TO WHAT EXTENT SHOULD NATIONAL SECURITY INTERESTS OVERRIDE PRIVACY IN A POST 9/11 WORLD?

Cynthia Laberge*

September 11, 2001, and the subsequent bombings in Madrid and London in 2004 and 2005, made it clear that no country was immune from terrorism. In the wake of those attacks, nations united to implement programmes to track terrorists and prevent future attacks. Leading the worldwide effort was the US with its programmes to screen travellers through airline reservation systems, mine data of unsuspecting telecommunication company customers, and track and intercept banking communications. As these programmes came to light (often through leaks to the press), many were criticised both in the US and overseas as invading privacy and violating laws. Some of these programmes have been challenged in courts in the US and Europe, others have been scaled back, restructured, or discontinued. The question is: Do these programmes actually work and, even if they do, are they worth the cost to privacy interests?

I INTRODUCTION

If a bird has two legs, and a man has two legs, a man must be a bird.[1]

If a man is suspected of being affiliated with terrorists, he must be a terrorist.[2]

* InternetNZ Senior Research Fellow in Cyberlaw, Victoria University School of Law, Wellington, New Zealand, 2008.

1 Professor John Haven *Mental Philosophy: Including the Intellect, Sensibilities and Will* (Sheldon and Company, New York, 1862) at <www.archive.org>. The original quote reads "All birds are bipeds, no man is a bird; therefore no man is a biped."

2 Department of Homeland Security (DHS), Office of the Secretary, Privacy Act of 1974 (US) 5 USC § 552a Public Law No 93-579; Customs and Border Protection Advanced Passenger Information System Systems of Records (23 August 2007) 72 Federal Register 163 48349- 48353 <www.edocket.access.gpo.gov>.

Is this where we are headed? In the name of stopping terrorists are we compiling data on innocent people who share a similar profile as those on our "most wanted" lists, and treating them the same?

Since 9/11, the world has become obsessed with terrorism. Understandably so. We expect our governments to protect us, at a minimum from foreseeable acts of violence. It is an onerous commission. But in its zeal to do the right thing, are governments actually doing more harm than good? And in the name of security, are we complicit in sacrificing liberty?

The security/liberty debate is not new. It has been ongoing since the time of Cicero at least:[3]

> Though liberty is established by law, we must be vigilant, for liberty to enslave us is always present under that very liberty. Our Constitution speaks of the 'general welfare of the people.' Under that phrase all sorts of excesses can be employed by lusting tyrants to make us bondsmen.

But with the law unable to keep pace with technological advances, are we letting technology determine how best to protect us? With oversight and accountability at an all-time low, are the technological programmes that are being put in place to combat terrorism effective? And if so, at what cost?

Regional, national and global databases, containing records on everything from finances and vehicle ownership, to DNA records, are booming. Investment in technologies to analyse and cross-reference data in those databases is also booming. The security-related goal: to stop the next terrorist attack. Governments justify this previously unprecedented accumulation of data on the grounds that they are faced with an unprecedented threat. If this is true, does it also justify the unprecedented secrecy surrounding our governments' activities?

This paper is an attempt to chart the path we are currently on in balancing national security with privacy and, ultimately, liberty by giving an overview of the co-operative efforts, privacy and counter-terrorism laws of four countries (the United Kingdom, United States, Australia and New

---

3 Marcus Tullius Cicero, Roman orator – 106- 43 BC (Thanks Earl). For more recent writing on this topic see: Christopher Slobogin *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (The University of Chicago Press, Chicago, 2007); Daniel J Solove "Data Mining and the Security-Liberty Debate" (2008) 74 University of Chicago Law Review at 343; George Washington University Law School Public Law Research Paper no 278 Social Science Research Network <www.ssrn.com>; Daniel J Solove "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review at 745, George Washington University Law School Public Law Research Paper no 289; K A Taipale "Technology, Security and Privacy: The Fear of Frankenstein, The Mythology of Privacy and The Lessons of King Ludd" (2004/2005) 7 Yale Journal of Law & Technology at 123; Gregory J Walters "Privacy and Security: An Ethical Analysis" in Chapter 5 of *Human Rights in an Information Age: A Philosophical Analysis* (University of Toronto Press, London and Toronto, 2001); Jacob R Lilly "National Security at What Price? A Look into Civil Liberty Concerns in the Information Age under the USA PATRIOT Act" from Adam D Moore (ed) *Information Ethics: Privacy, Property, and Power* (University of Washington Press, Seattle, 2005) at 417.

Zealand) and four international institutions (the United Nations, the OECD, the Council of Europe, and the European Union), and the technologies employed in the fight against terrorism (used predominantly in the United States). It makes no predictions, nor does it presume to present an in-depth analysis of privacy or counter-terrorism laws, which have already been covered in depth elsewhere by experts.

What this paper attempts to do is provoke thought and stimulate discussion on the direction that the West (primarily) is taking to fight the "scourge of international terrorism."[4] And to posit what role we can play in holding government accountable for protecting our security, without unduly sacrificing our privacy, and thereby our liberty.

II BACKGROUND

The mere mention of 9/11 evokes images of destruction, and conjures up feelings of shock and disbelief. In the United States, the attacks by terrorists wielding four commercial airliners as weapons against the World Trade Center buildings in New York, the Pentagon, and an unsuccessful attempt on the White House,[5] spawned a massive government and legislative overhaul almost immediately. Although the 9/11 Commission Report[6] into the events leading up to the 2001 tragedy was not finalised until 2004, it was not hard to suspect from the outset that communications failures among government agencies would bear at least part of the blame for the effectiveness of the attacks.[7] As it turns out, they played a substantial part.

As the various United States government agencies pulled together in the aftermath, so too did the nations of the world. Just as the attack on Pearl Harbour almost 60 years earlier had "convinced the American people that preparing for the next sneak attack was everybody's business,"[8] so the events of 9/11 convinced the rest of the world that no country was immune from terrorism and

---

4 Resolution on threats to international peace and security caused by terrorist acts UNSC Res 1377 (2001) < www.un.org>.

5 United Airlines flight 93 crashed in a field in Pennsylvania. There is evidence to suggest that passengers and crew may have overtaken the highjackers to prevent it from returning to Washington, D.C. where its destination is suspected to have been the White House. See Ted Bridis "Last Minutes of Suicide Flight 93, Destination the White House" (9 August 2003) *The Sydney Morning Herald* <www.smh.com.au>.

6 *The 9/11 Commission Report* (22 July 2004) 1 <www.911commission.gov>.

7 The coordinated suicide attacks in New York, Washington, Virginia and Pennsylvania killed 2,974 victims, and the 19 highjackers. See <www.wikipedia.org>. See also *The 9/11 Commission Report,* above n 6 and FBI whistleblower Coleen Rowley's memo to FBI Director Robert Mueller (21 March 2002) *Time.com* < www.time.com>.

8 Douglas T. Stuart *Creating the National Security State* (Princeton University Press, Princeton, New Jersey, 2008) at 3.

something had to be done. That 77 nations lost citizens in the attacks only added to the strength of their conviction.[9]

To be sure, terrorism awareness did not start on 12 September 2001. Europe had experienced terrorism on its own soil well before,[10] and had enacted laws on terrorism since at least the 1970s.[11] Yet the events of 2001 spurred much of the world into accelerated action:[12]

> [P]olicy-makers around the world rushed to examine their law enforcement capabilities and the suitability of these tools to the new *war on terror*. This examination resulted in a wave of legislation around the world, aimed at increasing the power of law enforcement agencies.

But more than national introspection and legislating was happening post-9/11. Intergovernmental co-operation was also on the rise. While this in itself was not unprecedented, the scale of it was. Not since the era immediately after World War II, which gave us the United Nations, had the world concentrated its focus so single-mindedly. Not only were new joint efforts occurring through pre-existing institutions (the UN, the Council of Europe and the European Union, to name a few), but new alliances were also being forged, both between governments, and between government and private enterprise.

For its part, the United States was enlisting national co-operation to create programmes to combat terrorism. Most, if not all, involved personal data. Many involved "data mining", for example, "Total Information Awareness," and Fusion Centres. (See below.)

Data mining is not new; it is a new application of pre-existing technology. Sometimes called data or knowledge discovery, it is "the process of analyzing data from different perspectives and summarizing it into useful information." Data mining software "allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases."[13]

---

9 See the International Criminal Police Organization (Interpol) website <www.interpol.int>.

10 At the 1972 Summer Olympic Games in Munich, 11 Israeli athletes and coaches and one West German police officer were killed. Five of the eight terrorists who had taken the Israelis hostage were also killed. < www.wikipedia.org>.

11 European Convention on the Suppression of Terrorism (27 January 1977) ETS No 090 < www.conventions.coe.int>.

12 Martin Charles Golumbic *Fighting Terror Online* (Springer Science+Business Media, LLC, New York, 2008) at 1. See also Transnational Terrorism Security and the Rule of Law "Notions of Security: Shifting Concepts and Perspectives" (15 February 2007) at 54-55 <www.transnationalterrorism.eu>.

13 Bill Palace, Anderson Graduate School of Management at UCLA (Spring 1996) *UCLA.edu* < www.anderson.ucla.edu>.

Other US programmes (also involving personal data), concerned the screening of airline passengers before their arrival in the United States (APIS,[14] CAPPS II,[15]ATS,[16] Secure Flight), and the screening of telecommunications (TSP).[17] (See below.) Most of these efforts were in place well before 2001 was over.

There were also other programmes in place requiring international co-operation. Shortly after 9/11, co-operation was sought from abroad to assist the US in its "War on Terror" through access to financial transaction data (SWIFT),[18] as well as airline passenger records (PNR)[19] from every airline carrier flying over, landing in or departing from the United States. Moreover, the US had continued to have access to international telecommunications information since World War II through the UK/US Agreement. (See below.)

As these programmes came to light (often through leaks to the press, sometimes years after they started), many were criticised, not only in the United States, but around the world, as invading privacy**,** and violating the law. Some programmes have been challenged in court both in the United States and Europe; others have been scaled back, restructured, or discontinued altogether.[20] Whether or not any of these programmes actually work to protect national security is not entirely clear. Although there are clues as to their effectiveness, the ultimate question remains: even if they are effective, are they proportionate to the degree of privacy they are invading, or do they go too far?

In addition to challenging legal barriers, these programmes are doing something else: they are challenging cultural ones. As our post-9/11 world becomes even smaller, it has become manifestly evident that success in defeating terrorism will depend on how well the nations of the world can overcome national differences, both legal and cultural.

One legal and cultural challenge lies in bridging the gap between differences in the concept of privacy. All Western societies value privacy but they protect it differently. These differences, unless harmonised,[21] have the potential to undermine the fight against terrorism, particularly with regard to the sharing of data.

---

14 Advance Passenger Information System.

15 Computer Assisted Passenger Pre-screening Program II.

16 Automated Targeting System.

17 Terrorist Surveillance Program.

18 The Society for Worldwide Interbank Financial Telecommunication.

19 Passenger Name Records.

20 Total Information Awareness (TIA), CAPPS II, Multistate Anti-terrorism Information Exchange (MATRIX).

21 A term used in the EU, meaning to make uniform and coherent.

Added to this challenge is the availability of new technology (or the new application of old technology) allowing for the expeditious analysis of volumes of data never before imagined. How much access should government have to data on its citizens? The institutions of Europe (the Council of Europe and European Union), and the UK, US, Australia and New Zealand have decided this question differently. But if the world is to work together to combat the threat of terrorism, these are some of the obstacles that it must overcome. To achieve a unity of vision requires a unity of action.

This paper is set out in nine substantive parts:

Part III is a snapshot of our post-9/11 world;

Part IV posits why we should continue to care about privacy;

Part V reviews the evolution of the concept of privacy in the above four countries;

Part VI reviews the development of the concept of data protection in the 20th century;

Part VII reviews present-day efforts to protect data privacy;

Part VIII reviews salient pre-9/11 counter-terrorism instruments and recommendations of the Council of Europe, the UK, US, Australia and New Zealand;

Part IX reviews post-9/11 instruments and co-operative efforts regarding personal data privacy;

Part X considers whether any of these programmes stops terrorism; and

Part XI considers where we are headed.[22]

III WHERE WE ARE TODAY – A SNAPSHOT

In 1888, with the slogan "You press the button – we do the rest,"[23] Kodak introduced its snap camera. Its ability to capture someone's image instantaneously without their knowledge or consent was one technological development that led to a review of privacy law in the United States.[24]

Today's technological revolution – computers with the ability to process unprecedented amounts of information – is again raising the question of whether the law needs updating to protect our privacy, our *data* or *information privacy*. Just what is data or information privacy? It has a number

---

22 *Note: At the time of writing* throughout the paper means March 2009. Unless otherwise noted, websites were accessed between February and March 2009. References to "the West" refers specifically to: the Council of Europe, the European Union, the UK, US, Australia and New Zealand. While not technically accurate, for ease of reference the term also encompasses the United Nations and the Organisation for Economic Co-operation and Development.

23 See Kodak history web page at <www.kodak.com>.

24 Samuel D Warren and Louis D Brandeis "The Right to Privacy" (1890) 4 Harvard Law Review at 193. As articulated by Warren and Brandeis, another development was the rapid rise of newspaper distribution and the attendant invasive reporting of information previously considered private.

of current definitions, including: the "collection, dissemination, and use of personal information"[25] or "control over access to oneself and to information about oneself."[26] These definitions do not stray too far from that proffered by Dr Alan Westin in the 1960s: "The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[27]

But how much information about ourselves should we be able to control? Is it reasonable to expect that all personal information be kept private? Or should only personally identifiable information be protected, and only in certain contexts?[28]

Consider the case of Deena Pawson, a store employee who lost her job for "serious misconduct" by writing on her Bebo web page that "work sux" and that having to work until midnight was "gay like the management."[29] Was it reasonable for her to expect that information posted on her personal Web page on the Internet would remain private, or at least accessible only by a select few?

There is also the case of Katherine Evans. The nineteen year old was suspended from school for three days for "cyberbullying" a teacher, and demoted from her advanced placement classes for writing on her Facebook page: "Ms. Sarah Phelps is the worst teacher I've ever met!" She also posted a photo of the teacher and invited other students to "express your feelings of hatred."[30] What reasonable expectations of privacy did she have upon inviting others to comment on her posting? She is suing for breach of her right to freedom of speech under the US Constitution.

And then there are the tragic cases of Megan Meier and Marie Davis. Megan struck up an apparent online relationship on MySpace with "Josh Evans," a fictitious character created by a mother trying to investigate Megan's role in the spreading of rumours about her daughter. When "Josh" ultimately told Megan that the world would be a better place without her, Megan committed

---

25 Daniel J Solove "A Brief History of Information Privacy Law" in Christopher Wolf, Proskauer Rose LLP's *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (PLI, New York, 2006) at 1-4.

26 Adam D Moore "Toward Informational Privacy Rights" (2007) 44 San Diego L Rev at 809, 812.

27 Dr Alan F Westin *Privacy and Freedom* (New York, Atheneum, 1967) at x.

28 For a fuller discussion on conceptualising privacy, see Mark Hickford, Senior Consultant to the New Zealand Law Commission *A Conceptual Approach to Privacy* (NZLC MP19, Wellington, 2007) < www.lawcom.govt.nz>. See also New Zealand Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLC SP19, Wellington, 2008) <www.lawcom.govt.nz>.

29 "Website comment 'sux'" (19 December 2007) NewstalkZB Auckland <www.newstalkzb.co.nz>. Launched in 2005, Bebo is the largest social networking site in the UK, Ireland, and New Zealand, and is the third largest in the United States. See <www.crunchbase.com> (accessed 30 June 2009).

30 David Kravets "Student Who Created Facebook Group Critical of Teacher Sues High School Over Suspension" (9 December 2008) <www.blog.wired.com>.

suicide. The defendant was charged with, among other things, illegally accessing a protected computer.[31]

Marie Davis was a teenager from Christchurch. Her Bebo account was scrutinised for clues relating to her disappearance and eventual murder.[32] Although the cases of Megan and Marie involve more than a mere breach of information privacy, the crimes that were ultimately committed, at least in Megan's case, started with access to personal information.

It is no exaggeration, then, to state that privacy, defined as "control over access ... is necessary for human well-being."[33] And while there are those who may argue that persons putting information about themselves on the Internet contribute to their fate, does that mean that no further effort should be devoted to better protecting their privacy? What about those whose data is posted online without their consent?

While we may be prepared to live with some invasions of privacy, especially if that means aiding the fight against terrorism, just how much access to our personal information is too much? Anyone who has travelled internationally is accustomed to surrendering personal information about themselves such as passport details, but what about other details? For example, information about who paid for your ticket, your travel itinerary, the identity of the person walking you to the gate? Just how important is privacy post-9/11, and how much are we comfortable giving up to potentially stop terrorism, are questions the remainder of this paper is devoted to examining.

IV WHY WE SHOULD CONTINUE TO CARE ABOUT PRIVACY

Whether more comprehensive privacy safeguards would have prevented the occurrence of some of the events and crimes described above is impossible to know. But it is possible to predict that without privacy protections in place, these types of incursions will only increase.

As illustrated, information privacy regarding each other as individuals is important to our well-being. But it is also important in relation to our governments. Some would argue, even more so:

> In cases where there is a lack of accountability provisions and independent oversight, governments may pose the greater security risk.[34]

---

31 KTLA-TV Los Angeles "Judge Throws Out Conviction in Deadly MySpace Hoax" (2 July 2009) < www.ktla.com> (accessed 9 July 2009).

32 "Bebo Features at Marie Davis Murder Trial" (27 May 2009) <www.tvnz.co.nz> (accessed 30 June 2009). See also Catherine Woulfe "The Not-So-Private Life of Teens" *Sunday Star Times* (Auckland) (20 April 2008) at A-7. For another report on privacy implications for those using social networks, see the 2005 study on 4,000 college students using Facebook at <www.heinz.cmu.edu>.

33 Moore "Toward Informational Privacy Rights", above n 26, at 811.

34 Ibid, at 838.

To those thinking that a slight infraction of privacy, for example the surrender of an itinerary, is a small price to pay for a potential increase in security, see Parts IX and X below. But in the interim, consider the foreboding wisdom in Justice Brandeis' dissent in the 1928 case of *Olmstead v United States,*[35] a case in which the US Supreme Court held that the Fourth Amendment to the Constitution, while protecting a person, their papers and home, did not protect against tapping a public telephone line:[36]

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. *The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.*

If one accepts that the basic tenets of democracy are to enjoy "Life, Liberty and the pursuit of Happiness,"[37] then how would our enjoyment of these goals fare if, for example, the results of one of our most private democratic activities, voting, could be affected by accessing, collecting, disseminating or using personal information? What if the justification was to potentially increase our security? Would it be worth it, or would we be on the slippery slope away from democratic ideals?

Proceeding on the premise that information privacy is indeed essential not only to our well-being, but indeed to our fundamental democratic ideals, there must be rules regulating how we interact with each other and what our governments should and should not have access to. The question is how best to do so post-9/11, especially in the face of continuously advancing technology:[38]

> [M]ost of our privacy-related legal challenges lie at the intersection of a legal circumstance and a technological circumstance. The legal circumstance consists of the fact that several different types of law are involved in regulating privacy. Some laws ... protect particular places or sites, ... [o]ther laws protect not places but kinds of information....
>
> The technological circumstance consists of the fact that advancing technology has made the protective effects of present law uncertain, unpredictable, and incomplete.

---

35 *Katz v United States* (1967) 389 US 347. *Katz* expanded the reach of the Fourth Amendment to a person's reasonable expectation of privacy.

36 *Olmstead v United States* (1928) 277 US 438, 479, Brandeis J dissenting. See also Moore "Toward Informational Privacy Rights", above n 26, at 834 citing Justice Brandeis' dissent. (Emphasis added.) Later overruled by *Katz v United States.*

37 United States Declaration of Independence 1776 para 2.

38 US Supreme Court Justice Stephen Breyer *Active Liberty: Interpreting a Democratic Constitution* (Oxford University Press, New York, 2008) at 63-64, 66.

To assess the current state of the law on privacy in the West and how it intersects with today's technology, a review of post-9/11 laws is helpful. But to understand how we arrived at that intersection, and what some of the challenges may be in developing a unified approach to our security, we must first understand where we've been.

V PRIVACY – HOW HAS IT BEEN PROTECTED HISTORICALLY?

A United Kingdom – Cradle of Western Privacy Law

In the UK today, privacy cases arise in the context of preserving confidences in social relationships.[39] Cast as the law of confidence, not only does it preclude those in confidential relationships from disclosing private information, but it also precludes third parties from doing so.

This concept of the law of confidence was exported to former UK colonies, including Australia and New Zealand.[40] But another former colony, the United States, was to take a different path in the late 19th century, moving away from the concept of the preservation of confidences, and toward an inherent right to privacy encapsulated in law as the concept of "liberty".[41] Interestingly, both versions of privacy sprang in significant part from the same 1849 English case: *Prince Albert v Strange*.[42]

In *Prince Albert v Strange*, Vice-Chancellor Knight Bruce granted plaintiffs an injunction against (1) the exhibition, publication, copying, parting and disposing of 63 private drawings and etchings made by Prince Albert and Queen Victoria, and (2) the printing, publishing and selling of a descriptive catalogue of these etchings made by one of the defendants.[43]

The Lord Chancellor upheld the injunction against publication of the catalogue (the only issue on appeal) even though the catalogue was not compiled by the plaintiffs. Although a list of the etchings had not been enjoined from publication, the publication of a detailed description of the etchings was held to be tantamount to a publication of the contents of the etchings themselves and was therefore enjoined.[44]

---

39 Neil M Richards and Daniel J Solove "Privacy's Other Path: Recovering the Law of Confidentiality" (2007) 96 Georgetown Law Journal at 123.

40 New Zealand Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1*, above n 27, at 13, para 20 and 73.

41 James Q Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale Law Journal at 1151.

42 *Prince Albert v Strange* 41 ER 1171, 1 McN & G 2 (1849) EWHC Ch J20 (1849) 2 De Gex & Sim 652.

43 Ibid. For more information on the "Royal Etchings" see <www.donaldheald.com>.

44 Robert C Post "Rereading Warren and Brandeis: Privacy, Property, and Appropriation" (1990-1991) 41 Case Western Reserve Law Review at 647, 656-657.

In dicta in the underlying decision, Vice-Chancellor Knight Bruce speculated that the publication of a mere "list of ... papers" could also have been enjoined because "[i]t may also shew the bent and turn of the mind, the *feelings* and taste of the artist ...."[45] But this was not the court's ruling, nor was it true, since a list of the etchings was indeed published.

To understand how *Prince Albert* came to be interpreted differently in the US and how it was used to substantiate the view of privacy as "liberty," it helps to review the early privacy law of Germany and its focus on the "inviolate right of personality".[46]

B Germany and the Right of Personality[47]

In continental Europe the concept of privacy developed as a right to control one's public image, that is "dignity" where "[t]he prime enemy of ... privacy, according to [the] continental conception, is the media, which always threatens to broadcast unsavoury information about us in ways that endanger our public dignity."[48] In mid-1800s Germany and France, it was not uncommon for the courts to step in to protect an individual's dignity under what was to become known as "the right to one's image."[49] In practice, this resulted in the banned distribution of photographs portraying individuals on their deathbeds. Among the more famous were the cases of Otto von Bismarck (1815-1898), an influential German statesman,[50] Rachel (1821-1858) a well-known tragic actress,[51] and Soeur Rosalie (1786-1856), a nineteenth century Mother Teresa.[52]

By the 1870s, Germany's law of personality was taking shape. Considered "an amalgam of personal honor and artists' rights,"[53] it developed from the Roman law of insult and later combined with an expanded version of intellectual property rights to include control over one's work and

---

45 *Prince Albert v Strange*, above n 44, at 696-697. (Emphasis added.)

