2010, available at: http://www.edri.org/edrigram/number8.3. Since then, the European Parliament has (2/11/2010) rejected the latest agreement (http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-565959) and the discussions continue.

26 For some of the early research on this section, we are grateful to Vincenzo Sainato.

the situation becomes rather more complicated when we shift our focus to a different controversy – that concerning the issuing of National Identity (ID) cards. Such is the strength of feeling against them in the US that there is at best a perfunctory discussion about the use of ID cards – it is, by and large, a political non-starter.[27] Australians are also largely opposed to ID cards. The Labor government of Bob Hawke attempted to introduce the Australia Card in the late 1980s but abandoned the attempt in 1987 (largely as a result of concerns about the accuracy and security of data). However, most countries within the EU have mandated ID cards for years and make considerable use of them for access to a variety of government services as well as for security measures. India is set to introduce an ID card for similar reasons. Needless to say, aside from privacy concerns, there are prodigious logistical and other problems in a large developing country such as India.

In this context, it is worth tracing some of the recent contours of the ID card controversy in the United Kingdom (UK) – a controversy that puts it at some odds with its fellow European Unionists. Some ten European countries have compulsory ID cards, another ten have voluntary ones while four, including the UK, as yet have none.

Though mooted in 2002, the UK Identity Cards Bill was first presented to Parliament in 2004. It contained a number of components, one of which was the development of a National Identity Card. The card was supported as a "public interest" measure, where the public interest was understood to encompass "national security", "the prevention and detection of crime", "the enforcement of immigration controls", "the enforcement of prohibitions on unauthorized working or employment" and the securing of "efficient and effective provision of public services". In later discussions, considerable weight was given to its supposed benefits in countering identity theft. The card was not required to be carried at all times.

Following a general election in early May 2005, a revised Bill was presented on May 25, 2005, to a Labour government with a reduced majority.[28] It gained narrow approval in the House of Commons in October but criticism in the House of Lords led to significant amendments in 2006. The amendments were

27 Although some have argued – at least in the context of health care, that some system of patient ID numbers would be more protective of privacy (as well as more efficient and less mistake-prone) than the present system for matching health data, there is strong opposition even to this. For the argument in favor of such see the RAND study, Richard Hillestad, James H. Bigelow, Basit Chaudhry, Paul Dreyer, Michael D. Greenberg, Robin C. Meili, M. Susan Ridgely, Jeff Rothenberg, Roger Taylor, *Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System* (Santa Monica, CA: Rand, 2008), available at: http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG753.pdf. In the UK, NHS members already have an identifying number which entitles them to a European Health Insurance Card.

28 The Bill is available at: http://www.publications.parliament.uk/pa/cm200506/cmbills/009/2006009.htm.

not passed and the Bill shuttled back and forth between the House of Lords and House of Commons. After five renditions the Bill was finally passed by both houses in March 2006. The agreement reached made the card voluntary (provided a passport was held) and delayed its implementation, though 51 types of individual data including fingerprints, iris scans and face scans would still be entered into a National Identity Register (NIR), one of the Bill's other components. The major parties declared that it would be an election issue in 2010, with the Labour Party indicating that, if it won, it would make the card mandatory. The new Conservative leader, David Cameron, indicated his opposition to the card on principle. The Conservatives now govern in a coalition with the Liberal Party and, for a time, the ID card issue is dead.

In consequence, the cards have not been introduced (though some were slated to be issued in 2009), and if they had been it would have taken several years for most people to have them (or an upgraded passport). As it is, practical difficulties plagued both the development of the NIR and the introduction of the cards, and if in the future there is any end product it may not exactly match the legislation. The debate about the cards was particularly vigorous, some opposing the cards altogether and others focusing on particulars associated with the UK card. Major concerns included the following:

- that the cards would be no more (or not significantly more) effective than measures already in place to achieve what they were intended to achieve;
- the huge cost involved in introducing them – a cost for the government as well as for individuals;
- that the card would provide a pretext for discrimination against minorities, a problem that had arisen in other European countries that have identity cards;
- that, as with all governmental data gathering initiatives, government misuse of data would increase its control of individuals – such initiatives were viewed as further encroachments of the so-called surveillance society[29]; and
- the possible vulnerability of data either gathered for the NIR or inscribed on cards. Several notorious cases in which data have been lost or stolen have shaken confidence that personal data will be secure. Although it was argued that a National ID Card would help to counteract rising identity theft, it was also argued that a national register or card would, in fact, make it easier by providing a "one stop" opportunity for the theft of salient data.

29 Once again, the inescapable need for useful accountability mechanisms comes to the fore of the discussion. Although the existence of the "Surveillance Society" means different things to different people, what seems to be generally accepted is that the means for retaining control of its growth is accomplished through increasing transparency and monitoring of actions in a better lit environment. We believe that the utilization of tools such as STAAT and internal oversight bodies such as Techno-ethics Boards could satisfy part of this requirement.

What the three foregoing cases illustrate is the great complexity involved in developing appropriate standards for security and privacy both between and within liberal democratic societies. They constitute the practical challenge of the present study.