46 James Q Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty", above n 42, at 1180.

47 This paper reviews only the laws of the UK and Germany not because they are the only countries developing the concept of privacy at the time (France made significant contributions), but because their laws are most relevant to the development of the laws of those countries covered in this paper.

48 Whitman, above n 42, at 1161.

49 Ibid, at 1175-1176, 1185, 1201, 1206.

50 Ibid, at 1173-1175, 1185.

51 For more information on Rachel, see <www.VisWiki.com>.

52 For more information on Soeur Rosalie, see <www.VisWiki.com>. See also J M Rendu *The Life of Soeur Rosalie, of the Daughters of St. Vincent de Paul* (Burns and Lambert, London, 1858).

53 Whitman, above n 41, at 1185.

protection of the artist's reputation.[54] At its core, the law was intended to protect a person's dignity and enable a person to fully express their own unique self.

It was not long before Germany's law of personality found its way into US law.

C United States – Germany Meets the UK

In 1890, Samuel D Warren and Louis D Brandeis published their now famous article, "The Right to Privacy"[55] in the fourth edition of the Harvard Law Review.[56] This article was to change the course of American privacy jurisprudence.

In their article, the authors elaborated on the concept of "inviolate personality"[57] and the "right to be let alone."[58] Although these concepts continue to be associated with the writers to this day, both first appeared elsewhere.[59]

As set out above, the concept of inviolate personality harks back to late 19th century Germany, and the right to be let alone (as credited by the authors), was first espoused by Michigan Supreme Court Justice Thomas M Cooley[60] in his 1888 treatise on torts.[61]

In addition to citing the two concepts above, Warren and Brandeis discussed *Prince Albert v Strange*:[62]

> Although the courts have asserted that they rested their decisions on the narrow grounds of protection to property, yet there are recognitions of a more liberal doctrine. Thus in the case of Prince Albert v Strange, ... *the opinions both of the Vice-Chancellor and of the Lord Chancellor, on appeal, show a more or less clearly defined perception of a principle broader than those which were mainly discussed, and on which they both place their chief reliance.* Vice-Chancellor Knight Bruce [in] referr[ing] to publishing of ... possibly injurious disclosures as to private matters, [stated] that the courts would in a

---

54 Ibid.

55 Warren and Brandeis "The Right to Privacy," above n 24.

56 Louis Brandeis was to play a formative role in the Law Review's founding. For more information see Erwin N Griswold "The Harvard Law Review - Glimpses Of Its History As Seen By An Aficionado" (2004, The Harvard Law Review Association) <www.harvardlawreview.org>.

57 Warren and Brandeis "The Right to Privacy", above n 24, at 206.

58 Ibid.

59 Daniel J Solove, Marc Rotenberg, and Paul M Schwartz *Privacy, Information and Technology* (Aspen Publishers, New York, 2006) at 22-23.

60 For more information see the Thomas M Cooley Law School website <www.cooley.edu>.

61 Justice Thomas M Cooley *Cooley on Torts* (2nd ed, Callaghan, 1888) at 29. [p 195, Note 4 in the first edition.]

62 Warren and Brandeis "The Right to Privacy", above n 24, at 204-205. (Emphasis added).

> proper case prevent [their publishing]; yet it is difficult to perceive how, in such a case, any right of privacy, in the narrow sense, would be drawn in question, or why, if such a publication would be restrained when it threatened to expose the victim not merely to sarcasm, but to ruin, it should not equally be enjoined, if it threatened to embitter his life.
>
> ...
>
> These considerations lead to the conclusion that the *protection afforded* to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, *is merely an instance of the enforcement of the more general right of the individual to be let alone.*
>
> ...
>
> The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an *inviolate personality*.

What started out as the intimation of a right to protect an individual's feelings in *Prince Albert v Strange*[63] was to become the bedrock of the American right to privacy. Whereas England followed and developed the concept of protecting social relationships and the confidences inherent in them, Warren and Brandeis found support for the inherent right of individuals to choose when and how to divulge information about themselves by extrapolating dicta from *Prince Albert v Strange* and calling it "the right to privacy".

At the turn of the 19th century, England and the United States were not poles apart in their attempts to protect individuals' privacy. In fact, all of Europe and the United States were grappling with establishing a balance between an individual's entitlement to dignity and privacy on the one hand, and the freedom of the press on the other.

In Europe and the United States, where vindication of dignity did not play out in the courts, it was not uncommon for it to surface on a duelling ground. Imported from medieval Italy, the duel of honour continued until as late as until World War I in France and Germany. In the United States, the first duel was reported in 1621, one year after the Pilgrims landed.[64] Duels became less common after the Civil War of 1861-1865.[65]

---

63 *Prince Albert v Strange*, above n 42, at 696-697.

64 Whitman "The Two Western Cultures of Privacy: Dignity Versus Liberty", above n 41, at 1166-67, 1169, 1171, 1173-76. For the history of duelling in Europe and the US, see Douglas W Allen and Clyde G Reed "The Duel of Honor: Screening for Unobservable Social Capital" (2006) 8 American Law and Economics Review at 81-115.

65 Among the more famous duellists in the US during the 1800s were Andrew Jackson, future President of the United States (involved in an estimated 100 disputes or duels – <www.people.colgate.edu>), and Alexander

In addition to interpreting the *Prince Albert v Strange* case to suit their construct of an inherent right to privacy, Warren and Brandeis used the invasions of the press and technology to paint a bleak picture of a future without more explicit protections. By the time they wrote their famous article, Kodak had invented instantaneous photography with the snap camera (as mentioned above), and the press was increasingly invading individuals' privacy, just as it was in Europe:[66]

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'

Where copyright and breach of confidence had served to protect the expression and disclosure of one's art in England, Warren and Brandeis believed what was needed was a more expansive right to protect man's essence, his personality, his privacy. As quoted above, they argued that copyright was actually part of the principle of inviolate personality, which in turn was based on the more comprehensive right to privacy:[67]

> [N]o basis is discerned upon which the right to publication and reproduction of such so-called literary and artistic works can be rested, except the right to privacy, as part of the more general right to the immunity of the person, the right to one's personality.

Why did Warren and Brandeis' reading of *Prince Albert v Strange* take hold in the United States? One reason may be the resonance of this interpretation with the American concept of liberty.

In the United States today, the concept of privacy is mostly associated with liberty from government intrusion.[68] Its Constitution, and especially its Bill of Rights, reflects this inherent "us versus them" approach:

The First Amendment protects, among other things, the freedom of association (as interpreted by the Supreme Court[69]);

The Second Amendment enshrines the right to keep and bear arms;

The Third Amendment ensures protection from having to quarter soldiers in homes without consent or, in times of war, quartering must be in accordance with law;

Hamilton, Treasury Secretary under President George Washington who, on 11 July 1804, lost his life in a duel with US Vice President Aaron Burr (see <www.pbs.org>).

66 Warren and Brandeis "The Right to Privacy", above n 24, at 195.

67 Ibid, at 207.

68 Richards and Solove "Privacy's Other Path", above n 39, at 127; Robert C Post "Rereading Warren and Brandeis", above n 44, at 653; Robert C Post "Three Concepts of Privacy" (2001) 89 Georgetown Law Journal at 2087, 2096.

69 *NAACP v Alabama* (1958) 357 US at 449; *Boy Scouts of America v Dale* (2000) 530 US at 640.

The Fourth Amendment protects against unreasonable searches and seizures and prohibits the issuance of warrants without probable cause; and

The Fifth Amendment protects against, among other things, self-incrimination in criminal trials, and provides the right to due process before deprivation of life, liberty, or property.

Unlike the 1689 English Bill of Rights, which gives Parliament supremacy, and protects the rights of citizens as vested in Parliament vis-à-vis the Crown, exactly one century later the US Bill of Rights applies to citizens directly as against the federal government. The UK also has its Human Rights Act 1998, and approximately 130 Acts of Parliament that convey rights of a constitutional nature, including freedom of association and assembly, right to security and liberty, and prohibition of torture. In that respect, they have been compared to the US Constitution, but many of these rights are not as engrained as they are in the United States, and can more easily be amended. For example, in the UK the right to remain silent was significantly diminished in 1994 with the passage of the Criminal Justice and Public Order Act: adverse inferences can now be drawn from silence.[70]

Inherent distrust of government (manifest in its founding document) underlies the principles that govern the United States to this day. The right to be free from government intrusion dovetails neatly with the belief in an inherent right to privacy.[71] Although the right to privacy is not specifically set out in the Constitution, the courts have not struggled to find its roots there, even if only by inference.[72]

Set against this backdrop, it is not surprising that Warren and Brandeis' view of an inherent right to privacy found an eager audience willing to expand upon what seemed a natural right. After all, the groundwork for this "right" had been laid by the Constitution in the late 1700s, and developed by the judiciary starting as early as 1816,[73] decades before the Warren and Brandeis article. It was only a matter of time before Professor William Prosser, after reviewing decades of privacy cases, organised them into four distinct torts: 1) unreasonable intrusion upon seclusion; 2) appropriation of name or likeness; 3) unreasonable publicity given to private life; and 4) publicity that unreasonably

---

70 James Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism* (Ashgate Publishing, Ltd, Aldershot, Hampshire, 2007) at 52-53.

71 This right, however, is not absolute, especially in cases of First Amendment freedom of speech, which in many cases trumps an individual's right to privacy.

72 *NAACP v Alabama*, above n 69 (privacy in one's associations is a peripheral First Amendment right); *Griswold v Connecticut* (1965) 381 US at 479 (inference of zones of privacy in the First, Fourth, Fifth and Ninth Amendments); *Katz,* above n 35, at 347 (arbitrary government eavesdropping violated reasonable expectation of privacy, constituting an unreasonable search and seizure under the Fourth Amendment).

73 Susan P Stuart "Fun with Dick and Jane and *Lawrence:* A Primer on Education Privacy as Constitutional Liberty" (2004) 88 Marquette Law Review at 563, 605 citing *Ward v Bartlett* 1 New Hampshire 14 (1816) ("right of domestic privacy and security of habitation").

places the other in a false light in the public eye.[74] These torts were first published in his now famous *Prosser on Torts* in 1941, followed, inter alia, by his equally famous article, "Privacy"[75] and the privacy provisions in the *Restatement of Torts*.[76]

D Australasia – Following in Others' Footsteps or Independent Thinkers?

Like the United States, New Zealand and Australia inherited significant legal foundations from the UK. New Zealand (like the UK) did not develop a written Constitution. Australia (like the United States) did, albeit not until 1900.

As comparatively young countries, most of Australia's and New Zealand's laws are set forth in a number of relatively recent Acts. New Zealand's Constitution Act 1986 does not have the same constitutional force as that of the United States Constitution, (a New Zealand court cannot hold a law inherently unconstitutional under that Act).[77] But New Zealand does have a Bill of Rights Act similar to that of the United States with, inter alia, provisions against unreasonable government searches and seizures. By comparison, although there has been discussion in Australia about enacting a Bill of Rights since its Constitution was signed, it does not currently have one.[78]

Neither country has enacted legislation incorporating a right to privacy in a civil (as opposed to a criminal) context. The New Zealand Law Commission has yet to reach a conclusion on whether stand-alone breach of privacy legislation should be enacted.[79] By comparison, in 2007, the Australian Law Reform Commission recommended enacting breach of privacy legislation, but at the time of writing this has yet to occur.[80] Both have Privacy Acts that protect the collection, storage, access to and disclosure of personal information. (See Section VII below.)

---

74 American Law Institute *Restatement of Torts* (2nd ed, St Paul, 1977) ss 652A(2)(a)-(d).

75 William L Prosser "Privacy" (1960) 48 California Law Review at 383.

76 American Law Institute *Restatement of Torts,* above n 74. See also Christopher J Robinette "The Prosser Notebook: Classroom as Biography and Intellectual History" (January 20, 2009) Widener Law School Legal Studies Research Paper No 09-04 Social Science Research Network <www.ssrn.com>.

77 For other New Zealand Acts with constitutional overtones see: the Treaty of Waitangi (and subsequent Acts regarding the Treaty), Bill of Rights Act 1990, Electoral Act 1993, Human Rights Act 1993, and Judicature Act 1908. See also Grant Morris *Law Alive: The New Zealand Legal System in Context* (Oxford University Press, Melbourne, 2009) at 72.

78 The Hon Mr Justice David Malcolm AC "Does Australia Need a Bill of Rights?" (Speech September 1998) 5 Murdoch University Electronic Journal of Law 3 <www.murdoch.edu.au>.

79 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3* (NZLC IP14, Wellington, 2009) at 173 <www.lawcom.govt.nz>.

80 In addition to the federal Australian Law Reform Commission review, the states of Victoria and New South Wales are also engaged in their own review. The NSW review is largely concerned with the tort of privacy <www.privacy.org.nz>.

As far as a common law right to privacy, there have been advances. In New Zealand, there has been a trend towards a selective adoption of the privacy torts in US case law, namely Prosser's tort of unreasonable publicity given to private life.[81]

In the opinion of the New Zealand Law Commission, however:[82] "[T]he tort of invasion of privacy is in its infancy. It remains liable to be changed, or even reversed, by the Supreme Court." But more recently, the New Zealand Privacy Commissioner came out in support of not just one but two privacy torts: (1) Invasion of privacy by publicity given to private facts and (2) intrusion into personal or private space.[83]

As far as establishing a common law right to privacy in Australia, courts in Queensland and Victoria have recognised a right to privacy in and of itself.[84] It remains to be seen whether this will become a federal and not just a state-by-state trend in Australia.

With this historical background on how different countries initially treated privacy, we can proceed with more in-depth analysis of 20th century advances. The post-World War II era saw the arrival of significant instruments and recommendations in the West, many of them relating to personal data privacy. While one of the most important instruments was enacted in Europe, its effect would be felt much more widely. Ultimately, it would have a pervasive effect on how the West would advance, both legally and culturally, in the post-9/11 world. Following is a comparison of some of the most noteworthy instruments between the post-World War II era and immediately

---

81 American Law Institute *Restatement of Torts,* above n 74, ss 652A(2)(c). See *Hosking v Runting* [2005] 1 NZLR 1 (CA). Although the Court denied injunctive relief to stop publication of photos of a television personality's twin 18-month-old daughters (photographed while in public), it held (in a 3-2 decision) that an invasion of privacy tort (public disclosure of private facts) did exist in New Zealand. For cases leading up to the decision in this case, see *Tucker v News Media Ownership Ltd* [1986] 2 NZLR at 716, *Bradley v Wingnut Films Ltd* [1993] 1 NZLR at 415 and *P v D* [2000] 2 NZLR at 591. For viewpoints on the impact of this decision and where it could lead, see Katrine Evans "Hosking v Runting Balancing Rights in a Privacy Tort" [2004] PLPR at 28. See also the New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy Stage 3*, above n 79, at 155 <www.lawcom.govt.nz >. For subsequent application of *Hosking* see *Mafart and Prieur v Television New Zealand Ltd* [2006] 3 NZLR at 534 (CA), *Andrews v Television New Zealand Ltd* (15 December 2006) HC AK CIV 2004-404-3536, Allan J, and *Television New Zealand Ltd v Rogers* [2008] 2 NZLR at 277.

82 New Zealand Law Commission *Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy Stage 3*, above n 79, at 155 <www.lawcom.govt.nz>.

83 Office of the Privacy Commissioner "Gaps To Be Plugged – Privacy Commissioner on Privacy Tort, Surveillance and Intrusion" (9 July 2009) Media Release <www.privacy.org.nz>.

84 The Queensland Court held that the plaintiff had suffered a breach of privacy in the form of intrusion upon seclusion, after being stalked by a former lover (*Grosse v Purvis* (2003) Australian Torts Reports 81-706.) The Victoria Court found a breach of the right to privacy in a case involving disclosure of personal information, including the name of the victim and facts relating to rape, on the television news (*Doe v Australian Broadcasting Corporation* [2007] VCC 281).

before 11 September, that set the stage for the way the West views and treats personal data privacy today.

VI EARLY DATA PROTECTION INSTRUMENTS

A Post World War II

In the aftermath of the Second World War, efforts were made to ensure that similar atrocities did not occur again. Leading the way was the United Nations.

On 10 December 1948, the UN General Assembly adopted, without dissent, the non-binding Universal Declaration of Human Rights (UDHR), Article 12 of which includes significant protections for privacy:[85]

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence*, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

In 1949 the Treaty of London established the Council of Europe (CoE) to promote more unity between members by protecting human rights, democracy and the rule of law. Among the ratified CoE treaties regarding privacy, was the Convention for the Protection of Human Rights and Fundamental Freedoms, also referred to as the European Convention on Human Rights (ECHR),[86] which entered into force in 1953.

Taking into consideration the goals set out in article 12 of the UDHR, the ECHR's article 8 incorporates many of the same protections, but makes a distinction between protecting "privacy" and protecting one's "private life":[87]

> Everyone has the right to respect for his private and family life, his home and his correspondence.

All 47 member states have since ratified the Convention.[88]

---

85 Universal Declaration of Human Rights (UDHR) (10 December 1948) GA Res 217A (III), UN Doc A/810, art 12, at 71. (Emphasis added.)

86 Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950) ETS 005 < www.conventions.coe.int>. *Note:* CoE conventions that opened for signature through 2003 were part of the European Treaty Series (ETS 001 – 193); from 2004, they were part of the Council of Europe Treaty Series (CETS 194 -).

87 UDHR, art 8, above n 85. (Emphasis added.)

88 With the Human Rights Act 1998, which came into force in 2000, the UK incorporated the ECHR into English law. See James Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, above n 70, at 52.

The Council of Europe was not the only new European entity to come into existence in the post-war years. Two years after the CoE, the European Coal and Steel Community (ECSC) was created by France, Germany, Italy, and the Benelux[89] countries.

In 1957, these same six countries went on to sign the two Treaties of Rome. One of the two treaties created a common market, the European Economic Community (EEC). (This Treaty is now known as the European Community Treaty or EC Treaty.) The other created the European Atomic Energy Community (Euratom) to co-ordinate research into the peaceful use of nuclear energy.

In 1965, these three European entities (ECSC, EEC and Euratom), while still retaining independent legal status, merged their individual legislative, judicial and executive branches into a single Council and single Commission. Under the Merger Treaty,[90] they became collectively known as the European Communities.

While the treaties that were entered into after World War II made references to privacy, private life, or correspondence, protection for other personal information did not occur until a couple of decades later. It would take the rise of computer technology and concerns about the increasing prevalence of databases of personal information to bring about future instruments and recommendations.

B The 1970s

In 1966 the United Nations' Office of the High Commissioner for Human Rights opened the International Covenant on Civil and Political Rights (ICCPR) for signature. It entered into force exactly 10 years later. One of the protections within the ICCPR is the right to privacy contained in article 17. Except for the insertion of "unlawful" twice in paragraph 1, it is identical to article 12 of the UN UDHR, which is not surprising given that it is based on the UN Declaration:[91]

> 1. No one shall be subjected to arbitrary or *unlawful* interference with his *privacy, family, home or correspondence,* nor to *unlawful* attacks on his honour and reputation.

The UK, New Zealand, Australia, and the United States all signed and ratified the treaty – in that order. However, the United States' five reservations, five understandings and four declarations, have lead to substantial criticism that its accession to the treaty is in name only:[92] in addition to

---

89 Belgium, Netherlands and Luxembourg.

90 Also known as the Treaty of Brussels.

91 International Covenant on Civil and Political Rights (19 December 1966) 999 UNTS 171, art 17. (Emphasis added.) It was signed by the UK in 1976, New Zealand in 1979, Australia in 1980, and the United States in 1992.

92 US reservations, declarations, and understandings, International Covenant on Civil and Political Rights (daily ed, 2 April 1992) 138 Congressional Record s 4781-01.

declaring that Articles 1- 27 of the Covenant are not self-executing vis-à-vis the US, many of the other derogations involve a commitment to abide by its own Constitution, which in some cases conflicts with the ICCPR.[93]

But the 1970s did not just see reiteration of pre-existing privacy protections in new laws. The advent of modern computing and increased international interdependence and co-operation brought with them additional concerns for privacy and, more specifically, information privacy.[94] Just as UK and US views on privacy were shared in the mid-1800s, so they overlapped again over a century later in establishing principles protecting information privacy. This convergence of paths in the 1970s, however, would be short-lived.

One of the first co-operative efforts between European and American legal scholars on privacy (there would be more) led to the creation of the Fair Information Practice Principles (FIPPs). Over time they have been categorised as anywhere between five and eight principles. Today, they comprise the following essential protections:[95]

- the Collection Limitation Principle: personal data collection should be limited and lawful;
- the Purpose/Use Limitation Principle: the purpose of data collection should be disclosed and data should not be used for other purposes without consent;
- the Transparency Principle: data subjects should be informed about data privacy policies;
- the Data Quality Principle: data should be accurate, complete and current;

---

93 For example, article 6, paragraph 5 of the ICCPR, precludes execution of both pregnant women and children under the age 18. In the US, 38 states still enforce the death penalty and, as of 1976 when the US Supreme Court reinstated it, 21 men who were underage at the time of the crime, have been put to death. Moreover, the US has neither signed Optional Protocols 1 or 2 (regarding administration by the Human Rights Committee and abolition of the death penalty, respectively), nor amended its national laws to comply with the Convention. Ibid. See also Human & Constitutional Rights *Is Capital Punishment in the United States Illegal Under International Law?* (13 March 2003, updated 15 May, 2007) <www.hrcr.org>. For more information on the US death penalty and the effect it is having on extradition post 9/11, see Nora V Demleitner "The Death Penalty in the United States: Following the European Lead?" (2002) 81 Oregon Law Review at 131.

94 See Westin *Privacy and Freedom*, above n 27; Dr Alan F Westin and Michael A Baker *Databanks in a Free Society; Computers, Record-keeping and Privacy* (Crown Publishing Group, New York, 1972).

95 For a summary of the Fair Information Practice Principles, see Abraham L. Newman *Protectors of Privacy* (Cornell University Press, New York, 2008) at 26. For more detailed information on the principles and their origin, see Fred H Cate *The Failure of Fair Information Practice Principles* in Jane K Winn (ed) *Consumer Protection in the Age of the Information Economy* (Ashgate Publishing Limited, Aldershot, Hampshire, 2006). For the US view of FIPPs, see the US Federal Trade Commission website at <www.ftc.gov> and Hugo Teufel III, Chief Privacy Officer of the Department of Homeland Security, Privacy Policy Guidance Memorandum of 29 December 2008 at <www.dhs.gov>.

- the Access and Correction Principle: data subjects may request information about held data and challenge incorrect data;
- the Security Principle: stored data must be kept secure; and
- the Accountability Principle: organisations must be held accountable.

The first countries to implement legislation incorporating the FIPPs regarding information privacy were Sweden and the United States.[96] Arguably as influential as the Warren and Brandeis article almost a century earlier, FIPPs laid the groundwork for future international co-operation on the protection of personal data privacy. Over the next few years there was not only an increase in bilateral and multilateral efforts to protect personal data privacy, but the implementation of laws that were increasingly more explicit.

C The 1980s

Continuing advances in computer processing in the 1980s were creating concerns about privacy similar to those raised by Kodak's instant camera one century earlier:[97]

> The development of automatic data processing ... has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries ... to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

With these words in 1980, the Organisation for Economic Co-Operation and Development (OECD) prefaced its non-binding Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Like other post-WWII entities, the OECD came into existence in 1948 with the goals of co-ordinating economic policies and liberalising trade in Europe. Although its goals remain economic- and trade-focused, it has since expanded its membership to 30 states, including countries outside Europe: Canada, the United States, Mexico, Japan, Australia, and New Zealand.[98] This diversity in member states, with their equally diverse privacy systems, has challenged the development of privacy guidelines that all could agree to.

---

96 In 1973, Sweden enacted the Data Act regarding processing of personal data. One year later it enacted the Instrument of Government Act, which provides for individual privacy protection. In 1974, the US enacted the Privacy Act to protect records held by US government agencies.

97 Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 <www.oecd.org>.

98 Rosemary Jay *Data Protection Law and Practice* (3rd ed, Sweet & Maxwell Limited, London, 2007) at 7.

Europe's comprehensive privacy law systems contrasted dramatically with the United States' more limited system.[99] Comprehensive systems actively regulate information privacy both in the public and in the private spheres, and incorporate specific data protection for anyone within its borders regardless of nationality.

The limited system in the United States regulates information privacy primarily in the public sphere. While those following the comprehensive approach create regulatory government agencies (Information Officers or Privacy Commissioners), the United States does not. Instead, the United States engages in piecemeal legislation: a smattering of federal statutes governing certain sectors of the economy, and many individual state laws or authorities,[100] leaving privacy primarily to the regulation of the market – or the legal system in the event of a breach.[101] Moreover, only US citizens and legally resident aliens are protected under its Privacy Act of 1974**.** (See below.)

Despite the challenge in finding common ground among the vastly different member states' privacy systems, the OECD succeeded by taking the FIPPs, expanding on them, and creating eight privacy principles:[102]

- the Collection Limitation Principle
- the Data Quality Principle
- the Purpose Specification Principle
- the Use Limitation Principle
- the Security Safeguards Principle
- the Openness Principle
- the Individual Participation Principle
- the Accountability Principle

---

99 While there are other countries such as Singapore, China and Malaysia with limited systems of privacy protection, for the purposes of this paper, discussion on systems of limited privacy protection will be restricted to the United States.

100 For example, art 1, s 1 of the California Constitution recognises a right to pursue and obtain "safety, happiness and privacy." In 2001, California opened its Office of Privacy Protection, becoming the first state to have an agency tasked with assisting consumers regarding various privacy-related issues, identity theft in particular. See the California Office of Information Security and Privacy Protection website at < www.oispp.ca.gov>.

101 Newman *Protectors of Privacy*, above n 95.

102 OECD Guidelines, above n 97, paras 7-14.

(For a chart comparing the differences between various international privacy instruments, see Table 1 below.)

Although the OECD Guidelines added more protections than they took away, they nevertheless refrained from making the security and accountability principles mandatory as they had been under FIPPs. And while there is a suggestion under the OECD Guidelines that data be destroyed or made anonymous once it no longer serves a purpose,[103] there is no limit on how long data should be stored, leaving it to individual countries to implement national legislation in that regard.[104] There appears to be a presumption that if data continues to serve a purpose it can be kept indefinitely, similar to FIPPs. Also like FIPPs, the Guidelines apply to both public and private sectors and to automated and non-automated processing of data.[105]

In recognition of the differences between limited and comprehensive systems, there was no requirement in the Guidelines for specific supervisory authorities to be set up to ensure compliance. Rather, reference was made to a variety of possibilities, including supervisory authorities, existing public authorities or courts.[106]

Similarly with regard to sensitive data (for example, data regarding race, religious beliefs, or criminal records), the Guidelines did not propose different treatment, but allowed for possibilities. This choice enabled some member nations possessing limited systems of privacy protection (namely the United States) to sign up to the Guidelines.[107]

During the time that the OECD was working on its Guidelines, the CoE was in the process of enacting its own Convention. In 1981, the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Convention 108) became the "first legally binding international instrument in the data protection field."[108] It entered into force on 1 October 1985. At the time of writing, 41 out of 47 member states have signed and ratified it.[109]

---

103 Ibid, above n 97, para 54.

104 In the first paragraph of the OECD Guidelines there is a reference to a number of member countries enacting or introducing legislation to prevent "unlawful storage of personal data, [and] the storage of inaccurate personal data … .", above n 98.

105 Ibid, paras 2 and 3(c).

106 Ibid, paras 19(d), 69 and 70.

107 Ibid, paras 19(a), 50, 51 and 67.

108 Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (28 January 1981) ETS 108 (Convention 108) <www.conventions.coe.int>.

109 For a list of countries ratifying Convention 108, see <www.conventions.coe.int>. Countries that have signed but not ratified Convention 108 are: Russia, Turkey, Ukraine. Countries that have not signed are: Azerbaijan, Armenia, and San Marino.

Its purpose was "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his *right to privacy*, with regard to automatic processing of personal data relating to him... ."[110] (Emphasis added.) In some states its provisions are self-executing, although the Convention was not designed this way. In others, national laws are implemented incorporating its core principles.[111] Some states extend the principles only to natural persons while others extend them to legal persons as well.[112]

Convention 108 includes:[113]

- the Collection Limitation Principle (article 5a);
- the Purpose Specification Principle (articles 5b and 5c);
- the Use Limitation Principle (article 5b);
- the Data Quality Principle (article 5d);
- the Preservation Limitation Principle (article 5e);
- the Data Security Principle (article 7); and
- the Access and Correction Principle (articles 8a-d).

(For more detail, see chart at Table 1 below.)

Like the OECD Guidelines, Convention 108 applies to both public and private sectors, and automated and non-automated data.[114] The Convention is open to any nation (upon a unanimous vote), not only members of the Council of Europe. At the time of writing, no other non-CoE country has adopted it.

Unlike the OECD Guidelines, Convention 108 offers data subjects protections with more bite. While many OECD Guidelines were couched in terms of what the data controller "should" do, the Convention tells the controller what they "shall" do. Some of these mandatory provisions hark back to FIPPs (for example, the mandatory security provision). Considering the non-binding nature of the

---

110 Convention 108, above n 108, art 1.

111 Jay *Data Protection Law and Practice*, above n 98, at 9. See also Convention 108 Explanatory Report, Chapter II, Article 4, para 38 <www.conventions.coe.int>.

112 See Convention 108 Explanatory Report, National Legislation, above n 111, para 7.

113 Most relevant principles are listed under the Data Quality provisions of art 5. Descriptive principle titles are used for convenience only. See Convention 108, above n 109.

114 Convention 108, above n 108, art 3. Amendments to Convention 108 in June1999 extended the reach of the convention to non-automated data. See also Jay *Data Protection Law and Practice*, above n 98, at 10.

OECD Guidelines compared to the binding nature of the Convention, this was an historic achievement.

Other differences are the Convention's Use Limitation and Preservation Limitation principles. Unlike the OECD Guidelines, under the Convention there are no exceptions for consent or authorisation by law for data to be used for incompatible purposes, and there is a limit for the preservation of data. And for the first time, automatic processing of special categories of data, ie "personal data revealing racial origin, political opinions or religious or other beliefs ... health or sexual life ... [and] criminal convictions" is now precluded without appropriate domestic law safeguards.[115] No longer is there discretion (as under the OECD Guidelines) for states to determine for themselves what is or is not sensitive data.

Instruments and recommendations enacted in the 1980s reflected a growing urgency to protect the way personal data was being collected, used and stored. The EU would soon add to these efforts by implementing an instrument that would ultimately affect the way the West deals with the processing of personal data (and each other) to this day. The privacy system differences that had been simmering in the background, although softened by the OECD Guidelines,[116] were about to come to a head.

VII DATA PROTECTION INSTRUMENTS TODAY

A The United Nations' Contribution

On 14 December 1990, via Resolution 45/95, the UN General Assembly adopted the Guidelines for the Regulation of Computerized Personal Data Files. Comprising ten principles, they largely mirror the principles set out in earlier privacy protection law, with some significant new additions. The UN Guidelines, however, are non-binding and apply only to governmental international organisations.

The UN Guidelines include:[117]

- the Principle of Lawfulness and Fairness (article 1);
- the Principle of Accuracy (article 2);
- the Principle of Purpose Specification (article 3);

---

115 Convention 108, above n 108, art 6.

116 In 1985, out of concern for trans-border policy issues propelled by rapid computer technology development, the OECD member states adopted a declaration on Trans-Border Data Flows <www.oecd.org>. And in 2007 the OECD Council adopted a recommendation on "Cross-border Co-operation in the Enforcement of Laws Protecting Privacy" <www.oecd.org>.

117 United Nations Guidelines for the Regulation of Computerized Personal Data Files (14 December 1990) adopted by Resolution GA Res 45/95 <www.unhcr.org>.

- the Principle of Interested-person Access (article 4);
- the Principle of Non-discrimination (article 5);
- the Principle of Security (article 7);
- Supervision and Standards (article 8);
- Transborder Data Flows (article 9); and
- Field of Application (article 10).

(For more detail, see chart at Table 1 below.)

The UN's Principle of Non-discrimination *(A5)* is similar to Convention 108 article 6 dealing with sensitive types of information: data that is "likely to give rise to unlawful or arbitrary discrimination ... should not be compiled."[118]

Among the differences between the UN Guidelines and its closest predecessor, Convention 108, the UN Guidelines are not mandatory with reference to fair and lawful data collection, specific purpose designation, compatible use, or even data security, but revert to the earlier standard of the OECD Guidelines with "should".[119]

The UN Guidelines, however, did trailblaze in a few new areas. The active duty to conduct regular checks on the accuracy of the data is unique as is the duty to have data corrected or deleted at the data controller's expense.[120] Also unique to the Guidelines (at least at the time of their drafting in 1990) was the provision calling for independent supervising authorities. And for the first time, the Guidelines raised the possibility of criminal remedies for the violation of any national law incorporating the UN Guidelines' principles.[121] None of the earlier conventions or guidelines had these provisions. The UN Guidelines also became the second international instrument to consider the issue of transborder data flows after the OECD Guidelines.[122] The EU and CoE would soon follow suit with more specific transborder data flow instruments.

---

118 Ibid, principle A5.

119 Ibid, principles A1 and A2. See also OECD Guidelines, above n 97: Collection Limitation Principle (para 7), Purpose Specification Principle (para 9), Use Limitation Principle (para 10), and Security Safeguards Principle (para 11).

120 UN Guidelines, above n 117, principles A2 and A4.

121 Ibid, principle A8.

122 OECD Guidelines, above n 97, paras 15-18.

B European Union Sets the Standard

1 EU Data Protection Directive

In 1992, the Treaty of European Union (TEU) was signed.[123] In addition to advancing economic goals, including the creation of a unified currency, the TEU's agenda included the advancement of social and political agendas by institutionalising co-operation. To accomplish the Treaty's goals, EU members ceded part of their sovereignty, enabling EU institutions to adopt regulations, directives and decisions, all of which would take precedence over members' national laws.[124]

The EU has a three-pillar policy structure:

(I) The European Community is concerned with economic, social and environmental policies. The EC governs how the member states share sovereignty through community institutions. More recently, the areas of external border control, asylum, illegal immigration, visas and judicial co-operation in civil matters have been moved from the third pillar to this pillar.[125] These areas of asylum, illegal immigration, and visas/judicial co-operation, together with remaining third pillar areas, are collectively referred to as the Area of Freedom, Security and Justice (AFSJ) (replacing the former Justice and Home Affairs (JHA));

(II) Common foreign and security policy (CFSP), which allows Member States to take joint action in matters of foreign policy; and

(III) Police and judicial co-operation in criminal matters (PJCC).

Under the first pillar, legislation affecting the community is enacted via the "Community process," ie, the Commission submits a proposal, which the Council and the European Parliament then adopt. The Council's decision is arrived at by a qualified majority vote.

Although the first pillar operates supranationally, under pillars two and three member states co-operate intergovernmentally, retaining full sovereignty. There is no co-decision procedure. Parliament may only advise the Council, and there must be unanimity in the Council. This unanimity rule has resulted in actions passing on a lowest common denominator basis, generating significant criticism of the system.[126] Moreover, under pillar two the European Court of Justice, the

---

123 Treaty on European Union (7 February 1992) Official Journal C 191 of 29.7.1992. Also know as the Treaty of Maastricht.

124 Bulgaria and Romania joined in 2007. Croatia and Turkey have also made applications to join, and the former Yugoslav Republic of Macedonia's application has been formally accepted. Future additions are expected to include Bosnia & Herzegovina, Serbia, Montenegro and Albania. At the time of writing, the EU has 27 members.

125 See the Treaty of Amsterdam (2 October 1997) EC Treaty 97/286/EC <www.eurotreaties.com>.

126 Alfonso Scirocco "The Lisbon Treaty and the Protection of Personal Data in the European Union" (February 2008) <www.dataprotectionreview.eu>.

highest-ranking court enforcing EU law, has no role whatsoever. Under this pillar structure, one of the most substantial personal data privacy instruments of the twentieth century was about to be born.

In 1995, information privacy law turned a critical corner with the EU Data Protection Directive (EU Directive).[127] Labelled the de facto international model,[128] it was published five years after its initial introduction, and became effective on 25 October 1998.

After Convention 108 entered into force in 1985, many states lagged behind in enacting legislation, and even when they did, there were significant discrepancies between different member states' laws. By virtue of its mandatory nature, the EU Directive had the ability to harmonise the various states' laws and create independent mechanisms to ensure compliance.[129] Based on the 1980 OECD Guidelines, the EU Directive's opening recitals incorporate article 8 of the European Convention on Human Rights[130] (protection of privacy in personal and family life, home and correspondence) and Convention 108 by name,[131] and make clear that the Directive is not to circumscribe those rights, but to "amplify"[132] them. One example of that amplification is the fact that the Directive applies not only to data controllers located in the EU, but also to those whose data processing equipment is located inside the EU.[133]

Like its predecessors, the Directive was enacted with dual goals: to protect the "right to privacy with respect to the processing of personal data",[134] and to enable the "free flow of personal data between Member States" under the EU's now common and unified market.[135]

The Directive's main principles regarding the collection and processing of personal data are set out in articles 6 and 7.

The Directive defines "personal data" as "any information relating to an identified or identifiable natural person" such as an identification number or specific "physical, physiological, mental, economic, cultural or social identity," characteristics[136] (for example, address, bank statements, and

---

127 European Union Data Protection Directive (EU Directive) (24 October 1995) 95/46/EC.

128 Newman *Protectors of Privacy,* above n 95.

129 Diane Rowland, Elizabeth Macdonald *Information Technology Law* (3rd ed, Routledge-Cavendish, Milton Park, UK, 2005) at 322.

130 EU Directive, above n 127, recital 10.

131 Ibid, recital 11.

132 Ibid.

133 <www.techtarget.com>.

134 EU Directive, above n 127, art 1 para 1.

135 Ibid, art 1, para 2.

136 EU Directive, above n 127, art 2(a).

credit card numbers).[137] A "data controller" is anyone directing the data processing, and a "processor" is anyone doing the processing for the controller.[138] Under the Directive, "Member States *shall* provide that personal data *must* be":

- "Processed fairly and lawfully" (Collection Limitation Principle (article 6 paragraph 1(a));
- "Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Although *additional processing for "historical, statistical or scientific purposes"* is not considered an incompatible purpose. Data may only be processed with **"***unambiguous***"** consent or meet specific exception and processing must be **"***necessary***."** (Purpose/Use Specification Principle (articles 6.1(b) & 7));
- "Adequate, relevant and not excessive … ." (Use Limitation Principle (article 6 paragraph 1(c));
- "Accurate and, where necessary kept up to date; …" Inaccurate or incomplete data *must* be "erased or rectified" where it is reasonable to do so. *Third parties must be notified of changes and corrections unless "impossible or involves a disproportionate effort.***"** (Data Quality/Access/Correction Principles (article 6 paragraphs 1(d) & 12)); and
- "Kept … for no longer than is necessary …" *Safeguards shall be enacted where data is "stored for longer periods for historical, statistical or scientific use."* (Preservation Limitation Principle (article 6 paragraph 1(e)).

(See chart at Table 1 below for further comparison with earlier treaties and principles.)

Significant differences between the Directive and pre-existing privacy principles include the addition of the words "unambiguous" to the level of consent required, and "necessary" to the act of processing. Before the Directive, it was not uncommon for data controllers to presume that consent had been given unless an objection had been received, and that processing was justifiable if only to accommodate the controllers.[139]

Other variations from pre-existing privacy instruments include the Directive's explicit provision for further processing and storage of historical, statistical or scientific data,[140] although FIPPs[141] and the UN Guidelines[142] did provide for obtaining consent to use data for purposes other than

---

137 <www.techtarget.com>, above n 133.

138 EU Directive, above n 127, arts 2(d), (e). (Emphasis added: the amplification of principles over those in earlier treaties is in italics).

139 Rowland and Macdonald *Information Technology Law*, above n 129, at 328.

140 EU Directive, above n 127, arts 6.1(b) and 6.1(e).

141 Fair Information Practice Principles (FIPPs) Use Limitation Principle, above n 95.

142 UN Guidelines, above n 117, principle A3.

those originally stated. And the OECD Guidelines[143] provided for consent in the event of non-compatible use.

Like the UN Guidelines[144] and Convention 108[145] (and less like the OECD Guidelines[146] and FIPPs[147]), the EU Directive also adopted a mandatory stance on the accuracy of data.[148] Security was also made mandatory[149] in alignment with Convention 108[150] and the original FIPPs.[151] Another amplification of rights under the Directive was the requirement that processors now have the same level of security as data controllers,[152] and data subjects now had a vast array of remedies, including the availability of sanctions for infringement of the Directive's provisions.[153]

Overall, data subjects' protections were more comprehensive than they had been. They now had more assurances of security, accuracy and access to remedies should anything go wrong. And while private citizens were not able to sue other citizens (the Directive does not have direct effect "horizontally"), they could sue their government "vertically" if it failed to properly implement the Directive.[154]

Most international instruments regulating data privacy protection up to this point have exceptions for national security, with the exception of FIPPS, which makes no reference to national security one way or the other. The EU Directive not only has exceptions for national security, it is unique in explicitly applying only to pillar one activities. What this means is that pillar two issues regarding national security and pillar three issues regarding police and criminal justice matters are completely outside its scope. The effect of this limited scope will have overriding implications in subsequent data protection negotiations between the EU and United States in the years to come. While Convention 108 also has exceptions regarding national security, unlike the Directive it does

---

143 OECD Guidelines, above n 97, para 10.

144 UN Guidelines, above n 117, principle A2.

145 Convention 108, above n 108, art 5(d).

146 OECD Guidelines, above n 97, para 8.

147 FIPPs Data Quality Principle, above n 95.

148 EU Directive, above n 127, art 6 para 1(d).

149 EU Directive, above n 127, arts 6.1(e) and 17.

150 Convention 108, above n 109, art 7.

151 FIPPs Security Principle, above n 95.

152 EU Directive above n 127, art 17.

153 EU Directive, above n 127, arts 6.1(d), 10, 11, 12, 14, and 22-24. For more detail on remedies, see Table 1.

154 Paul Craig and Gráinne de Búrca *EU Law: Text, Cases and Materials* (4th ed, Oxford University Press, Oxford, 2007) at 284.

apply to pillar three issues. For those 41 out of 47 countries that have signed and ratified Convention 108, it provides for personal data privacy regulation at least in the area of police and criminal justice matters. (See Table 1 for a comparison of national security exceptions in other international data privacy instruments.)

Under article 28, the Directive became the first binding international privacy instrument to establish independent supervisory authorities to monitor compliance. Article 29 provided for the establishment of an independent advisory group called, not surprisingly, the "Article 29 Working Party." Comprising representatives of the supervisory authorities of each member state, the Working Party's mandate was to consider and report on a variety of issues impacting data privacy.[155] The Working Party's opinions are not binding, but they nevertheless carry significant weight: at least one judge has referred to them, and multinational corporations have implemented changes in accordance with them.[156] They were soon to play a role in the issue of transborder data flows.

For the first time in the history of personal data privacy legislation, the EU Directive enacted provisions relating to transborder data flows not just between member states, but between member states and countries outside the Union:[157]

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an *adequate level of protection*….

As intimated above, although the Directive only binds EU member states, its reach is broader than might at first seem. Its impact was soon to be felt in non-EU states. Limited and comprehensive privacy systems were about to collide under this new law.

2 EU Charter of Fundamental Rights

With the signing of the European Union Charter of Fundamental Rights (Charter) on 7 December 2000, personal data privacy made great strides. For the first time in EU history, the Charter encapsulated in one document a panoply of civil, political, economic and social rights, including the right to protection of personal data.[158] While the Charter is not yet legally binding, it

---

155 The Article 29 Working Party's mandate is further elucidated in the EU Directive, above n 127 art 30. See also arts 31-33 regarding the roles of the Commission and the Committee in relation to the Working Party.

156 Abraham L Newman *Regulating Personal Data in the Global Economy*, above n 95, at 95, 118-120 citing the Union of Industrial and Employers' Confederations of Europe *Implementation of Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data of 24 October 1995,* Brussels, UNICE 2002, at 1-10.

157 EU Directive, above n 127, art 25 para 1. (Emphasis added.)

158 European Union Charter of Fundamental Rights 2000/C 364/01 <www.europarl.europa.eu>.

was written as though it were. It is expected to become legally binding once the 2007 Treaty of Lisbon (discussed below) enters into force sometime in 2009 or 2010.[159]

Article 7 of the Charter corresponds to ECHR article 8's right to private and family life, home and communications.[160] Article 8 paragraph 1 of the Charter protecting personal data, however, is new: "Everyone has the right to the protection of personal data concerning him or her." While many EU states have a constitutional history of respect for personal data protection, for the most part EU member states' constitutions do not incorporate an explicit data protection right (with the exception of the constitutions of Portugal, Spain and Austria).[161]

The rest of article 8 summarises the basic elements of the various iterations of former data privacy legislation in calling for fair processing of personal data for specified purposes with consent or as authorised by law, and gives the data subject the right to access and correct the data. And like the EU Directive, compliance is to be monitored by an independent authority.[162]

3 Treaty of Lisbon

The Treaty of Lisbon (also known as the Reform Treaty), was signed on 13 December 2007, and amends pre-existing EU treaties. It took the place of the EU's attempt to create an EU Constitution in 2004, which failed to enter into force when Dutch and French citizens voted against it. To enter into force it must be ratified by all 27 member states. Its goals are to reform the TEU and EC Treaty,[163] and create a more efficient, transparent, coherent, and democratic process.

Some of the changes to the TEU and EC treaties included in the Treaty of Lisbon are the use of the qualified majority voting rule in the Council instead of the unanimity rule (thereby reducing

---

159 Shawn Pogatchnik "Ireland to Vote Again on EU Treaty Oct. 2" (8 July 2009) <www.news.yahoo.com> and "German Court Clears EU Treaty for House Approval" (30 June 2009) <www.euractiv.com> (both accessed 9 July 2009).

160 "Communications" in art 7 of the Charter is referred to as "Correspondence" in art 8 of the ECHR, above notes 158 and 86, respectively.

161 Convention 108 Explanatory Report, above n 111, National Legislation, para 5, lists only Portugal, Spain and Austria as incorporating data protection as a fundamental constitutional right. < www.conventions.coe.int >. Cf Ronald Leenes, Bert-Jaap Koops, Paul De Hert (eds) *Constitutional Rights and New Technologies* (T-M-C Asser Press, The Hague, 2008) at 271: only Sweden and the Netherlands incorporate an explicit, separate data protection right in their constitutions.

162 See the EU Charter, above n 158, art 8.3. For explanations of EU Charter provisions, see Draft Charter of 11 October 2000 <www.europarl.europa.eu>.

163 The EC Treaty will be renamed the Treaty on the Functioning of the European Union (TFEU). See Consolidated versions of the Treaty on European Union and Treaty on the Functioning of the European Union <www.eur-lex.europa.eu>.

voting bottlenecks), and the allocation of more authority to the European Parliament by making more legislative processes ones of co-decision by both the Parliament and Council.[164]

Also, the European Court of Justice will now have jurisdiction over new areas, including AFSJ, and national parliaments will gain additional strength and power.[165] Not only will national parliaments be able to screen EU legislative proposals, but if a majority disapproves of a particular proposal, with support from either Parliament or Council, they can have that proposal abandoned.[166] The Treaty even gives power to individuals by enabling EU citizens to petition the Commission to consider legislation (as long as they have one million signatures from a number of member states).[167]

If the Treaty of Lisbon comes into force, the three-pillar system of the EU will cease to exist. Whether the abolition of the three-pillar structure will contribute more to personal data privacy protection remains to be seen, although preliminary indications are good. To the extent that there is a lack of harmonisation on the issue of personal data protection in the current pillar system (with the EU Directive applicable only to pillar one issues), it has to be an improvement.

For one thing, the addition of a general data protection provision mirroring the one in the Charter ("Everyone has the right to the protection of personal data concerning them"[168]) is welcome. Moreover, the Treaty's guaranteed enforceability of the EU Charter itself, with its historic right to the protection of personal data, and the Treaty's provision requiring accession to the ECHR by the EU which, unlike the individual states of the Union, is not a signatory to the Convention, has some EU law experts hopeful.[169]

4 Other Instruments

The instruments discussed above are by no means a comprehensive list of recent laws addressing the right to personal data privacy. Others include:

---

164 The voting system will change to a weighted system in 2014 whereby 55% of EU countries representing at least 65% of the EU populace must agree in order to pass a law. See the Law Society of England and Wales "A Guide to the Treaty of Lisbon: European Union Insight" (January 2008) at 23-24 < www.lawsociety.org.uk>.

165 Ibid, 7, 23.

166 Ibid, 24.

167 Ibid, 27.

168 TFEU, above n 163, art 16 para 1, <www.eur-lex.europa.eu> (last accessed 7 July 2009).

169 Scirocco "The Lisbon Treaty and the Protection of Personal Data in the European Union," above n 126. See also Peter Hustinx, European Data Protection Supervisor "Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations" presentation at the 11th Conference on Data Protection and Data Security, Berlin, 8 June 2009 <www.edps.europa.eu>.

- Additional Protocol 181 (to Convention 108), added in 2001 to set up national supervisory authorities and regulate transborder data flows.[170] Implemented to fill the gap created by Convention 108's failure to address data transfers to countries that are not parties to the Convention and that have lesser privacy protections.[171]
- Directive 97/66/EC (replaced by Directive 2002/58 below) concerning the processing of personal data and the protection of privacy in the telecommunications sector. This covers new digital technologies in public communications networks, such as interactive television and video-on-demand;[172]
- Article 286 of the EC Treaty (added by the Amsterdam Treaty in 1997) extending the application of privacy principles to the processing of personal data by EC institutions and bodies;[173]
- Regulation 2001/45 (based on article 286 above), establishing the European Data Protection Supervisor (EDPS), an independent supervisory authority tasked with ensuring that EU institutions respect personal data and privacy;[174]
- Directive 2002/58/EC (ePrivacy Directive, repealing Directive 97/66/EC), regarding the processing and free movement of personal data including in the electronic communication technology sector;[175] and
- Directive 2006/24/EC (on the retention of data, and amending the ePrivacy Directive above) requiring the retention of data generated or processed in connection with the provision of publicly available electronic communications services (Internet) or of public communications networks (telephone, both fixed line and mobile, including prepaid) for a minimum of six months and a maximum of two years from the date of communication. Information to be retained includes names, addresses, telephone numbers, Internet user ID

---

170 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows (8 November 2001) CETS 181 <www.conventions.coe.int>.

171 The UK is absent from the list of ratifying countries. Protocol 181 entered into force on 1 July 2004. At the time of writing, 23 states have ratified it.

172 EU Directive 97/66/EC (15 December 1997) <www.eur-lex.europa.eu>.

173 Amsterdam Treaty, above n 125. See also Franziska Boehm "Confusing Fundamental Rights Protection in Europe: Loopholes in Europe's Fundamental Rights Protection Exemplified on European Data Protection Rules" (24 February 2009) 3 University of Luxembourg, Faculty of Law, Economics and Finance, Law Working Paper Series, Paper no 2009-01 Social Science Research Network <www.ssrn.com>.

174 European Parliament and Council Regulation 2001/45/EC (18 December 2000). For more information about the EDPS, see <www.edps.europa.eu>.

175 EU Directive 2002/58/EC (12 July 2002) <www.aedh.eu>.

> numbers, start and end times of communication. Content is not to be retained. Data is to be provided to "competent authorities without undue delay."[176] Its purpose is to ensure the availability of data to detect, investigate, and prosecute serious crimes.[177]

In implementing the EU Directive, member states have enacted their own national legislation. One example is the UK.

C United Kingdom – The Enforcer

The United Kingdom implemented the Data Protection Act 1984 in compliance with Convention 108. And it followed suit with the Data Protection Act 1998 in compliance with the EU Directive.[178] The 1998 Act came into force in early 2000. Among its exemptions are the areas of national security[179] and journalism.[180]

A national security exemption will apply as long as a Minister of the Crown (a member of the Cabinet, the Attorney General or Lord Advocate) certifies that personal data (described in a general manner) is exempt from the protections of the Act for reasons of national security. Although the certificate is conclusive evidence of the facts stated, any persons directly affected by the issuance of a certificate may appeal to the Data Protection Tribunal and the Tribunal may quash any certificate that was not issued on reasonable grounds.[181]

As an example of how the two Data Protection Acts compare, the first provided for a Data Protection Registrar, whereas the second provides for a Data Protection Commissioner, which position was subsumed into that of Information Commissioner after enactment of the Freedom of

---

176 EU Directive 2006/24/EC, arts 5 – 6 and 8 (15 March 2006).

177 Case C-301/06 – *Ireland v European Parliament, Council of the European Union* [2009] ECR I-00593. For the Advocate General's opinion see *Ireland v Parliament and Council* Case C-301/06 < www.curia.europa.eu>. For an article critical of this decision see Virginia Keyder "Someone in Brussels Should Listen to Ireland" (26 November 2008) <www.euobserver.com>. Ireland recently challenged the Directive's legal basis under EU Directive 95/46 since it concerns data retention to assist in law enforcement matters (a pillar three type activity outside the scope of the EU Directive). But the ECJ upheld the Advocate General's opinion, which held that despite the Directive's crime-fighting purpose, since it served to harmonise different data retention laws in the various Member States and eliminate disparate pricing schemes resulting from different states' data retention requirements, the EU Directive enacted under pillar one was the appropriate legal basis. Without the Directive, state-by-state variations in the type of data to be retained, and the amount of time to retain it, would impact the cost of providing electronic communication services, which would ultimately affect the internal EU market.

178 Data Protection Act 1998 (UK).

179 Ibid, s 28.

180 Ibid, s 32.

181 Ibid, ss 6 and 28(5).

Information Act 2000.[182] Because the first Act applied only to those who registered, this made enforcement hit or miss. Whereas the second Act applies to all, demonstrating exactly why the EU Directive was necessary to fill the gaps left by Convention 108 (the basis for the first Act).

The Commissioner enforces not only the Data Protection Act, but also the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations. Day to day duties include promoting good information handling practice, resolving complaints, running spot checks on government departments (as of late 2007),[183] and enforcing the law through legal sanctions.[184] This ability to prosecute, even criminally, is a feature not common to other Privacy Commissioners who act more as Ombudsmen.[185] (See New Zealand and Australia, below.)

This ability to prosecute personal data privacy breaches has the potential to make the UK one of the countries with the highest data privacy safety records in the EU. But as recent newspaper headlines attest, this is far from the case: there were reports of up to 300 serious breaches of data protection in 2008 alone.[186] However action is being taken: in 2008, data controllers' reckless or repeated disclosures of data were made a civil offence punishable by a fine,[187] and enforcement actions were commenced against two government departments for serious data breaches.[188]

While the EU was moving ahead on personal data privacy legislation (the UK had no choice), the United States, Australia and New Zealand did more than just take notice. With comprehensive privacy systems almost immediately joining the movement, the United States had no choice but to come onboard, sectoral views on privacy notwithstanding.

---

182 Rowland and Macdonald *Information Technology Law*, above n 129, at 343-344, 368.

183 In the wake of Revenue & Customs' loss of 25 million people's personal details, the Information Commissioner was granted the right to conduct independent audits. See Ian Grant "ICO Gets Right to Spot Check Government Departments in Wake of HMRC Privacy Catastrophe" (21 November 2007) < www.computerweekly.com>. However, a proposal to enable the Commissioner to audit private companies, did not become law <www.ico.gov.uk>.

184 For more information on the role of the Information Commissioner see <www.ico.gov.uk>.

185 Rowland and Macdonald *Information Technology Law*, above n 129, at 369.

186 Robert Verkaik "Big Brother Database Setback over Security Shockers" *New Zealand Herald* (Auckland, 29 October 2008).

187 Nick Heath "'Reckless' Data Loss Made Civil Offence" (13 May 2008) <www.news.zdnet.co.uk>; Nick Heath "The UK's Privacy Watchdog Could Get New Powers to Raid Organisations under Government Proposals to 'Sharpen its Teeth'" (18 July 2008) <www.news.zdnet.co.uk>.

188 Tom Espiner "Information Commissioner to Act against HMRC, MoD" (25 June 2008) < www.news.zdnet.co.uk>.

D United States – Capitalism Is Still King(?)

As noted above, the United States has a limited privacy system with federal legislation governing some sectors of the economy, leaving the rest to the market (or individual states) to legislate. Examples of federal legislation impacting data privacy in the United States include:

- the Fair Credit Reporting Act of 1970 (FCRA) – regarding the collection, dissemination and use of consumer credit information;
- the Privacy Act of 1974 – outlines the federal government's duties under FIPPs. It applies to US citizens and legal resident aliens (visitors are not protected), regarding the gathering, handling, and sharing of records maintained by government agencies. Significant exceptions to its application include defining activities as "routine use," which enables disclosure of personal data to other agencies without notifying the data subject, and using records that do not fall within the government maintained "system of records" definition to which FIPPs apply. For example, even though the government may use private systems of records, since these are not maintained by the government, they do not fall under the "system of records" definition in the Act. Moreover, even in circumstances where systems of records fall within the definition of the Act, certain government agencies (for example, FBI, DHS) are permitted to exempt them from its protections;[189]
- the Family Educational Rights Privacy Act of 1974 (FERPA) – protects students' educational records;
- the Right to Financial Privacy Act of 1978 – protects personal financial records;
- the Privacy Protection Act of 1980 – protects journalists from having to turn over work or divulge sources to law enforcement agencies before dissemination to the public;
- the Cable Communications Policy Act (1984) – protects the personal information of cable service customers;
- the Electronic Communications Privacy Act of 1986 (ECPA) – outlines access to, use, disclosure, interception and privacy protections of "real-time" electronic communications and applies to government entities, although there are exceptions for those authorised by law to intercept or conduct surveillance under the Foreign Intelligence Surveillance Act (see below);
- the Stored Communications Act of 1986 (part of the ECPA above) – protects the file contents stored by service providers, and records about the subscriber, including subscriber name, IP addresses and billing records (see below);

---

189 Francesca Bignami "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining" (2007) 48 Boston College Law Review at 609, 633-635.

- the Videotape Privacy Protection Act of 1988 – protects against wrongful disclosure of video rental and sales records;
- the Driver's Privacy Protection Act of 1994 – precludes disclosure of an individual's photograph, social security number, driver identification number, name, address (but not 5-digit zip code), telephone number, and medical or disability information;
- the Telecommunications Act of 1996 – protects the confidentiality of proprietary customer information;
- the Health Insurance Portability and Accountability Act of 1996 – regulates the use and disclosure of medical records or payment history by medical services providers and insurers;
- the Children's Online Privacy Protection Act of 1998 – regulates online collection of personal information about children under the age of 13;
- the Gramm-Leach-Bliley Act 1999 – prohibits disclosure by financial institutions of consumers' personal information to unaffiliated parties, unless advance notice is provided and consumers are given the opportunity to opt out; and
- the Telephone Records and Privacy Protection Act 2006 – bans pretexting (ie lying about identity and/or purpose, also called "blagging" in the UK) to acquire records.

Although the United States' sectoral approach to data privacy has not changed since the 1970s, the EU Directive forced the United States to modify its approach. The market's reign over privacy regulation, at least insofar as interactions with the EU were concerned, would have to be circumscribed.

The Directive was anticipated by non-EU members. In fact, the United States and EU had been in discussion about the business implications of the Directive well before it entered into force.[190] The question for the United Sates was how to comply with its requirements. Under the Directive, transfers of personal data to third countries for processing were only permitted provided there was an "adequate level of protection."[191] Just what "adequate" meant was unclear. The EU was concerned that the United States' limited privacy protection system fell short, especially its lack of a specific data-protection right for anyone not a United States citizen or legal resident. An impasse between the two blocs with the potential to adversely affect trade, among other things, loomed.

---

190 Rowland and Macdonald *Information Technology Law*, above n 129, at 340.

191 EU Directive, above n 127, art 25 para 1. See also reference to "adequate" protection addressed in the Directive art 26 para 2. For an explanation of the EU definition of "adequate" protection, see Article 29 Working Party *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (24 July 1998) Working Document WP 12 <www.ec.europa.eu>.

After extensive (sometimes antagonistic) negotiations, the EU and the US finally reached an agreement incorporating the salient features of the Directive. On 21 July 2000 the Department of Commerce (DOC) issued what have come to be known as the "Safe Harbor Principles."

Five days later, the European Commission issued a formal decision regarding the adequacy of the principles and DOC's accompanying "Frequently Asked Questions."[192] Effective as of 1 November 2000, these principles consist of: Notice, Choice (option to opt-out), Onward Transfer, Security, Data Integrity, Access and Enforcement.[193] Missing from this list are provisions limiting data preservation or storage, applicability to the public sector, and manually processed data. (See Table 1 below for more detail on the Safe Harbor Principles as they relate to other international privacy instruments.)

As long as American entities receiving data from the EU comply with the principles above, in a way that sufficiently protects privacy (either via self-regulation or compliance with regulatory, statutory, or other law), then they may take advantage of the safe harbour provided in the agreement. Contractual compliance with the Directive has also resulted in EU approval of standard contract clauses enabling the transfer of data to third countries.[194] Questions of interpretation and compliance with the principles are decided under US law.[195]

With the Safe Harbor Principles in place, the looming impasse between two different systems of privacy was averted, at least for the time being. Despite the success of the EU/United States agreement, this was not the last collision between these two systems. The EU was not standing still: in the next decade, it introduced groundbreaking treaties with the potential to expand data privacy protection rights, and create new challenges for those outside the EU.

Despite finding common ground in 2000, Europe and the United States were again on divergent paths. While the events of 9/11 brought co-operation in some fields, they pitted the two privacy systems against one another yet again. And as those events played out, the EU's personal data privacy protection scheme was also under scrutiny from within as a result of the inherent limitations of its three-pillar structure.

---

192 See US Department of Commerce FAQs at <www.ec.europa.eu>.

193 See Safe Harbor Principles at <www.ita.doc.gov>.

194 European Commission "Data Protection: Commission Approves Standard Contractual Clauses for Data Transfers to Non-EU Countries" (18 June 2001) Press Release <www.europa.eu>; European Commission "Data protection: Commission Approves New Standard Clauses for Data Transfers to Non-EU Countries" (7 January 2005) Press Release <www.europa.eu>.

195 Commission of the European Communities *Commission Staff Working Paper* (13 February 2002) SEC (2002) 196 <www.ec.europa.eu>.

E Australasia – A Contrast in Approaches

Australia was the first of two countries to adopt the OECD Guidelines in 1984.[196] New Zealand modelled its Privacy Act on Australia's, although the former is broader in coverage. Australia's Privacy Act 1988 (Commonwealth), like New Zealand's Privacy Act, deals with the collection, storage, access to, and disclosure of personal information regarding natural persons.[197] But unlike New Zealand, Australia's Act applies primarily to the Commonwealth and Australian Capital Territory (ACT) governments, and covers only part of the private sector. The credit reporting industry was added to Australia's Act in 1990, and part of the private sector was added in 2000. In addition to the Privacy Act and Codes of Practice,[198] Australia has a number of binding and advisory guidelines with similarly restricted application to certain private and government sectors.[199] The Privacy Act does not apply to intelligence agencies and the press is exempt.[200]

The 2000 amendment to Australia's Privacy Act has been much criticised as long, unclear, and imprecise:[201] "[T]he 2000 private sector amendment [is] so bad that some people think it is merely the world's worst privacy legislation whereas other people regard it as anti-privacy legislation." For example, in addition to the 11 Information Privacy Principles (IPPs) applicable to Australian and ACT government agencies,[202] the 2000 Amendment also created ten National Privacy Principles (NPPs) applicable to parts of the private sector and all health service providers. In the 2008 report of the Australian Law Reform Commission (ALRC), recommendations were made, and seconded by the Privacy Commissioner, to create a unified set of privacy principles for both public and private sectors, and to make privacy law consistent at all levels of government.[203] At the time of writing, this had yet to occur.

The regulation of data-matching, used by government to detect fraud, is either mandatory or voluntary in Australia depending on the area being regulated. The matching of tax file numbers is

---

196 For a timeline of Australian federal and state privacy legislation see "A Brief History of Information Privacy" (19 June 2002) Info Sheet 07.02 <www.privacy.vic.gov.au>.

197 For a summary of the privacy principles and guidelines available in Australia, see <www.privacy.gov.au>.

198 For example, the General Insurance Industry Code and the Code for Licensed Clubs in Queensland.

199 For a summary of the privacy principles and guidelines available in Australia, see *Privacy.gov.au,* above n 197.

200 Privacy Act 1988 (Cth) ss 7(1)(f)-(g), 7(1A), 7(2)(a)-(b), 7B(4).

201 See the Australian Office of the Privacy Commissioner's website at <www.privacy.gov.au>.

202 Ibid.

203 Ibid.

subject to a mandatory regulation.[204] Other public sector areas are not,[205] despite Australia's Privacy Commissioner recommending in 2007 that voluntary public sector matching guidelines be made so.[206]

New Zealand's Privacy Act 1993, with its 12 privacy principles, also regulates the collection, storage, access to, and disclosure of personal information of natural persons. But unlike Australia, New Zealand's principles apply across both public and private sectors.[207] New Zealand's recent introduction of its Privacy (Cross-border Information) Amendment Bill could make it the first country in the South Pacific to acquire an "adequacy" ruling from the EU.[208]

As with the UK Data Protection Act, the US Privacy Act, and the Australian Privacy Act, national security or intelligence agencies (and in some countries news media as well) are treated differently. New Zealand's Privacy Act is similar to Australia's in that it does not apply to the media "in relation to its news activities."[209] But it does not completely exempt intelligence agencies: they are exempt from most of the privacy principles (1-5 and 8-11),[210] but must still comply with principles 6, 7 and 12 (access to data, correction of data, and use of unique identifiers) Interestingly, in a 1998 Review of the Privacy Act, submissions from the two major intelligence agencies (NZSIS

---

204 The Data-matching Programme (Assistance and Tax) Act 1990 (Cth) regulates matching of tax file numbers to personal information held by the Australian Taxation Office and by other agencies (for example, the Department of Veterans' Affairs) <www.privacy.gov.au>.

205 For programmes not specifically mentioned in the Data-matching Programme (Assistance and Tax) Act 1990 (Cth), the Privacy Commissioner has issued advisory Guidelines for the Use of Data-Matching in Commonwealth Administration at <www.privacy.gov.au>.

206 The Office of the Privacy Commissioner "Amend Privacy Act to Address Security Breaches, Biometrics and Data-matching, says Privacy Commissioner" (8 March 2007) Press Release <www.privacy.gov.au>. For a list of advisory and binding guidelines, see <www.privacy.gov.au>. In addition to the federal Australian privacy scheme, the states of New South Wales, Victoria, Tasmania, Queensland, South Australia and the Northern Territory also have privacy laws along of the lines of either the IPPs, NPPs or both, but analysis of individual state privacy laws exceeds the scope of this paper. For more information, see <www.privacy.gov.au>.

207 For a summary of New Zealand's Privacy Act principles, see <www.privacy.org.nz>.

208 See the Privacy Act 1993 and Cross Border Information Bill (2008). See also Office of the Privacy Commissioner "Privacy Bill Important for Trade and Consumer Protection" (1 July 2009) Media Release < www.privacy.org.nz> (accessed 21 August 2009).

209 Privacy Act 1993, above n 208, s 2(1)(b)(xiii). The news media is not completely without regulation. There are standards the media must observe, including respecting the privacy of the individual. (Broadcasting Act 1989 s 4(1)(c)). A complaint may also be brought before the Broadcasting Standards Authority.

210 Principles 1-5 and 8-11 refer to purpose, source, collection, manner of collection, storage and security, accuracy, retention, limits on use, and limits on disclosure, respectively. For more detail, see the Privacy Act 1993, above n 208, s 57.

and GCSB[211]) stated that they agreed with principles 1, 5, 8 and 9 being applied to them.[212] At the time of writing, they are still exempt.

Industries with access to sensitive data (for example, medical, telecommunications and credit data) are regulated by more specific Codes of Practice.[213] Data matching, used by government agencies to compare records to detect fraud, is also a regulated activity.[214] Whereas the UK has the independent ability to conduct spot checks on government agencies, in New Zealand audits are initiated upon an agency's request.[215] Australian legislation does not specifically state one way or the other who initiates audits.[216] There are provisions for complaints against intelligence agencies for unwarranted invasions of privacy, but that is addressed in Section VIII below.

Both countries' legislation establishes Privacy Commissioners tasked with, among other things, promoting good information-handling practices, reviewing proposed legislation impacting privacy, conducting audits, reviewing complaints of privacy breaches, and making reports as necessary to Parliament.[217] (Both created the positions pursuant to the OECD Guidelines.)

Most recently, both the Australian and the New Zealand Law Commissions (ALRC and NZLC), have either reviewed, or are in the process of reviewing, their privacy legislation, with input from their respective Privacy Commissioners. The NZLC is finalising a lengthy four-stage review into New Zealand's privacy laws on which the Privacy Commissioner has commented along the way.[218] Its anticipated fourth-stage paper will address, among other things, the framework protecting data privacy in New Zealand.[219] As mentioned earlier, the Australian Law Reform Commission

---

211 The New Zealand Security Intelligence Service and Government Communications Security Bureau.

212 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Intelligence Organisations Submissions* (May 1998) <www.privacy.org.nz>.

213 See the Health Information Privacy Code 1994, Telecommunications Information Privacy Code 2003, and Credit Reporting Privacy Code 2004. In addition to sector-specific codes regarding unique identifiers, there is also an Internet Service Providers Code in development <www.internetnz.net.nz>. In the event of interference with privacy either by a breach of the Privacy Act or Code of Practice, and ensuing significant harm, a complaint may be filed with the Office of the Privacy Commissioner. For additional information see New Zealand Privacy Commissioner's website <www.privacy.org.nz>. Other avenues of relief in the event of interference with privacy exist in New Zealand, including the ability to bring complaints before the Broadcasting Standards Authority, and the Press Council, but these are beyond the scope of this paper.

214 See the Privacy Commissioner's web page on Data Matching at <www.privacy.org.nz>.

215 Privacy Act 1993, above n 208, s 13(1)(b).

216 Privacy Act 1988 (Cth), above n 200, ss 27(1)(h), (ha), 28(1)(e), 28A(g), 32(1).

217 Privacy Act 1993, above n 208, s 13; Privacy Act 1988 (Cth), above n 200, ss 27-29.

218 See Privacy Commission submissions at <www.privacy.org.nz>.

219 New Zealand Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy: Stage 1* (NZLCSP19, Wellington, 2008), above n 27, at 68, para 3.53 <www.lawcom.govt.nz>.

recommended enacting breach of privacy legislation in 2007; the New Zealand Law Commission is still undecided on this issue, although the development of two privacy torts in New Zealand is supported by the Privacy Commissioner. (See Section V above.)

The discussion above provides the backdrop for many of the instruments and co-operative efforts the world engaged in after 9/11. In the same way that nations came together after World War II in the hope of preventing future atrocities, so they did now. And leading the way again was the United Nations.

If the principles protecting information privacy had faced challenges before 2001, they would soon be put through even more rigorous trials in the aftermath of 9/11. While the full implications of these challenges are still evolving, we can glean from recent actions the direction the West is taking to combat terrorism, and the role that personal data is playing.

VIII PRE-9/11 COUNTER-TERRORISM INSTRUMENTS

In the days before 9/11, the UK, US, Australia, and New Zealand all had legislation dealing with terrorism. So did the Council of Europe.[220] Set out below are some of those instruments enacted during the latter part of the 20th century.[221]

A Council of Europe

In 1977, the Council of Europe signed its Convention on the Suppression of Terrorism.[222] Reclassifying terrorist actions as "offences" and not political acts, this Convention enabled extradition for acts that were previously not susceptible to foreign prosecution. It set out the grounds for mutual assistance, including extradition or prosecution of those accused of terrorist offences:[223]

> [E]xtradition is a particularly effective measure for combating terrorism.
>
> ...

---

220 But post-9/11 EU counter-terrorism efforts outpace those pre-9/11. See Section IX below.

221 Laws regarding treason and sedition date back centuries, for example the United States' Alien and Sedition Acts from 1798, and New Zealand's proclamations of martial law to quell Maori resistance in the mid- to late-1880s, but these exceed the scope of this paper. For more information on these and other countries' laws, see John Smith "New Zealand's Anti-Terrorism Campaign: Balancing Civil Liberties, National Security, and International Responsibilities" (December 2003) 1 <www.fulbright.org.nz> citing New Zealand Law Commission *Final Report on Emergencies* (NXLC R22, Wellington, 1991). For a comparison of the counter-terrorism laws of various nations, see Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, above n 70.

222 Ibid.

223 Convention ETS No 090 1977-01-27 Explanatory Report, General Considerations, paras 13 and 22 < www.conventions.coe.int>. For a summary of the Convention see <www.conventions.coe.int>.

> This method, which was already applied to genocide, war crimes and other comparable crimes ... as well as to the taking or attempted taking of the life of a head of State or a member of his family ... accordingly overcomes for acts of terrorism not only the obstacles to extradition due to the plea of the political nature of the offence but also the difficulties inherent in the absence of a uniform interpretation of the term 'political offence'.

The Convention started a trend of redefining terrorism; countries soon followed suit.

B United Kingdom

Between 1974 and 1989, the UK enacted a series of Acts granting the police emergency powers to deal with the situation in Northern Ireland (the Prevention of Terrorism Acts).[224] The UK also enacted the Criminal Justice and Public Order Act 1994, which amended the Prevention of Terrorism (Temporary Provisions) Act 1989 by expanding the definition of terrorism to include the possession of articles suspected to be for terrorist purposes and the unlawful collection of information. It also put the burden on the defendant to disprove their guilt, contrary to centuries of legal precedent regarding the assumption of innocence.[225]

The 1994 Act also vastly limited the right against self-incrimination by allowing adverse inferences to be drawn from silence, and increased the rights of police to take bodily samples, and stop and search vehicles and persons.[226] It continued to limit the definition of terrorism geographically, however, describing terrorist acts either as ones committed in relation to Northern Ireland, or ones unrelated to events in the UK.[227] With the Terrorism Act 2000, the Prevention of Terrorism (Temporary Provisions) Act 1989 was repealed.[228] However, the 1994 Act remained intact.

While the 2000 Act was intended to bring UK terrorism laws into line with human rights standards set out in the ECHR and the Human Rights Act of 1998, certain provisions actually had the opposite effect. For example, in addition to expanding the definition of terrorism to include not just those principally engaged in terrorist acts, but also those that assist in inciting, financing, and training, article 41 paragraph 1 gave a constable the right to arrest anyone without a warrant that

---

224 Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, above n 70, at 58.

225 Criminal Justice and Public Order Act 1994 (UK) s 82.

226 Ibid, ss 34-39, 54-59, and 81.

227 Ibid, s 81.

228 Terrorism Act 2000 (UK) s 2(1)(a).

they "*reasonably suspect* to be a terrorist." (Emphasis added.) Banks could also now be compelled to disclose customer information "in relation to a terrorist investigation".[229]

Also in 2000, the UK enacted the Regulation of Investigatory Powers Act (RIPA),[230] which regulates the interception, acquisition and disclosure of communications data, surveillance, and access to encryption- or password-protected electronic data in cases involving national security. (Since parts of this Act were not in force until 2007, RIPA will be treated separately in the Section on post-9/11 legislation below.)

As far as oversight of counter-terrorism legislation in the UK went, a review process had been in place since before 9/11 to deal with the problems of Northern Ireland.[231] Just hours before the attacks on 9/11, Lord Carlile was appointed Independent Reviewer of Terrorism Laws by the British Home Secretary.[232] His mandate is laid out on the Home Office's website: "Terrorism laws must strike a delicate balance between providing effective tools to investigate and prevent terrorism, while ensuring that our civil liberties are not unnecessarily infringed."[233]

Still, Lord Carlile has been controversial in his support of legislation in opposition to the bipartisan Joint Committee on Human Rights. His most recent reports have concerned "control orders" (orders restraining any suspect's communications, travel or interactions) and the definition of terrorism.[234]

C United States

Like the UK, the United States had piecemeal legislation dealing with terrorism until the new millennium. But, whereas, the UK enacted its terrorism legislation in 2000 during a time of relative peace, the US did so in response to a terrorist event.[235]

Prior to 9/11, the United States used a variety of laws and actions to combat terrorism, ranging from the criminal law (used to convict the terrorists in the first World Trade Center bombing in

---

229 Terrorism Act 2000 (UK) Schedule 6. See also Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, above n 70, at 59-61.

230 Regulation of Investigatory Powers Act 2000 (UK). For an explanatory note on the legislation see < www.opsi.gov.uk>.

231 Andrew Lynch, Nicola Garrity "At Last, an Independent Reviewer of Terrorism Laws" (16 July 2009) *Inside Story* <www.inside.org.au> (accessed 3 August 2009).

232 See the UK Home Office's Independent Reviewer of Terrorism Laws website < www.security.homeoffice.gov.uk>.

233 Ibid.

234 Lynch and Garrity "At Last, an Independent Reviewer of Terrorism Laws", above n 231.

235 Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, above n 70, at 58-59.

1993) to military operations (for example, President Reagan authorised air strikes on Libya in 1986; and President Clinton authorised the launch of cruise missiles on suspected targets in Afghanistan and Sudan after bombings of the US Embassy in Tanzania and Kenya in 1998).[236] After the 1995 Oklahoma City bombing of a federal building by domestic terrorists that killed 168 and injured almost 700, it enacted the Antiterrorism and Effective Death Penalty Act of 1996 to "deter terrorism, provide justice for victims, [and] provide for an effective death penalty … ."[237]

Supervision of the intelligence community has historically been the province of the Senate and House Intelligence Committees. With the assistance of the Congressional Research Service and the General Accounting (now Accountability) Office, Congress has held a number of hearings on the implementation of counter-terrorism laws and programmes, frequently on an ad hoc basis, when they are brought to their attention by the press, or public outcry. (See below.)

D Australia

Although Australia did not have specific terrorism laws before 2001 (except measures enacted by the Northern Territory),[238] it has had laws protecting national security since the late 1960s and 1970s.[239] These were enacted largely in response to politically motivated local terrorist acts: the 1965 assassination attempt on Arthur Calwell, Australian Labour Party Leader, over his stance on the Vietnam War; the 1968 bombing of the US Embassy in Melbourne; in 1978 a bomb outside the Sydney Hilton Hotel disrupting the Commonwealth Heads of Government Regional Meeting (3 killed, 11 injured); and the 1986 Turkish Consulate bombing (where the bomber alone was killed).[240]

As far as oversight of security agency activities, Australian legislation provided for an Inspector-General of Intelligence and Security, whose duty it was to assist Ministers in overseeing and reviewing security agencies' compliance with the law, and reviewing the appropriateness and effectiveness of security agency activities, including compliance with human rights.[241] Inquiries

---

236 The African embassy bombings resulted in more than 220 deaths and 4,000 injured. Benjamin Wittes *Law and the Long War: The Future of Justice in the Age of Terror* (Penguin Books, Ltd, London, 2008) at 23. For more information on the Embassy bombings in Africa, see the US State Department website < www.state.gov>.

237 Antiterrorism and Effective Death Penalty Act of 1996, Pub Law No 104-132, 110 Stat 1214 (1996) 104 < www.fas.org>. For a comprehensive summary of the Act see <www.fas.org>.

238 For a list of (and links to) Australian laws to combat terrorism, see <www.nationalsecurity.gov.au>. See also John Smith "New Zealand's Anti-Terrorism Campaign: Balancing Civil Liberties, National Security, and International Responsibilities", above n 221, at 47.

239 See also Mark Pearson and Naomi Busst "Anti-terror Laws and The Media after 9/11: Three Models in Australia, New Zealand and the Pacific" (2006) 9 Pacific Journalism Review 12(2) at 2.

240 For more detail on the terrorist events in Australia, see <www.wikipedia.org>.

241 Inspector-General of Intelligence and Security Act 1986 (Cth) s 4.

could be commenced at the behest of a Minister, in response to a complaint, or on the Inspector-General's own initiative.[242] In an attempt to avoid politicisation of the position, the Inspector-General was appointed only after the Prime Minister had consulted with the Leader of the Opposition, and his annual reports were provided to both.[243]

The Australian Security Intelligence Organisation (ASIO) was also required to report annually on its activities to the Minister, with a copy to the Leader of the Opposition. Its reports frequently ran over 130 pages in length.[244] Still, many considered meaningful parliamentary oversight of antiterrorism legislation in Australia pre-9/11 lacking.[245]

E New Zealand

In addition to a history of responding to UN-initiated sanctions programmes, New Zealand had terrorism legislation on the books well before 9/11. After the bombing by French government agents of the Greenpeace vessel Rainbow Warrior, in Auckland Harbour in 1985 (killing one Portuguese photographer),[246] it enacted the International Terrorism (Emergency Powers) Act 1987.[247]

Over the years, a number of amendments to the definition of "security" in the New Zealand Security Intelligence Service Act 1969 (NZSIS Act) have been enacted. The first revision in 1996[248] changed the definition to include New Zealand's international or economic well-being.[249] Like the UK's Regulation of Investigatory Powers Act 2000 (see below), the Act allowed the intelligence service to protect not just against traditional threats to national security (such as espionage, sabotage, and subversion) but also ones impacting New Zealand's economy.[250]

Other changes in 1996 were the creation of the Intelligence and Security Committee (to increase the level of oversight of the NZSIS and the GCSB),[251] and the position of Inspector-General of

---

242 Ibid, s 8.

243 Ibid, s 35(3).

244 Australian Security Intelligence Organisation Act 1979 (Cth) s 94(1)-(3).

245 Christopher Michaelsen "Australia's Anti-terrorism Laws Lack Adequate Oversight Mechanisms" < www.webdiary.com.au>.

246 For more information on the sinking of the Rainbow Warrior, see the Greenpeace website < www.greenpeace.org>.

247 International Terrorism (Emergency Powers) Act 1987.

248 Added by the New Zealand Security Intelligence Service Amendment Act 1996.

249 Geoffrey R Weller "Change and Development in the New Zealand Security and Intelligence Services" (Spring 2001) The Journal of Conflict Studies. The Gregg Centre for the Study of War and Society (Vol XXI No 1.

250 New Zealand Security Intelligence Service Act 1969 ss 2(1) (b) and (c)(iii).

251 Intelligence and Security Committee Act 1996.

Intelligence and Security.[252] The Intelligence and Security Committee comprises the Prime Minister, the Leader of the Opposition, two additional members nominated by the Prime Minister, and one nominated by the Leader of the Opposition. Its duties include reviewing NZSIS annual reports and matters referred to it by the Prime Minister.[253] The Inspector-General's duties, much like his counterpart in Australia, are to assist each minister responsible for an intelligence agency in conducting oversight and review of that agency.[254]

But unlike Australia, New Zealand intelligence agencies must comply with some Privacy Act principles, giving the Office of the Privacy Commissioner another level of oversight. In 1996 New Zealand's first Privacy Commissioner prepared a lengthy report regarding the proposed intelligence agency legislation amendments:[255] among his recommendations were the replacement of a Prime Ministerial warrant with a judicial one, and greater detail in NZSIS annual reports.[256]

The level of reporting by the NZSIS pales in comparison to that of the ASIO. The NZSIS 2008 report, for example, is 27 pages long, and only 12 lines actually concern interception warrants. The most recent report (for the year ended 30 June 2008) is typical: 25 domestic interception warrants in force, only 14 of which were newly issued that year (11 remained in force from the year before). Although foreign interception warrants were in force in 2008, no number was provided.[257]

Despite the Privacy Commissioner's recommendations, the warrants continue to be ministerial and, as shown above, no greater detail has since been provided in NZSIS' annual reports. Nevertheless, the Privacy Commissioner did sanction the creation of the position of Commissioner of Security Warrants to be filled by a retired High Court Judge.[258] (See below.)

In the case of allegations of intelligence agency interference with individual privacy, New Zealand's Privacy Act enables the Privacy Commissioner to investigate and, if satisfactory action is not taken by the intelligence agency, they may report to the Prime Minister. The Prime Minister may, in turn, bring the Commissioner's report before Parliament.[259] The New Zealand Privacy Act's

---

252 The New Zealand Inspector-General of Security and Intelligence Act of 1996.

253 See the NZSIS website <www.nzsis.govt.nz>.

254 Inspector-General of Security and Intelligence Act of 1996, above n 252, s 11.

255 B H Slane *Report By The Privacy Commissioner To The Minister Of Justice On The Intelligence And Security Agencies Bill* (26 February 1996) <www.privacy.org.nz>.

256 Ibid.

257 *New Zealand Security Intelligence Service Annual Report for the Year Ended 30 June 2008* at 20 < www.nzsis.govt.nz>.

258 B H Slane *New Zealand Security Intelligence Service Amendment Bill (No 2)* (12 April 1999) < www.privacy.org.nz>.

259 Privacy Act 1993, above n 208, ss 69-72B, and s 81.

review procedure is more in line with the UK's Data Protection Act appeals process than with Australia's Privacy Act, which does not have a comparable provision.

New Zealand has been moving toward more openness and accountability in government. As stated by Sir Kenneth Keith in his essay "Freedom of Information and International Law:[260]

> New Zealand is a small country. The Government has a pervasive involvement in our every-day national life. This involvement is not only felt, but is also sought, by New Zealanders, who have tended to view successive Governments as their agents, and have expected them to act as such.

In the case of *Choudry v Attorney-General*,[261] the Government was held accountable in a case of a warrantless search of a political demonstrator's home to effect an interception warrant. Holding that an interception warrant did not imply a right to invade private property without consent, the interlocutory decision of the New Zealand Court of Appeal made clear that while Ministers may be better placed "to evaluate the needs of national security," that did not mean that courts will be *"beguiled by the mantra of national security into abdicating [their] role in the balancing exercise."*[262] (Emphasis added.) Despite its initial strong stance, when the government produced a more detailed ministerial certificate (and an additional 20 documents), the Court of Appeal ultimately granted the government public immunity on national security grounds. In so ruling, the government did not have to disclose documents supporting its covert entry.[263]

This decision was not popular, as evidenced by the rash of stories circulating in the press at the time.[264] Still, the government actually admitted wrongdoing and settled with Mr Choudry. The amount of settlement was confidential.[265] This may have been a minor concession in view of the government's actions, but the message was clear. If the government was going to engage in covert action, it had better have Parliament's blessing to back it up. Which is exactly what it did – not

---

260 Sir Kenneth Keith "Freedom of Information and International Law" in Jack Beatson and Yvonne Cripps (eds) *Freedom of Expression and Freedom of Information: Essays in Honour of Sir David Williams* (Oxford University Press, Oxford, 2000) at 349-374.

261 *Choudry v Attorney-General* [1999] 2 NZLR 582.

262 Ibid, at 592, 593.

263 *Choudry v Attorney-General* [1999] 3 NZLR 399.

264 See the editorial "Court in Awe Again" *New Zealand Herald* (Auckland, 8 July 1999); Warren Berryman "Appeal Court Abdicates its Role as Democratic Watchdog" *The Independent* 14 July 1999; Steven Price "Passing Judgement: Who Will Hold PM Accountable if Appeal Court Will Not?" *New Zealand Herald* (Auckland 23 July 1999). As reported by Murray Horton in "Aziz Choudry Wins Case Against SIS: Out Of Court Settlement; Damages; Government Apology" in *Peace Researcher* (November/December 1999) 19/20 <www.converge.org.nz>.

265 Ibid.

unlike what the United States would do a few years later in its own warrantless wiretapping fiasco. (See below.)

After the Court's ruling, the government enacted two amendments to the NZSIS Act 1969 that effectively eviscerated the interlocutory ruling in *Choudry*. The first amendment gave the NZSIS power to intercept not just communications, but any "document, or thing", and expanded its power of entry to any "place" in New Zealand, including ″any land, building, premises, dwellinghouse, vehicle, vessel, or aircraft."[266] The second amendment outlined additional parameters of NZSIS activities (for example keeping Ministers or government departments, public authorities and anyone else the Director believes should know, apprised of the "protective measures that are directly or indirectly relevant to security"), and made clear that it was not the job of the SIS to enforce security measures.[267] It also created the new position of Commissioner of Security Warrants.

Domestic interception warrants now had to be corroborated by the Commissioner of Security Warrants. (Not so foreign interception warrants.) The Commissioner was to be appointed by the Governor-General on the recommendation of the Prime Minister, and upon consultation with the Leader of the Opposition. Their duties include advising the Prime Minister on applications for domestic interception warrants, consulting with the Prime Minister on the parameters of the applications, and issuing them jointly with the Prime Minister.[268]

Finally, in April 2001, the Terrorism (Bombings and Financing) Bill, the precursor to the Terrorism Suppression Act 2002,[269] was introduced. Although introduced in early 2001, it would not come into force until after 9/11. Upon introduction, it received no submissions. After 9/11, significant amendments in the form of a Supplementary Order Paper were added to it. These received 140 submissions.[270]

---

266 New Zealand Security Intelligence Service Act 1969 (as amended) ss 4A(1); and 2(1) definition of "Place".

267 New Zealand Security Intelligence Service Act 1969 (as amended) ss 4(1)(ba) and 4(2). See also Weller "Change and Development in the New Zealand Security and Intelligence Services", above n 249; and John Smith "New Zealand's Anti-Terrorism Campaign", above n 222, at 12.

268 New Zealand Security Intelligence Service Act 1969 (as amended), above n 266 s 5A.

269 Terrorism Suppression Act 2002.

270 Tim McBride "Heightened State Surveillance in New Zealand, Post-'9/11' – Privacy Under Threat" Privacy Law and Policy Reporter (2005) at 3-4. For more information on New Zealand's counter-terrorism laws see Alex Conte *Counter-Terrorism and Human Rights in New Zealand* (New Zealand Law Foundation, Wellington, 2005 – statutory references updated April, 2007). See also Pearson and Busst "Anti-terror Laws and The Media after 9/11, above n 239.

This national, unco-ordinated approach, often in response to acts of domestic terrorism, would soon change.[271] September 11 would see to that.

IX POST-9/11 INSTRUMENTS AND CO-OPERATIVE EFFORTS RELATING TO PERSONAL DATA PRIVACY

Almost immediately after the attacks, all of the above international bodies and many countries (including the UK, US, Australia and New Zealand), either enacted legislation, created new entities, or engaged in co-operative efforts, to combat the threat of terrorism; some did all three. And the United Nations became, for all intents and purposes, the spearhead of all the efforts being made.[272]

A The United Nations – International Ringmaster

> [We] call on all States to work together urgently to bring to justice the perpetrators, organizers and sponsors of today's outrages. [We] call on the international community to redouble its efforts to prevent and suppress terrorist acts by increased cooperation and full implementation of relevant anti-terrorist conventions and Security Council resolutions.

With this press release, the UN Security Council made clear its intentions to thwart terrorism through international co-operation.[273]

UN Secretary-General Kofi Annan issued a heartfelt and sober statement that same day, warning that while "[t]errorism must be fought resolutely wherever it appears ..., cool and reasoned judgement is more essential than ever."[274] The events of 11 September 2001 were to be the catalyst for renewed co-operative legal efforts in the international arena.

The United Nations is no stranger to terrorism. At the time of writing, it has elaborated dozens of international instruments to fight it. Since 9/11, its efforts have ranged from the adoption of resolutions at both the Security Council and General Assembly level, to the establishment of several counter-terrorism bodies, and the implementation of a Global Counter-Terrorism Strategy with an associated Plan of Action.

Only one day after the attacks, the UN Security Council adopted Resolution 1368 calling on all states to work together to bring to justice the perpetrators and anyone "aiding, supporting or

---

271 For a comparison on the counter-terrorism laws of various nations, see Beckman *Comparative Legal Approaches to Homeland Security and Anti-Terrorism*, above n 70.

272 Smith "New Zealand's Anti-Terrorism Campaign", above n 221, at 1.

273 UN Security Council President "Press Statement by Security Council President on Terrorist Attacks in United States" (11 September 2001) SC/7141, 11 <www.un.org>.

274 UN Secretary-General "Secretary-General Condemns Terrorist Attacks on the United States" (11 September 2001) SG/SM/7948 <www.un.org>.

harbouring" those responsible.[275] Echoing its press release of the day before, the Security Council now resolved to increase co-operation, including full implementation of Resolution 1269 of 19 October 1999, which included, among other things, a call to action to all states to co-operate through bilateral and multilateral agreements and information exchange to (1) prevent terrorist attacks and their financing, and (2) deny terrorists safe havens or refugee status.[276]

These resolutions were given teeth on 28 September 2001, when the Security Council adopted Resolution 1373, "one of the most strongly-worded resolutions in the history of the Security Council."[277] Among other things, it required that states "[f]reeze without delay funds and other financial assets or economic resources of persons who commit ... or participate in or facilitate the commission of terrorist acts;" and "...[a]fford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings ... including assistance in obtaining evidence ...." This Resolution also established the Counter-Terrorism Committee (CTC), (comprising all members of the Security Council) to monitor states' progress and assist with "technical, financial, regulatory, legislative or other programmes."[278]

On 16 January 2002, the Security Council added one more tool to its arsenal: naming specific people and organisations, not just nations, who were in some way involved in terrorism. Resolution 1390 required that the assets of persons or groups associated with Osama bin Laden, Al-Qaida and the Taliban be frozen "without delay."[279]

The Security Council was not alone in its efforts. In July 2005, the Secretary-General established the UN Counter-Terrorism Implementation Task Force (CTITF) to co-ordinate various UN counter-terrorism initiatives. One of its accomplishments is the creation of an Online Handbook, which contains information ranging from the types of counter-terrorism activities in which member states are engaged, to contact information for UN resources, including its partners: Interpol, its European equivalent (Europol),[280] the International Civil Aviation Organization, Organization of American States, Organization of African Unity, and Arab Interior Ministers Council. Apart from a

---

275 *Threats to international peace and security caused by terrorist acts* SC Res 1368 (2001) <www.un.org>.

276 *Resolution on the responsibility of the Security Council in the maintenance of international peace and security* SC Res 1269 (1999) <www.un.org>.

277 Smith "New Zealand Anti-Terrorism Campaign", above n 221, at 19, quoting Alex Conte "A Clash of Wills: Counter-terrorism and Human Rights" (June 2003) 20 NZULR at 338, 342.

278 *Threats to international peace and security counsel by terrorist acts* SC Res 1373 (2001) paras 1(c), 2(f) and 6. See also *Combating Terrorism* SC Res 1377 (2001) <www.un.org>.

279 *The situation in Afghanistan* SC Res 1390 (2002) para 2(a) <www.un.org>.

280 The European Police Office (Europol), set up in 1992, handles criminal intelligence throughout Europe to combat organised international crime and terrorism. Based in The Hague, it is staffed by representatives of national law enforcement agencies including police, customs, and immigration. See <www.europa.eu>.

mere information resource, the CTITF provides practical assistance, through its partners. For example, Interpol assists with training, responding to incidents, and operating "a range of databases covering key data such as names ..., fingerprints, photographs, DNA profiles, stolen or lost travel documents, and wanted persons" that it shares with Member states.[281] Interpol has also been responsible for the development of a secure global police communication system.

Shortly after these developments, the General Assembly implemented an overarching strategy of its own to co-ordinate all UN efforts in the fight against terrorism. On 20 September 2006, with the adoption of General Assembly Resolution 60/288[282] and its annexed Plan of Action, the United Nations Global Counter-Terrorism Strategy (UN Strategy) was born. Passed by all 192 member states, it constitutes the UN's most comprehensive, concrete approach to thwarting terrorism to date.

The Strategy is organised by themes and grouped into four pillars: (1) addressing conditions conducive to the spread of terrorism; (2) preventing and combating terrorism; (3) building state capacity to counter terrorism; and (4) defending human rights while combating terrorism. While co-operation, including the sharing of information among states, ranks highly among the UN Strategy's goals, it is careful to preface any such efforts with compliance with international law obligations "including the Charter of the United Nations and relevant international conventions and protocols, in particular human rights law, refugee law and international humanitarian law."[283] Although not binding, it does contain resolutions to comply with member states' international law obligations, and to enact provisions nationally to prohibit incitement to commit terrorist acts.[284] It also enables states to reaffirm and recommit to it by engaging in periodic reviews, the last of which occurred in September 2008. The next Strategy review is scheduled for 2010.

B European Institutions Follow UN Lead

The Council of Europe and the EU were not far behind the UN. One of the first actions the EU took was only ten days after 9/11. It created the European Council Action Plan on Combating Terrorism.[285] Its combination of offensive and defensive objectives included ending the funding of terrorist actions, and streamlining prosecutions.

This effort was followed in November 2001 by the Council of Europe's adoption of a second additional protocol to the European Convention on Mutual Assistance in Criminal Matters, to speed

---

281 See UN Web page on terrorism handbook <www.un.org>.

282 A/Res/60/288.

283 Annex, Plan of Action, para 3. See also Annex, Plan of Action Sections II 4, 14, and 15, and III 6 and 8 < www.un.org>.

284 Ibid, Section I, para 4.

285 European Council Action Plan on Combating Terrorism <www.consilium.europa.eu>. For 2004 Action Plan Realignment see Declaration on Combating Terrorism (25 March 2004) <www.consilium.europa.eu>.

up processes and facilitate investigations.[286] This alternating enactment of instruments continues to this day, with the Council of Europe and the EU both introducing programmes to counter terrorism. The bulk of the efforts have concerned broadening the definition of terrorism, stopping its funding, increasing cross-border co-operation, establishing entities to assist in prosecutions and derailing terrorism (Eurojust,[287] CODEXTER[288]), and providing airline passenger information across borders. (More on that below.)

(For more detail on the above instruments and programmes, and a comparative table on post-9/11 counter-terrorism legislation, see Table 2.)

C Countries and their Databases

9/11 wasn't the sole impetus for bringing the world together to fight terrorism. Spurring the world on were subsequent terrorist acts in Bali, Madrid and London. The three Bali bombings on 12 October 2002 killed 202 people (88 of whom were Australian), and injured 209 more.[289] The Madrid train bombings on 11 March 2004 killed 191 people and wounded 1,800,[290] and the London bombings on 7 July 2005 killed 56 people, (including the four British Muslim bombers) and injured 700.[291]

In an effort to stem the tide of such attacks, governments of the world went into overdrive to create new programmes, new laws, expand existing ones, and work collaboratively to prevent future terrorist attacks. Almost all of these efforts involved amassing vast amounts of data.

---

286 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No 182) <www.conventions.coe.int>.

287 Eurojust is a centralised team of international jurists and other legal experts from every Member State, established to give advice and co-ordinate cross-border prosecutions. For more information, see < www.europa.eu>.

288 The Committee of Experts on Terrorism (CODEXTER) is an intergovernmental committee consisting of representatives from various CoE and EU entities, as well as the UN, Organisation of American States (OAS), Interpol, Europol, and other observer states, including the United States, Mexico, Argentina, the Holy See, Japan and Canada. The International Committee of the Red Cross also has observer status. CODEXTER agenda items include identification of gaps in both international law and the actions needed to fight terrorism. For more information see <www.coe.int>.

289 Australian Federal Police "Bali Bombings 2002" <www.afp.gov.au>.

290 See 2004 Madrid train bombings <www.wikipedia.org>.

291 See 7 July 2005 London bombings <www.wikipedia.org>.

1 UK – DNA database on innocents

Some examples of the current programmes being rolled out in the UK include a giant database of every email, telephone call, text message and website visit,[292] an identity card programme for foreign nationals,[293] and a database containing approximately 4.5 million DNA profiles. Almost one million of those profiles are of persons with no criminal convictions, 40,000 of whom are children.

The European Court of Human Rights recently ruled that holding data on innocents breached the European Convention of Human Rights.[294] The UK has started to delete some 850,000 DNA profiles of people who have neither been arrested nor convicted of a crime. But it is retaining DNA profiles on those arrested, even if not convicted, for between 6 and 12 years, depending on the nature of the crime.[295] Other countries are assembling their own databases.

2 US – Databases "R" Us

The United States government maintains over 5,000 databases of information, or "systems of records," as defined under the Privacy Act.[296] Many were in existence prior to 9/11. Some have received more attention than others, often due to the efforts of a number of civil liberties organisations. In trying to obtain information about government databases, these organisations are often forced to file suit under the Freedom of Information Act, which inevitably creates more publicity. One example is the Department of Defense's (DOD) TALON.

In March 2007, the Department of Defense published a request for comments on law enforcement reporting.[297] In that request, Police intelligence was to send pre-TALON reports to counterintelligence agencies, who would in turn decide "if the suspicious incident/activity should be entered into the DOD TALON reporting system," a database of purported threats to military installations. After it was discovered that 186 domestic anti-war protests were included in the

---

292 Robert Verkaik "British Black Boxes Will 'Collect Every Email'" *New Zealand Herald* (Auckland, 5 November 2008).

293 Gregory Katz "Britain Begins Big Brother ID Card Programme" *New Zealand Herald* (Auckland, 26 November 2008).

294 Peter Walker "European Court Rules DNA Database Breaches Human Rights" (4 December 2008) < www.guardian.co.uk>. See also Tom Whitehead and Christopher Hope "DNA Database Innocents Win Landmark European Court Ruling" (4 December 2008) <www.telegraph.co.uk>.

295 Leo King London "UK Government to Delete DNA Profiles from Database Profiles of 850,000 Innocent People To Be Deleted" (11 May 2009) *Computerworld* <www.computerworld.co.nz>.

296 See <www.data-detective.com>.

297 Department of Defense, Department of the Army, Law Enforcement Reporting; Proposed rule; request for comments (15 March 2007) 72 Federal Register 50 12143 <www.bulk.resource.org>.

database, it was shut down by incoming Defense Secretary, Robert Gates, who succeeded Donald Rumsfeld.[298]

In addition, the US government relies on commercial databases (CDBs), which are not subject to regulation by the Privacy Act. Commercial databases sell information, either directly or indirectly, to law enforcement agencies, debt collectors, insurance claim adjusters, lawyers and private investigators, or to any other licensed professional with a valid business need.[299] Examples of some commercial databases include, Accurint, Autotrack and LexisNexis.

Accurint contains personal name, address and telephone information, and uses association algorithms to find new contact details if provided with old information. Autotrack has access to 13 billion records in the US, Puerto Rico and the Virgin Islands, regarding drivers' licence information for 36 US states, and registered vehicle owner information (derived from licence plates). It also has a person locator feature: if provided with a person's name, address or other identifying details, it can provide contact details and real-time credit header information.[300] LexisNexis provides legal, news, business and public record information, and is used mainly by government, business, the legal profession and academia.[301]

ChoicePoint, one of the more famous active CDBs (which bought Autotrack), provides government and industry with data on Americans and foreigners alike. The US government's reasoning in purchasing this data is that since it is in the public realm, data subjects have no expectation of privacy. That someone entered a contest or filled out a loyalty card and provided this information for those purposes does not preclude the data from being later on-sold for completely different purposes, a concept anathema to European lawmakers.

One of the most famous historical examples of misuse of ChoicePoint data is its contribution to skewing the 2000 US election results. By providing the State of Florida with a list of "suspected" felons (many registered black Democrats), at least 1,000 people were barred from the polls. President Bush's margin of victory in Florida was 327 votes. At stake were Florida's 25 electoral votes. The tally at the end of the day was 271 electoral votes for President Bush (including Florida's 25) and 266 for Al Gore. The National Association for the Advancement of Colored People (NAACP) sued. The case was settled with ChoicePoint agreeing to review its list of suspected ex-

---

298 Ryan Singel "Pentagon to Power Down Spy Database" (25 April 2007) <www.wired.com>.

299 Steven Kerry Brown *The Complete Idiot's Guide to Private Investigating* (2nd ed, Alpha Books/Penguin Books USA, New York, 2007) at 110-111.

300 Ibid, at 111, 117.

301 See <www.lexisnexis.com>.

cons.[302] This is an example of a legal data sale. But ChoicePoint has also been known to buy data of more dubious origins.

In 2003, three Mexican nationals were put under house arrest on a charge of treason after being suspected of selling voter registration rolls, protected by Mexican federal law, to ChoicePoint.[303] As of 2007, ChoicePoint was still settling cases for data breaches, including with the Federal Trade Commission and various states.[304] As of 2008, it was still unregulated and in business, and according to some reports, not the worst offender. While ChoicePoint restricts to whom it sells data, others do not.[305]

Another post-9/11 development was the creation of fusion centres. Created by states in response to the 9/11 Commission's finding that there was a need to "fuse" domestic and foreign intelligence, their goal was to integrate "various streams of information and intelligence … from the federal government, state, local, and tribal governments, as well as the private sector, [to create] a more accurate picture of risks to people, economic infrastructure, and communities [that] can be developed and translated into protective action."[306] The National Criminal Intelligence Sharing Plan[307] (developed after 9/11) served as the impetus.

Every state (with the exception of Idaho) has adopted some form of fusion centre.[308] In 2004-2005, these centres were developing at an exponential rate without any overarching structure, accountability or control. While state and local law enforcement agency co-operation to fight crime was not new, the inclusion of counter-terrorism analysis, the integration of private sector

---

302 Joseph Menn "Did ChoicePoint End Run Backfire?" (13 March 2005) *Los Angeles Times* <www.articles.latimes.com>. "Big Brother Goes Global: Assembling Electronic Dossiers on Millions of People" (12 January 2005) <www.globalresearch.ca>. See also <www.wikipedia.org>. For additional information on how ChoicePoint works see Chris Jay Hoofnagle "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement" (Summer 2004) University of North Carolina Journal of International Law & Commercial Regulation, at fn 111 Social Science Research Network <www.ssrn.com>.

303 Menn, above n 302.

304 "ChoicePoint Settles Data Security Case" (1 June 2007) *New York Times* <www.nytimes.com>.

305 Brad Stone "Is ChoicePoint a Model of Restraint in Releasing Criminal Records?" (2 August 2008) *The New York Times* <www.bits.blogs.nytimes.com>.

306 John Rollins Congressional Research Service (CRS) Report for Congress *Fusion Centers: Issues and Options for Congress* (updated 18 January 2008) Summary, 5 <www.fas.org>. See summary at *Opencrs.com* <www.opencrs.com>. Fusion Center Guidelines – Law Enforcement Intelligence, Public Safety and the Private Sector (August 2005) at 25 <www.fas.org>.

307 National Criminal Intelligence Sharing Plan (October 2003) <www.iir.com>.

308 For a map of fusion centres see <www.aclu.org>.

information, the involvement of the federal government, and the hundreds of millions of dollars of federal and state funding, was.[309]

In addition to accessing common commercial databases, different state fusion centres also access specific records databases, for example, credit reports, cell phone, unlisted and unpublished telephone numbers, and car-rental databases. Other states, use general data brokers like Entersect, which has 12 billion records on approximately 98 per cent of the American population.[310]

With a 2005 report suggesting that the establishment of fusion centres is a top priority for many states (some put the number at 70),[311] the need for some overarching framework was becoming increasingly apparent. In 2005, the US Departments of Justice and Homeland Security joined forces and produced the advisory Fusion Center Guidelines.[312]

While the Guidelines are a step in the right direction, concerns linger. Lack of transparency, accountability, ongoing reliance on inaccurate data, and exemptions from the Privacy Act, are still unresolved issues.[313] Civil libertarians are joined in some of their concerns by the Congressional Research Service, the investigative arm of Congress, which recently reported on fusion centres and their potential risks to civil liberties. Those concerns included "mission creep," the very real possibility of the investigations exceeding their parameters, lack of transparency (many have not engaged in public outreach and their agenda remains a mystery), and the violation of civil liberties, including "investigating" those who may merely be exercising their first amendment rights.[314] Moreover, there is an inherent lack of oversight and even a lack of understanding as to whom that duty falls. Is it the state or the federal government?[315] Although the Guidelines have a section

---

309 Brief of Amici Curiae Electronic Privacy Information Center (EPIC), Privacy and Civil Rights Organizations, and Legal Scholars and Technical Experts in Support of Petitioner in the *Herring v United States of America* case no 07-513 ("Concerning a Faulty Arrest Based on Incorrect Information in a Government Database") 9-13, argued in the US Supreme Court on 7 October 2008 <www.epic.org>. See also Rollins CRS Report for Congress on *Fusion Centers*, above n 306.

310 Robert O'Harrow Jr "Centers Tap into Personal Databases" (2 April 2008) <www.washingtonpost.com>.

311 Joshua Rhett Miller "'Fusion Centers Expand Criteria to Identify Militia Members" (23 March 2009) < www.foxnews.com>.

312 Fusion Center Guidelines – Law Enforcement Intelligence, Public Safety and the Private Sector, above n 306, at 1.

313 See EPIC Web page on Information Fusion Centers and Privacy <www.epic.org>.

314 Rollins CRS Report for Congress on *Fusion Centers*, above n 306, at 10-14.

315 Ibid.

dedicated to privacy and the FIPPs principles,[316] concern remains that what is offered with one hand[317] will be taken away by the other. (More on that below.)

One early example of a fusion centre project was the Department of Defense Total Information Awareness (TIA) project headed by Admiral John Poindexter, former National Security Advisor to President Reagan. (The name was later changed to Terrorism Information Awareness in a bid to quell concerns raised by civil libertarians). Although launched in 2002, it was based on programmes started during the Clinton administration. TIA was an attempt to collect in one database as much information as possible (about everyone), and then develop data mining tools to find patterns and associations in the data.[318] Outcries from the public and Congress resulted in Congress withholding its funding and shutting it down in 2003.[319] It is suspected that this programme may have moved underground and is continuing to operate.[320]

Another early post-9/11 fusion centre project was the US$12 million federally-funded Multistate Anti-terrorism Information Exchange (MATRIX) project.[321] A co-operative project between the State of Florida and private company, Seisint, its goal was to compile public and private records into a prototype database system with data mining capability. As with TIA, when the public became aware of the project, pressure forced participating states to withdraw from it.[322] While we will undoubtedly be reading more about fusion centres in the future, they have already caught the eye of the press.[323]

---

316 Ibid, Guideline 8, at 49.

317 DHS Privacy Officer "*encourages* fusion centers to implement the guidelines … [i]n particular Guideline 8 ["Develop, publish and adhere to a privacy and civil liberties policy"] *recommends* a number of elements fusion centers should include in their privacy policies." (Emphasis added) Hugo Teufel III, Chief Privacy Officer, DHS *Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative* (11 December 2008) <www.dhs.gov>.

318 See Web page on Information Fusion Centers and Privacy <www.epic.org>, above n 313.

319 Roy Mark "Wyden: No Funding for Total Info Awareness Program: Senator Amends Spending Bill to Eliminate Budget of Controversial DARPA Project that is Developing a 'Virtual Centralized Grand Database' on Americans" (16 January 2003) <www.internetnews.com>.

320 Adam Mayle and Alex Knott "Outsourcing Big Brother: Office of Total Information Awareness Relies on Private Sector to Track Americans" (17 December 2002) *The Center for Public Integrity* <web.archive.org >. See also "Gov't Quietly Brings Back Total Information Awareness" (3 June 2004) < www.democracynow.org>.

321 Jeffrey W Seifert CRS Report for Congress *Data Mining and Homeland Security: An Overview* (updated 27 August 2008) 17 <www.assets.opencrs.com>.

322 See web page on Information Fusion Centers and Privacy <www.epic.org>, above n 313.

323 Miller "'Fusion Centers Expand Criteria to Identify Militia Members," above n 311; O'Harrow Jr "Centers Tap into Personal Databases," above n 310; Julian Sanchez "DHS Report Surveys Fusion Center Privacy Concerns" (26 December 2008) <www.arstechnica.com>.

Lastly, a DNA database concept was not unique to the UK. In addition to the Combined DNA Index System of the Federal Bureau of Investigation (FBI) – which in 2007 had more than 4.7 million DNA profiles[324] – the latest FBI effort, expected to be online next year, will include not only DNA, but fingerprints, and iris scans.[325] This latest effort is in co-operation with the Departments of Defense and Justice, all but ensuring access for military and criminal law enforcement purposes. Moreover, future access may not be limited to just these agencies and departments in the United States. (See below.)

3 Australia –Sampling soldiers

Controversial programmes were not limited to the northern hemisphere. In 2007, the Australian Department of Defence was constructing a DNA database for Australian service men and women. Although the collection of information for this database was on a voluntary basis, criticism has been levelled that it was voluntary only to the extent that any instruction in the military is "voluntary."[326]

4 New Zealand –DNA and other databases

New Zealand also has DNA databases, but these existed prior to 9/11. One of them comprises 115,000 DNA profiles, 25,000 of which belong to unknown persons, retrieved from unsolved crime scenes. This information is highly guarded; police do not have direct access to it. Only 40 persons are cleared for access. Not surprisingly, there has only been one recorded disclosure breach, and that was only recently.[327]

Current law allows DNA samples to be taken from someone convicted of an offence with more than a seven-year sentence. It must be destroyed if a person is acquitted. Sixty-five per cent of DNA samples are received voluntarily and remain on the database. At the time of writing, there is legislation pending that would allow police to take DNA from anyone, regardless of the nature of the offence.[328]

---

324 Declan McCullagh "Global police database for fingerprints, airline data?" (13 July 2007) < www.zdnet.com.au>.

325 Kim Zettner "FBI 'Going Dark' with New Advanced Surveillance Programme" (11 May 2009) < www.wired.com> (accessed 21 July 2009).

326 Marcus Browne "Defence Force to Set Up DNA Database" (1 November 2007) <www.zdnet.com.au>.

327 Britton Brown "Diversion Offered over Alleged ESR DNA Security Breach" (5 June 2009) *The Dominion Post* Wellington <www.stuff.co.nz> (accessed 21 July 2009).

328 Ibid.

New Zealand also has a newborn DNA database started in the 1960s (which the Health Ministry is reviewing at the request of the Privacy Commissioner).[329] There is also a new, publicly accessible database of the country's worst criminal offenders, with 90 names on it as of April 2009.[330]

5 *Global databases*

In addition to national databases warehousing personally identifiable information, and regional databases,[331] there are new efforts to share this information and establish global databases. In 2007, the global G8[332] DNA database became active. It allows nations to share DNA profiles. As of 2007, it contained 65,000 to 70,000 profiles. And more recently, as mentioned above, the FBI is going global with its programme to track down criminals and terrorists by housing iris scans, fingerprints and palm prints of not only millions of criminals, but also of *suspects*. The United States, the United Kingdom, Canada, Australia and New Zealand have already formed an International Information Consortium working group regarding this programme.[333] Also in 2007, and independent of its other arrangements with the United States, New Zealand signed an information-sharing agreement to access a United States terrorist database.[334]

And then there are the Interpol databases. Interpol, "the world's largest international police organisation,"[335] was created in 1923 to assist cross-border police co-operation to combat and prevent international crime. It consists of 187 member countries, including the US, UK, Australia

---

329 "Newborn DNA Samples Rarely Used – Police" *The New Zealand Herald* (Auckland, 26 November 2008) <www.nzherald.co.nz>.

330 "A New Online Database Offers New Zealanders Free Access to the Country's Worst Criminals' Histories" *DataProtectionReview.eu* (22 April 2009) <www.madrid.org> (accessed 21 July 2009).

331 Some examples of regional databases include: Schengen* Information System (SIS) and second generation SIS II (EU immigration and border control database), Eurodac (database to identify Member States responsible for examining an asylum request), Visa Information System (VIS) (a database in development, which will include every visa application, including decisions rendered on each application). See Evelien Brouwer *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff Publishers, Leiden, The Netherlands, 2008) at 1-2.

*Schengen is a town in Luxembourg and is also the name given to the common territory of 25 European countries (22 EU and 3 non-EU – Iceland, Norway and Switzerland), eliminating borders in those countries. EU member states the UK, Ireland, Romania, and Bulgaria are not members of Schengen. For more information see <www.euroskop.cz>.

332 The UK, US, Canada, France, Germany, Italy, Japan, and Russia.

333 "NZ Police May Join FBI Network" *The Dominion Post* (Wellington, 1 January 2009) <www.stuff.co.nz>; Elizabeth Binning "NZ may join FBI-led global database to fight crime, terror" *New Zealand Herald* (Auckland, 16 January 2008) <www.nzherald.co.nz>.

334 "NZ Signs Up to US Terrorist Database" *The Dominion Post* (Wellington, 18 October 2007) < www.stuff.co.nz>.

335 See <www.interpol.int>.

and New Zealand.[336] It has databases for DNA, fingerprint and photo sharing, and has floated proposals for sharing all airline passenger data, convicted terrorist data, fingerprints of all arrestees, and most recently, automated face-recognition records.[337] In 2007, the United States began checking foreign travellers' details against Interpol's stolen passport database, which at the time contained 6.7 million passports. Through bilateral arrangements, the United States has access to 4.3 million records.[338] Other nations' co-operation with Interpol has been patchy.[339]

6 *How the world stacks up on privacy*

The rash of recent press reports on governments losing personal data have undoubtedly helped contribute to one human rights group giving poor privacy rankings to many countries, including the above four.[340] While Privacy International may have its critics regarding the assessment criteria it uses, it nonetheless provides some indication of countries' comparative privacy rankings. In 2007, Privacy International gave the UK the lowest grade (1 out of 5) on 9 out of 14 possible criteria relating to privacy. Five of those criteria involved data privacy: data-sharing, communication interception and communication data detention, surveillance of "medical, financial and movement", border and trans-border issues. Its median grade across all 14 data fields was 1.4. The criterion of government access to data received the marginally higher rating of 2. By comparison, the EU received only slightly higher rankings, scoring 2.3 out of a total 5. Overall, the UK ranked 43 out of a total 46 countries on privacy protection.

The US' privacy protection ranking was only slightly higher than the UK's at 1.5.[341] This is not surprising considering its refusal to overhaul privacy legislation, despite ongoing calls for reform,[342]

---

336 For a complete list of member countries, see <www.interpol.int>.

337 McCullagh, above n 324. See also Lewis Page "Interpol Proposes World Face-recognition Database: Old Skool Mugshot Files Too Slow, Say Globocops" (20 October 2008) <www.theregister.co.uk>.

338 Spencer Hsu "U.S. to Use Interpol Passport Database for Screening" *Washington Post* (6 May 2007) < www.washingtonpost.com>.

339 Brett Winterford "Australia Shares Very Little Biometric Data" (28 May 2009) <www.itnews.com.au>; "UK Counter-terrorism 'in Wrong Century'" (10 July 2007) <www.abc.net.au> (both accessed 22 July 2009).

340 See S A Matheison "UK Loses Data on 25 Million Britons" (20 November 2007) < www.computerweekly.com>; Tom Espiner "U.K. Government Loses Data on Driving-test Candidates" (18 December 2007) <www.news.cnet.com>; "Data Loss Examples in 2008" (7 January 2009) < www.whereismydata.wordpress.com>; Iain Thomson "US Government Loses Nuke Computer" (13 February 2009) <www.v3.co.uk>; J R Raphael "Lost Hard Drive and Other Government Data Blunders: The U.S. Government Has Lost a Hard Drive, but it Isn't the First to Screw Up with Data" (21 May 2009) < www.computerworld.com.au> (accessed 17 August 2009).

341 Privacy International "National Privacy Ranking 2007 – Leading Surveillance Societies around the World" <www.privacyinternational.org>.

and the implementation of a number of new programmes, including border searches of laptops, cell phones, and flash drives.[343] Both the UK and the US ranked among the worst countries in the world on nine privacy criteria.[344]

Australia's total Privacy International grade for 2007 was 2.2. New Zealand's was only slightly higher, and exactly the same as the EU, at 2.3. Australia received three dishonourable mentions in the fields of constitutional protection, surveillance of "medical, financial and movement" and border and trans-border issues. By comparison, New Zealand was only listed once on the world's worst countries list regarding communication interception.[345]

To put these numbers in perspective, the country with the highest score of 3.1 was Greece, followed by a tie for second with a score of 2.9 for Canada, Romania and Hungary. These lofty scores may just be temporary. Greece recently enacted laws approving a DNA database and camera surveillance.[346] Tied for last place with a score of 1.3 were Malaysia, China and Russia.

While these databases may have been started with the best of intentions, civil liberty challenges are unavoidable. As we have seen, they have already begun.[347] Fallout, both for the databases and civil liberties, is inevitable. Throughout history, whenever new technologies or capabilities emerge, a balancing of benefits and detriments inevitably ensues. While it is too soon to speculate on the future of these databases, there have been others in place since at least 2001 that have been (and continue to be) challenged, and that may provide insight into where these efforts may be headed.

D Technology, Terrorism and Privacy

The effect the bombings had on both sides of the world was plainly evident in the instruments that were enacted and the actions that were taken in response. Acting of their own volition, as well as in compliance with the UN resolutions, two prevalent efforts concerned (1) pre-screening airline passengers before boarding, (2) intercepting communications to find terrorists, and (3) stopping the funding of terrorism. Like the Council of Europe and EU, the UK, US, Australia and New Zealand

---

342 See Center for Democracy & Technology proposal to reform the federal Privacy Act and bring it into the 21st century <www.cdt.org> (last accessed 18 July 2009).

343 Declan McCullagh "Homeland Security: We Can Seize Laptops for an Indefinite Period" (1 August 2008) < www.news.cnet.com>. For information on the US government's border search policy see <www.cdt.org>.

344 The 14th field, "Democratic Safeguards", was not analysed.

345 See Privacy International National Privacy Ranking 2007, above n 341.

346 Mathias Vermeulen "Greece Approves DNA Database and Surveillance Camera Law" (24 July 2009) *The Lift: Legal Issues in the Fight Against Terrorism* <www.legalift.wordpress.com> (accessed 2 August 2009).

347 See also Web page regarding the Fusion Center Secrecy Bill lawsuit, *EPIC v the Virginia Department of State Police, et al,* Case No 08-01357 (Virginia General District Court filed March 12, 2008) < www.epic.org>.

all created or amended laws to support these efforts, (see attached Table 2), with significant implications for personal data privacy. Many of the programmes were steeped in controversy. Some have been (and still are) the subject of litigation. One of the first of these controversial programmes was created by the United States.

1 Accessing passenger data post-9/11 (APIS)

In the wake of 9/11, President Bush issued a number of Executive Orders (some secret) and Congress enacted laws (some retroactive) to give the President the power to fight terrorism without delay. One of the first public orders was Executive Order 13228 of 8 October 2001, which established the Office of Homeland Security (DHS) and the Homeland Security Council. Chief among Homeland Security's list of duties was the detection and prevention of future terrorist acts on American shores.[348]

> The Office shall … facilitate the exchange of information among such agencies relating to immigration and visa matters and shipments of cargo; and … ensure coordination … to prevent the entry of terrorists and terrorist materials and supplies into the United States and facilitate removal of such terrorists from the United States, when appropriate; ….

To identify future terrorists before they arrived in the United States would require that visitors be pre-screened.

The new application of data mining technology, coupled with the additional authority granted by a raft of post-9/11 legislation, resulted in the government's access to, and review of, vast databases of information in the name of stopping the "war on terror" – the term coined to encompass the United States' response to 9/11.

Before 9/11, people travelled into the United States with little restriction, although the provision of some personal data was not uncommon, if for no other reason than to confirm visa status.

The Advance Passenger Information System (APIS), developed in 1988,[349] contains personal information on travellers (and airline crew) that enter (or fly over) the United States. Information was provided by airline carriers on a voluntary basis to government border agents,[350] and consisted

---

348 Executive Order 13228 of 8 October 2001 Establishing the Office of Homeland Security and the Homeland Security Council (10 October 2001) 66 Federal Register vol 196 <www.frwebgate.access.gpo.gov>. Not to be confused with the Homeland Security Act of 2002 (US), which outlined how (and with how much money) the Office (now Department) of Homeland Security would do its job.

349 United States and European Union Passenger Name Record (PNR) Joint Review (September 20-21, 2005) at 8 <www.eff.org>.

350 US Customs and Border Protection (CBP), part of DHS, is the entity now handling APIS passenger data. DHS now includes the Customs Service and some functions of the former Immigration and Naturalisation Service (INS). Prior to 9/11, the APIS system was operated by Customs, INS and the Federal Aviation Administration. For more information see <www.answers.com>.

of 22 data elements, including passport details and flight information. Other items included information usually provided by passengers on arrival, including country of residence and address while visiting the United States.

With the signing into law of the Aviation and Transportation Security Act (ATSA) on 19 November 2001,[351] provision of APIS data became mandatory, not just for airline carriers coming to and departing from the United States, but seagoing vessels as well.[352] Details of passengers travelling by rail or bus continues to be provided on a voluntary basis only.

Other countries have begun adopting similar requirements. For example, most EU countries, 10 Caribbean countries, Australia, Spain, and Canada also require APIS data from air carriers. And starting in 2004, the UK began using Project Semaphore (the pilot project of its e-Borders programme), requiring all air, sea, and rail carriers to collect passenger information before arriving in or departing from the UK.[353] Although New Zealand provided APIS data on all passengers and crew only if requested, it is actually checking everyone.[354]

(a) What is PNR data?

Passenger Name Record (PNR) is data in computer reservation system databases developed by airlines and later used by travel agents. It overlaps somewhat with APIS, but also contains new categories of information, including itineraries, the name of the person making the booking, form of payment used, further contact details, frequent flyer data, and any comments logged into the database, such as "VIP." A number of countries, including, Canada,[355] Australia,[356] and New

---

351 Aviation and Transportation Security Act 2001 (US), Pub Law No 107-71 ss 115(2) and (3), and 136(2), 115 Stat 597, 636-37 amending 49 USC 4909(c)(3), (2001). Enacted just over two months after 9/11, it required airline carriers arriving into and departing from the United States to provide passenger and crew information to border security personnel to check it against US government consolidated watch lists of known and suspected terrorists. See <www.tsa.gov>. For more information see Department of Homeland Security, Office of the Secretary, Privacy Act of 1974(US), above n 2; Customs and Border Protection Advanced Passenger Information System of Records (18 November 2008) 73 Federal Register 223 < www.edocket.access.gpo.gov>.

352 Aviation and Transportation Security Act, above n 351, s 115, amending 49 USC 44909(c)(1)-(2).

353 Report on Article 29 Working Party Workshop on an EU Approach towards a New Passenger Data Agreement 3 (26 March 2007) Brussels <www.ec.europa.eu>. For stages of the programme's roll-out, see the Home Office Border Agency website regarding the e-Borders programme < www.ukba.homeoffice.gov.uk>.

354 Immigration Act 1987 s 125AA. See also 11 May 2005 National Air Carrier Association presentation regarding APIS World Customs Organisation/International Civil Aviation Organisation/International Air Transport Association (WCO/IATA) standards (endorsed by UN's International Civil Aviation Organization ICAO) <www.naca.cc>.

355 Aeronautics Act (Can) RS 1985, CA -2, ss 4.81 and 4.82 <www.laws.justice.gc.ca>.

356 Customs Act 1901 s 64AF (Cth) <www.austlii.edu.au>.

Zealand,[357] have enacted legislation requiring airlines to send PNR data to them on request. The UK began using PNR data through its e-Borders programme in 2009.[358] The United States made provision of PNR data mandatory from 1 January 2003.[359] (The US has been providing PNR data voluntarily since 1997.)[360]

(b) What are APIS and PNR used for?

In 2004, the "most comprehensive reform of the US Intelligence Community since its establishment over 50 years ago"[361] was enacted. Among other things, the 236-page Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)[362] created the position of Director of National Intelligence (DNI) to head the intelligence community and direct a national intelligence programme. Its explicit mandate was to create an "information sharing environment." In late 2005, President Bush enacted Executive Order 13388 that created the Information Sharing Environment Program, putting the DNI in charge.[363]

IRTPA also created the Privacy and Civil Liberties Oversight Board within the Executive Office of the President. The Board's duties are to advise the President and department heads of the Executive Branch of any impact the implementation of laws and policies may have on privacy and civil liberties. Departments and agencies are to comply with requests for information unless the DNI (in consultation with the Attorney General) determines that information must be withheld on national security grounds. The Attorney General may also withhold information on sensitive law enforcement and counterterrorism matters or ongoing operations independently. The Board comprises a chairman, vice chairman and three others, all appointed by the President. The chair and vice chair must be confirmed by the Senate. The Act also suggests that each executive department or agency should have a privacy and civil liberties officer.

---

357 Immigration Act 1987 s 125AD.

358 The Immigration and Police (Passenger, Crew and Service Information) Order 2008 (UK), Schedule 2 < www.opsi.gov.uk>; UK Home Office Border Agency website <www.ukba.homeoffice.gov.uk>.

359 Enhanced Border Security and Visa Entry Reform Act Pub Law 107-173, 116 Stat 543 s 402 (14 May 2002) <www.frwebgate.access.gpo.gov>.

360 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection, Automated Targeting System, System of Records (6 August 2007) 72 Federal Register 150 43650-56 < www.dhs.gov>.

361 Ed Terrance Paulson *Intelligence Issues and Developments* (Nova Science Publishers, New York, 2008) at xi.

362 Intelligence Reform and Terrorism Prevention Act of 2004 (also called the National Security Intelligence Reform Act of 2004) 50 USC 401 (2004) s 4012.

363 Executive Order 13388 of 25 October 2005 Further Strengthening the Sharing of Terrorism Information to Protect Americans 3 CFR 13388 (2006) <www.fas.org>.

With the mandate now official, and an oversight board now in place, information began to be shared at unprecedented rates. Starting with the expansion of old government "systems of records" as defined under the Privacy Act (like APIS), and the creation of new ones.

In 2007, APIS was given an extensive mandate:[364]

> The purpose of the information collection is to screen passengers and crew members arriving from foreign travel points and departing the United States to identify those persons who may pose a risk to border, aviation or public security, *may be a terrorist or suspected terrorist or affiliated with or suspected of being affiliated with terrorists*, may be inadmissible, may be a person of interest, or may otherwise be engaged in activity in violation of U.S. law, or the subject of wants or warrants.

In 2008, the United States had access to both APIS and PNR information to pre-screen international flights against two sublists of the consolidated terror watch list maintained by the FBI's Terrorist Screening Center: the "No-fly" list and the "Selectee" list.[365] The No-fly list has approximately 2,500 individuals on it, and the Selectee list (persons undergoing secondary inspection) contains approximately 16,000, including those on the No-fly list.[366]

The FBI sends these two sublists to Transportation Security Administration (TSA), which forwards them to airlines for pre-screening before departure. Once flights are en route, the US Customs and Border Protection (CBP) performs a second check to prepare for passenger arrivals. The consequences for missing someone on the list have resulted in flights being diverted to different destinations.[367] In 2005, six major international flights suffered that fate.[368] In accordance with the revised APIS mandate above, these lists were now to be used to identify anyone suspected of being a terrorist, affiliated with, or suspected of being affiliated with, terrorists.

In early 2007, the consolidated watch list contained over 700,000 names, which is not the actual number of individuals on the list since it also includes aliases. According to a report by the Inspector General of the Justice Department in September 2007, names were being added at the rate of 20,000

---

364 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; Customs and Border Protection Advanced Passenger Information System Systems of Records, above n 2. See also DHS, US Customs and Border Protection *Privacy Impact Assessment for the Advance Passenger Information System* (8 August 2007) 4 <www.dhs.gov>. (Emphasis added.)

365 Wyatt Kash "IT Snags Slow Secure Flight" (18 January 2008) <www.gcn.com>.

366 See the Transportation Security Administration website <www.tsa.gov>.

367 See Eileen R Larence, Director Homeland Security and Justice Issues, testimony before the Committee on Homeland Security and Governmental Affairs, US Senate *Terrorist Watch List Screening: Recommendations to Enhance Management Oversight, Reduce Potential Screening Vulnerabilities, and Expand Potential Use of the List* (24 October 2007) at 11-12 <www.gao.gov>.

368 House of Representatives Committee on Homeland Security *The State of Homeland Security 2006: An Annual Report Card on the Department of Homeland Security* (2006) 9 <www.homeland.house.gov>.

per month.[369] However in late 2007, the list was reduced to approximately 400,000 unique individuals after a "name-by-name scrub."[370] The details on this list are also shared with other countries.[371]

Individual countries also have their own, although significantly smaller, lists. Opinions differ on the actual number of persons on them. For example, in 2006, independent of those on the designated UN terrorist list, Australia had either 4 or 88 people on its list; Canada either 24 or 50.[372]

(c) Passenger pre-screening programmes

In the United States, Transportation Security Administration is slowly taking over the pre-screening function from the airlines under a new programme called "Secure Flight" (see below). This is not the first proposed pre-screening programme to be administered by TSA and its predecessors.[373]

(i) CAPPS

Computer Assisted Passenger Pre-Screening (CAPPS) has been in use since 1998. It involves pre-screening passengers using databases that contain, among other things, address, travel history and criminal records. It was in use on 9/11.

Michael Tuohey, a US Airways customer service representative, recalls checking in Mohammed Atta and Abdulazziz al Omari (two of the highjackers) onto a flight from Portland, Maine to Boston Logan Airport on the morning of 9/11. The PNR record confirms this. Mr Tuohey recalls that there was nothing suspicious about them, but he did remember them. They had one-way, first class tickets from Boston to Los Angeles, were running late, and Atta was angry that he was going to have to go through a second check-in in Boston; al Omari did not appear to speak English.[374] It does not seem

---

369 United States Department of Justice Office of the Inspector General Audit Division *Follow-up Audit of the Terrorist Screening Center* Audit Report 07-41, iii (September 2007) <www.usdoj.gov>.

370 See Transportation Security Administration website <www.tsa.gov>, above n 366. See also FBI "Letter to the Editor Regarding the Terrorist Watch List" (1 July 2009) Press Release <www.fbi.gov> (accessed 31 July 2009).

371 "NZ Signs Up to US Terrorist Database," above n 334.

372 See the website tracking the New Zealand parliament's debate on terrorism/border control (14 June 2006) < www.theyworkforyou.co.nz>. These numbers are in addition to the designated terrorists on the UN's list, which all countries are obliged to monitor. For a list comparing EU, UN, UK US terrorist designations see < www.statewatch.org>. The Consolidated UN list is the most updated (the last update was on 20 July 2009). It is 74 pages long: in addition to names and other identifying criteria, it also lists the individual's status. Some of those on the list are already incarcerated or have died.

373 *The 9/11 Commission Report* 1, above n 6.

374 Michael Smerconish "He Looked Terror In The Eye – And Blinked" (24 February 2005) *Philly.com* < www.web.archive.org>. Interview with Michael Tuohey, former US Airways Customer Service Representative (Interview Memorandum, 27 May 2004) prepared by John Raidt <www.911myths.com>.

that they were on the Selectee List because, according to Mr Tuohey, had they been identified by CAPPS as selectees, their checked bags would have been kept off the airplane until confirmation that the owners of the bags were onboard. Mr Tuohey did not recall the bags being hand-searched.[375] Atta was, however, randomly selected for additional screening by CAPPS.

Remarkably, nine highjackers on four of the five flights involved in the 9/11 attacks were selected for additional screening.[376] At that time, being selected for additional screening or being on the selectee list only meant that checked luggage went through additional screening. Conforming to intelligence risk analysis of the day that bombs were the biggest threat to security, neither persons nor hand luggage received additional scrutiny.[377] Two of the highjackers were on the No-fly list but because the Federal Aviation Administration was not provided with their names, they were not flagged.[378]

(ii) CAPPS II

In light of 9/11 and the failures of the pre-screening system in place at the time, a new programme focusing more on passengers than luggage was unveiled. Launched in 2003, CAPPS II was more of a profiling programme, and involved pre-screening passengers and giving them a low-, medium- or high-risk score based on information in commercial, law enforcement, and intelligence databases. CAPPS II did not become active largely because of the outcry from civil liberty organisations (both in the United States and abroad), and the fact that it failed to meet seven out of eight government accountability criteria in 2004, prerequisites to receiving funding from Congress.[379] The only criterion it did meet was the establishment of an internal oversight board to monitor development of the system.[380] More than US$100 million was spent on the programme,

---

375 Ibid, interview with Michael Tuohey, former US Airways Customer Service Representative.

376 All five highjackers on American Airlines Flight 77, three of the five highjackers on American Airlines Flight 11 (including Atta and al Omari), and one highjacker on United Flight 93 were selected for additional screening.

377 *The 9/11 Commission Report*, above n 6 at 6-7.

378 Ibid, at 11.

379 Accuracy of data, stress testing, abuse prevention, unauthorised access prevention, policies for operation and use, privacy concerns, and redress process.

380 For more information see the websites for Department of Homeland Security <www.dhs.gov>, Electronic Frontier Foundation <www.eff.org>, and <www.privacyactivism.org>. See also United States General Accounting Office *Report to Congressional Committees – Aviation Security: Computer-Assisted Passenger Pre-screening System Faces Significant Implementation Challenges* (February 2004) <www.gao.gov>; "GAO Report Finds CAPPS II Fails to Meet Congressional Criteria" *Tech Law Journal* (13 February 2004) <www.techlawjournal.com>; and Ryan Singel "Life After Death for CAPPS II?" (16 July 2004) < www.wired.com>.

before TSA finally stopped it in mid-2004.[381] Speculation on whether a CAPPS III programme was waiting in the wings did not last long.

(iii) ATS

Around August 2004, DHS extended to passengers the Automated Targeting System (ATS), already in use to screen seagoing cargo containers. This extension of ATS capability did not come to light until November 2006, when DHS published a System of Records Notice to that effect.[382]

ATS, with its six enforcement screening components, is one of many modules of the Treasury Enforcement Communications System (TECS or TEC system). TECS is both a repository of information and a law enforcement tool that collects data, and analyses risk in an "information sharing environment."[383] TECS is still in use.

On 19 December 2008, CBP published a new notice[384] regarding its plans to take TECS over from the Treasury Department and consolidate into this system of records other Treasury and Justice Department databases, including the Currency Declaration File,[385] Suspect Persons Index,[386] the National Automated Immigration Lookout System (NAILS)[387] and the Warnings to Importers in

---

381 House of Representatives Committee on Homeland Security *The State of Homeland Security 2006: An Annual Report Card on the Department of Homeland Security*, above n 368, at 57. See also Noah Shachtman "The Man Who Helped Kill CAPPS II" (19 July 2004) <www.wired.com>.

382 Department of Homeland Security (DHS), Office of the Secretary, Privacy Act of 1974 (US), above n 2; System of Records regarding the Automated Targeting System (2 November 2006) 71 Federal Register 212 64543-46 <www.edocket.access.gpo.gov>. Peter Hobbing *Tracing Terrorists: The EU-Canada Agreement in PNR Matters – CEPS Special Report* (September 2008; revised 17 November 2008) 14 <www.ceps.eu>.

383 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection, Automated Targeting System, System of Records (6 August 2007), above n 360. See also, above n 362, IRTPA s 1016(a)(2).

384 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection – 011 TECS System of Records Notice (18 December 2008) 73 Federal Register 245 77778-77782 < www.edocket.access.gpo.gov>.

385 Currency Declaration File: individuals covered by this system include those "departing from or entering the country who filed IRS Form 4790." Records in the system include: "Name, identifying number, birthdate, address, citizenship, visa date and place, immigration alien number, kinds and amounts of monetary instruments, address in the United States or abroad, passport number and country, and arrival or departure information." See <www.data-detective.com>.

386 Suspect Persons Index: individuals covered by this system include those "suspected of violation of Customs Laws." Records in the system include: "Name and related file number." See <www.data-detective.com>, above n 385.

387 The Immigration and Naturalization Service Index System consists of the following subsystems: Examinations Indexes: Service lookout system. Individuals covered by this system include: "1. Application and petition index: Individuals who have filed or assisted in filing petitions to classify aliens for the issuance of immigrant visas; 2. Correspondence control index: Members of the general public; 3. Service lookout

Lieu of Penalty.[388] It is CBP's "principal law enforcement and anti-terrorism database."[389] TECS was used to identify one person in particular in 2002 with disastrous consequences both for that individual and the government of Canada. (See below.) The Canadian Police Information Centre (CPIC), among others, has direct access to TECS.[390]

Automated Targeting System-Passenger (ATS-P), operational as of 1999, is the component that maintains PNR data. ATS-P "allows officers to determine whether a variety of potential risk indicators exist for travelers and/or their itineraries that may warrant additional scrutiny."[391]

ATS had nothing to recommend it over CAPPS II. Its techniques were considered imprecise and its implementation was denounced by privacy advocates as extremely risky in its then state of development, especially in light of the exemptions from the Privacy Act principles that DHS published on the programme.[392] (See below.) Privacy advocates weren't the only ones dissatisfied with its performance. In its 2006 report, the House Homeland Security Committee[393] gave ATS a mark of C-/D+ in its ability to detect suspect cargo.[394]

Exemptions from the Privacy Act for the ATS system (which the Act allows law enforcement agencies to claim) initially included:

- Access to and amendment of incorrect information (FIPPs Access and Correction Principle and Collection Limitation Principle); and

---

system: Violators or suspected violators of the criminal or civil provisions of statutes enforced by INS." See <www.data-detective.com>, above n 385.

388 Warnings to Importers in Lieu of Penalty: Individuals covered by this system include "[i]ndividuals and firms in violation of Customs's laws." Records in the system include "[b]rief record of violation and warning." See <www.data-detective.com>, above n 385.

389 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection – 011 TECS System of Records Notice (18 December 2008), above n 384.

390 Ibid.

391 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection, Automated Targeting System, System of Records (6 August 2007), above n 360.

392 See a 2007 post regarding the ATS system at <www.epic.org>.

393 The House of Representatives Homeland Security Committee, created in 2002, is a bipartisan committee tasked with overseeing DHS. See <www.homeland.house.gov>. The Senate Committee on Homeland Security and Governmental Affairs, whose origin traces back to the 19th century, is also a bipartisan committee with jurisdiction over the creation of DHS. It is the chief supervisory committee for the Senate. See <www.hsgac.senate.gov>.

394 House of Representatives Committee on Homeland Security *The State of Homeland Security: An Annual Report Card 2006* 1-4, above n 368. See also Peter Hobbing *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, above n 382, at 14.

- Relevant and necessary information (FIPPs Purpose/Use Limitation Principle).[395]

In response to early criticisms, DHS announced significant system changes in August 2007, including a redress procedure.[396] Although it added this new protection, it took away others by expanding ATS Privacy Act exemptions and the number of databases from which it could access information. The additional exemptions included:

- Accuracy, timeliness and completeness of records (FIPPs Data Quality Principle)**;**
- Notification of any correction or dispute (FIPPs Transparency Principle)**;** and
- Civil remedies (FIPPs Accountability Principle)**.**[397]

Exemptions from Privacy Act protections were extended only for risk assessment analyses and business confidential information. No exemptions were made regarding PNR data about the requestor.

The new databases available under ATS-P (in addition to PNR), included APIS, the Non-Immigrant Information System (NIIS), the Suspect and Violator Indices (SAVI),[398] and the Department of State visa databases. Records could be shared with law enforcement and intelligence agencies (both foreign and domestic), and those records could be kept for up to 15 years (down from the 40 years originally), after which time they would be deleted unless "linked to active law enforcement lookout records."[399]

The purpose of ATS-P was to use data from these databases to prevent and combat terrorism and other serious crimes, "[w]herever necessary for the protection of the vital interests of a data subject or other persons" or "[a]s otherwise required by law." To accomplish this broad mandate, ATS-P compared information in the databases "against lookouts and patterns of suspicious activity identified by analysts based upon past investigations and intelligence."[400]

ATS has not disappeared.

---

395 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; System of Records regarding the Automated Targeting System (2 November 2006), above n 382.

396 Traveler Redress Inquiry Program (TRIP). See DHS, US Customs and Border Protection *Privacy Impact Assessment for the Automated Targeting System* (3 August 2007) at 22 <www.dhs.gov>.

397 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection, Automated Targeting System, System of Records (6 August 2007) above n 360.

398 Suspect and Violator Indices (SAVI) is a database with arrest and seizure information on foreign nationals from 137 countries known as the *INS I-94 Database*.

399 See also DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; US Customs and Border Protection, Automated Targeting System (6 August 2007), above n 360.

400 Ibid.

(iv) Secure Flight

Almost simultaneously with the expansion of ATS capability, DHS unveiled its newest programme, Secure Flight.[401] This US$200 million programme[402] has TSA assuming the airlines' duty to check passenger information against the No-fly and Selectee watch lists, reserving the right to compare data against larger watch lists.[403]

Secure Flight uses a combination of customer-provided data (name, date of birth, and gender), APIS data, only one PNR criterion (itinerary), and a few categories of its own reflecting redress details in the event of misidentification. According to the TSA website, "Secure Flight does NOT assign a score to individuals, use commercial data or predict behavior" (distinguishing it from the earlier CAPPS II programme).[404] But while passengers may not be assigned a "risk score," it does appear to categorise passengers as either "cleared," "inhibited" (requiring additional inspection) or "not cleared."[405] Moreover, one of the government's contractors for "next generation airline passenger screening" openly states that its software performs "identity focused analysis to … identify hidden relationship[s]" and returns scores rather than actual data to protect privacy.[406]

Secure Flight's purpose "is to identify and prevent known or suspected terrorists from boarding aircraft or accessing sterile areas[] of airports… ."[407] Under this programme, personal details are required not just of travellers, but also of any person with access to secure airport areas, for example, anyone accompanying an infirm or elderly family member to a gate.[408] Information can be

401 See Web page on Secure Flight <www.tsa.gov>. Ryan Singel "Feds Begin Post-9/11 Airline Watchlist Takeover" (1 April 2009) <www.wired.com> (accessed 31 July 2009).

402 Majority Staffs of the House of Representatives Committee on Homeland Security and Committee on Foreign Affairs *Wasted Lessons of 9/11: How the Bush Administration Has Ignored the Law and Squandered Its Opportunities to Make our Country Safer* (September 2008) at 6 < www.homeland.house.gov>.

403 DHS, Transportation Security Administration *Privacy Impact Assessment for the Secure Flight Program* (21 October 2008) at 3 <www.tsa.gov>.

404 See Web page on Secure Flight at <www.tsa.gov>, above n 401.

405 Department of Homeland Security, Transportation Security Administration *Privacy Impact Assessment for the Secure Flight Program*, above n 403, at 9, 12. See also "Secure Flight: Frequently Asked Questions" *The Identity Project* <www.papersplease.org> and "Secure Flight to Use Same Data Mining Tools as CAPPS II" *The Identity Project* (17 July 2009) <www.papersplease.org> (accessed 10 August 2009).

406 See website at <www.infoglide.com> (last accessed 10 August 2009).

407 DHS, TSA *Privacy Impact Assessment for Secure Flight,* above n 405, at 1.

408 Ibid, at 3.

shared with government agencies for law enforcement, national security, intelligence, and immigration purposes.[409]

Like APIS, TECS, and ATS before it, Secure Flight has been exempted from almost all of the same fair information principles in the Privacy Act.[410] Lengthy explanations for these exemptions include not alerting subjects to pending investigations, inability to know at the time of collection what information is relevant or necessary, and inability to ensure accuracy since many of the records on which it relies are from other databases.[411] The data of those who are cleared will be deleted seven days after travel. Potential matches will have their data kept for seven years after travel. Confirmed matches will have their data kept for 99 years after travel.[412]

Both CAPPS II and Secure Flight were the subject of investigations by Homeland Security's Privacy Officer for potential Privacy Act violations (as were some airlines involved in programme testing). Among the reasons for the investigation were failure to disclose the type of information to be used in the programmes, and the manner in which it would be used.[413]

In the case of Secure Flight, "'the public was not adequately informed that a TSA contractor obtained over 100 million commercial data records.'"[414] Later representations that Secure Flight does not use commercial data begs the question of what happened to those 100 million commercial data records.

Like APIS and ATS, Secure Flight has been the subject of Privacy Impact Assessments, most recently on 21 October 2008.[415] It has also implemented a redress system,[416] and has announced that it is regularly updating the Cleared List to clear those misidentified on the terror watch lists.[417]

---

409 Ibid, at 15.

410 DHS, Privacy Act of 1974 (US), above n 2: Implementation of Exemptions and System of Records; Secure Flight Records; Final Rule and Notice (9 November 2007) 72 Federal Register 217 63706-10 <www.tsa.gov >; 5 US Code 552a Records Maintained on Individuals <www.caselaw.lp.findlaw.com>.

411 Ibid.

412 DHS, TSA *Privacy Impact Assessment for the Secure Flight Program*, above n 403, at 14.

413 House of Representatives Committee on Homeland Security *Report on the Department of Homeland Security* (2006), above n 368, at 56. See also the Web page regarding Secure Flight at <www.epic.org>.

414 Ibid.

415 DHS, TSA *Privacy Impact Assessment for the Secure Flight Program* (9 August 2007) <www.dhs.gov>, and DHS, TSA *Privacy Impact Assessment for the Secure Flight Program*, above n 403.

416 Traveler Redress Inquiry Program (TRIP). See DHS, TSA, Privacy Act of 1974 (US), above n 2: Implementation of Exemptions and System of Records; Secure Flight Records (9 November 2007), above n 410.

417 DHS, TSA *Privacy Impact Assessment for the Secure Flight Program*, above n 415, at 14, 18.

Although the Privacy Act does not apply to non-citizens or legal residents, its administrative remedies have been extended to all visitors to the United States.[418]

As far as where ATS leaves off and Secure Flight begins, since ATS-P contains PNR data, and since Secure Flight uses PNR data, it stands to reason that the ATS database is still being used to pre-screen passengers.[419] Moreover, in its 2007 Privacy Impact Assessment ATS stated that one of its six modules, the "ATS-Passenger (ATS-P) is the module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crew members prior to arrival or departure."[420] This appears still to be the case. Why dedicate time to reviewing a programme if it is not in use? Finally, not only do ATS and Secure Flight share the same redress system (Traveler Redress Inquiry Program (TRIP)),[421] but the DHS Privacy Officer's December 2008 review of the implementation of the EU/US PNR agreement confirms ongoing staff training not only with regard to TECS but also ATS.[422]

How much PNR data will be used in future to pre-screen passengers is evident from the EU/US agreement (see below). Unless the US is planning not to apply Secure Flight to those flights falling under the EU/US agreement, that agreement presages just how expansive Secure Flight truly is. Under the EU/US agreement, all PNR data (lodged in the ATS-P database) will be used to pre-screen passengers (not just the PNR "itinerary" criterion listed on the Secure Flight website), including sensitive data and any comments made by airline staff or travel agents. Secure Flight's ability to check data against larger databases than the No-fly and Selectee lists, makes any database a candidate, including ATS-P, which houses commercial PNR data. So even though the Secure Flight programme does not officially "assign a score to individuals, use commercial data or predict behaviour", there is evidence that it is relying on programmes that do.

---

418 DHS Notice of Privacy, Office of the Secretary, Privacy Act of 1974 (US), above n 2; United States Customs and Border Protection – 011 TECS System of Records Notice (19 December 2008) 73 Federal Register 245 <www.edocket.access.gpo.gov>.

419 Letter from Michael Chertoff to Luis Amado setting forth terms of EU/US PNR agreement (26 July 2007) 3 <www.dhs.gov>. See also DHS, US Customs and Border Protection *Privacy Impact Assessment for ATS*, above n 396, and DHS, Office of the Secretary, Privacy Act 1974 (US) NZ, US Customs and Border Protection, Automated Targeting System, System of Records (6 August 2007), above n 360.

420 DHS, US Customs and Border Protection *Privacy Impact Assessment for ATS* (3 August 2007), above n 396.

421 Ibid. See also DHS, TSA, Privacy Act of 1974 (US), above n 2: Implementation of Exemptions and System of Records; Secure Flight Records (9 November 2007), above n 410.

422 DHS Privacy Office *A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union* (18 December 2008) <www.dhs.gov>.

(d) The EU and PNR

The mandatory provision of PNR data was most controversial in the EU, where the collection, use and storage of personal data is highly regulated by the EU Directive. Countries that adopted laws requiring the provision of PNR data were essentially forcing EU airlines (and any others that processed data in the EU) to risk breaching EU law if they sent data to third countries without "adequate" systems of data privacy protection under the Directive. Since the United States was the first country to demand PNR data in late 2001, that is where the showdown occurred.

(i) EU/US PNR Agreements

After the requirement to send PNR data to the United States came into effect on 1 January 2003, some European carriers began giving it to Customs (now CBP). Some even went so far as to allow CBP access to their own databases.[423] Because the carriers were concerned that their actions constituted violations of EU data privacy law, the EU Commission intervened and entered into delicate negotiations on their behalf. It negotiated with the United States to postpone fining carriers that were in violation of US law, and it negotiated with European data protection authorities to refrain from fining carriers who were co-operating with the US, potentially in violation of EU data protection law.

The United States agreed to postpone fining non-co-operative airlines, but only for a couple of months.[424] An interim agreement was worked out in which CBP agreed that until such time as there was a finding of adequacy under the EU Directive regarding the transfer of PNR data to the United States, it would operate in accordance with a certain set of "Undertakings."[425]

In the meantime recommendations were being received from European data protection authorities, and the Article 29 Working Party on the Undertakings, outlining the finer points that should be included in any future agreement. These included:[426]

---

423 Hobbing *Tracing Terrorists: The EU-Canada Agreement in PNR Matters,* above n 382, at 7.

424 Commission of the European Communities *Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach* (16 December 2003) <ww.ec.europa.eu>.

425 Those Undertakings were updated at least twice, on 22 May 2003 <www.ec.europa.eu> and 12 January 2004 <www.statewatch.org>.

426 Article 29 Data Protection Working Party *Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data* (13 June 2003) <www.ec.europa.eu>; *Opinion of the European Data Protection Authorities on the Transfer of Passengers' Data to the United States* (17 June 2003) < www.ec.europa.eu>; Article 29 Data Protection Working Party *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)* (29 January 2004) <www.ec.europa.eu>.

(1) Periodic reviews to check for compliance and to gauge whether ongoing data transmissions were necessary;

(2) No transmissions of unnecessary, sensitive data;

(3) Data to be retained for only weeks or, at most, months (not the seven or eight years requested by the United States – down from its original request of 50 years);

(4) Transfer of data on a "push" not "pull" basis (that is, carriers should provide data to the US authorities, instead of the US authorities accessing data directly from carrier databases);

(5) Purpose limited to fighting terrorism; and

(6) Independent third-party supervision.

While progress was being made in the negotiations, at least in the minds of some, an agreement was a long way off. The Article 29 Working Party was still concerned about a number of things, including the scope of purpose, proportionality, use of data in the American CAPPS II programme, passenger access, correction and redress rights, the binding legal nature of the agreement, and onward use.[427] Despite its concerns, the Article 29 Working Party's tone was hopeful. In no way was it the most vociferous opponent of the proposed EU/US PNR agreement.

The Commission sent the European Parliament a draft decision on adequacy together with the draft US undertakings, and shortly thereafter sent a proposal for a Council decision on a US/EU PNR agreement. In response, Parliament set out in a Resolution its concerns about the legitimacy of the agreement's legal basis, the proposed "pull" system for accessing PNR data, and the unilateral nature of the US undertakings. It urged the Commission to withdraw its decision on adequacy and continue negotiations with the United States.[428] As set out in a later document, its position was unequivocal:[429]

---

427 Article 29 Data Protection Working Party *Opinion 2/2004* (29 January 2004), above n 426, at 13.

428 European Parliament Resolution on the Draft Commission Decision Noting the Adequate Level of Protection Provided for Personal Data Contained in the Passenger Name Records (PNRs) Transferred to the US Bureau of Customs and Border Protection (2004/2011 (INI)) (31 March 2004) <www.statewatch.org>.

429 Rapporteur Johanna LA Boogerd-Quaak *Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, European Parliament Report on the Proposal for a Council Decision on the Conclusion of an Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection(COM (2004) 190 – C5-0162/2004—2004/0064(CNS))* 5 (6-7 April 2004) < www.epic.org>.

The European Parliament ...

1. Does not approve conclusion of the agreement;

2. Instructs its President to call on the Council not to conclude the agreement;

3. Calls on the Council to refrain from concluding this agreement until the Court of Justice has delivered its opinion on the compatibility with the Treaty (Article 300(6) of the EC Treaty);

4. Instructs its President to forward its position to the Council and Commission and the governments and parliaments of the Member States and the United States of America.

Unwavering, Parliament then asked the European Court of Justice for an opinion on the Council's failure to seek Parliament's assent on the agreement.[430] In its actions, Parliament had the support of the European Data Protection Supervisor.

Irrespective of Parliament's disapproval and request for a judicial decision, the Council went ahead with the agreement. Stating that it had "exhausted all possibilities to obtain in time the opinion of the European Parliament[,]"[431] the Council adopted its Directive on the Obligations of Carriers to Communicate Passenger Data on 29 April 2004.

The deal, it seems, had been a fait accompli. It had been given to Parliament for review in name only. Parliament had effectively been excluded from its position as co-decider under the first pillar process because the deal was structured as a "light" international agreement, which allowed the Council to relegate Parliament to no more than observer status.[432] But this was not the end of the debacle:

- 14 May 2004: the adoption of the final Commission Decision on adequacy, including a final version of CBP Undertakings, due to expire in three and a half years;[433]
- 28 May 2004: EU/US PNR Agreement signed in Washington;[434]

---

430 European Commission "Commission Secures Guarantees for Protecting Personal Data of Transatlantic Air Passengers" (17 May 2004) Press Release <www.europa.eu>.

431 Council Directive 2004/82/EC on the Obligations of Carriers to Communicate Passenger Data recital 5 (29 April 2004). <www.eur-lex.europa.eu>. The directive was to enter into force 30 days after publication, on 5 September 2004.

432 Ibid.

433 Commission Decision of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914) 2004/535/EC (14 May 2004) <www.eur-lex.europa.eu>.

434 Agreement between the European Community and the United States of American on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of

- 20-21 September 2005: limited joint review of the implementation of CBP's Undertakings in Washington;[435]
- 30 May 2006: the European Court of Justice annuls the Council's decision on the EU/US agreement and annuls the Commission's decision on adequacy on a technicality, finding they are founded on an inappropriate legal basis. Because the transfer of PNR data concerns processing operations regarding public security and criminal law (matters under the EU's second and third pillars), EU Directive 95/46 (applicable only to pillar one matters) is inapplicable. The decision took effect 30 September 2006;[436]
- 16 October 2006: Interim EU/US agreement enters into force, with 31 July 2007 expiration date;[437]
- 12 July 2007: the European Parliament adopts a Resolution expressing regret at the proposed new EU/US PNR agreement;[438] and
- 23 and 26 July 2007: the current EU/US PNR Agreement, set out in five documents, is signed. This entered into force on 23 October 2007 and expires in 2014. Detailed terms are set out in Michael Chertoff's letter to Luis Amado, incorporated by reference into the agreement.[439]

Customs and Border Protection (28 May 2004) <www.ec.europa.eu>. See also Hobbing *Tracing Terrorists: The EU-Canada Agreement in PNR Matters – CEPS Special Report*, above n 382, at 7; and Bignami "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining", above n 189, at 669.

435 Commission of the European Communities Commission Staff Working Paper on the Joint Review of the Implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004 Redacted Version (20-21 September 2005; final version dated 12 December 2005) <www.ec.europa.eu>. See also United States and European Union Passenger Name Record (PNR) Joint Review, above n 349.

436 "The Court Annuls the Council Decision Concerning the Conclusion of an Agreement between the European Community and the United States of America on the Processing and Transfer of Personal Data and the Commission Decision on the Adequate Protection of those Data" (30 May 2006) Press Release < www.europa.eu>. Judgment of the Court (Grand Chamber) in Joined Cases C-317/04 and C-318/04 paras 56-59 and 68 (30 May 2006) <www.eur-lex.europa.eu>.

437 Council Decision 2006/729/CFSP/JHA (16 October 2006) <www.eur-lex.europa.eu>.

438 European Parliament Resolution of 12 July 2007 on the PNR Agreement with the United States of America <www.europarl.europa.eu>.

439 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) (signed 23 and 26 July 2007) <www.dhs.gov>; Conferring of Full Powers to Luis Amado to sign agreement with DHS dated 23 July 2007; Letter from Luis Amado to Michael Chertoff (23 July 2007); Declaration to Agreement <www.dhs.gov>; Letter from Michael Chertoff, Secretary of Homeland Security, to Luis Amado (26 July 2007), above n 419.

While some of the terms in the latest agreement are better for the EU than under the first agreement, most are worse. Positive terms include:[440]

- Immediate transition to a "push" system for those carriers that have the technical capability to do so;
- Notice regarding access to sensitive data to be provided within 48 hours of access (although sensitive data is now accessible, unlike under the former agreement);
- Extension of administrative protections under the Privacy Act for stored data regardless of nationality.

Negative terms include:

- A "pull" system still in effect for those carriers that have not moved to a "push" system of data transmission;
- DHS is only under an obligation "to advise" the EU of any new US legislation materially affecting the agreement;
- Sensitive data can be accessed in exceptional cases (under the former agreement it used to be filtered out and deleted);
- Data to be retained for seven years (it was three and a half years from the date of access), after which it is removed to a dormant database where it will remain for an additional eight years (as in the former agreement). The deletion process to be discussed with EU at a later date (it used to be deleted after eight years unless archived in reference to a specific enforcement record);
- Periodic review by DHS and EU (it was yearly or more often on request), and no provision for review by anyone from the EU other than the Commissioner for Justice, Freedom and Security. (The prior agreement contemplated an EU review team to include authorities of Member States);
- No terms on computer system security;
- No limitation on the use of data in the CAPPS II programme (although CAPPS II is not currently in use, at least not in its earlier form).

Terms staying the same:

- Categories of PNR data to be transmitted;[441]

---

440 For more detail on the differences between the 2004 and 2007 EU/US PNR agreements, see the European Parliament Resolution of 12 July 2007, above n 438.

- Onward transfers of data solely within DHS discretion;
- Data to be used to prevent and combat terrorism as well as serious crimes and warrant violations;
- Data to be transmitted to CBP at least 72 hours before scheduled departures, with subsequent data transmissions as required.

(ii) The future of PNR agreements and data protection under the EU third pillar

As set out above, shortly after the EU/US PNR agreement was signed, DHS prepared Privacy Impact Assessments for both ATS and Secure Flight.[442] It also published notices regarding these two new "systems of records"[443] which contained exemptions from the Privacy Act. This aroused suspicion from a European watchdog that was quick to ask whether the EU knew that these exemptions were in the offing when it signed the PNR agreement with the US.[444] All references in the EU/US agreement regarding protections in the Privacy Act seemed now to ring hollow.

Despite a Privacy Act exemption regarding access and ability to correct database information, the Secure Flight programme does provide some redress mechanism with its Cleared List process. But other Privacy Act protections such as the collection and use of only relevant and necessary information, notice, disclosure, accuracy of data, and access to civil remedies, have all been exempted. Having said that, the EU/US PNR agreement provided that if the EU believed the US had breached the agreement, its remedy was to terminate, which it has not done.

In December, 2008, the DHS Privacy Officer conducted a review of CBP's implementation of the terms of the EU/US PNR agreement to check for compliance with the ATS System of Records Notice published in August 2007, and the terms of the agreement. Although DHS determined that CBP was generally in compliance, areas for improvements were noted. Findings included: no reports of PNR misuse were received since the 2005 review; staff training regarding TECS and ATS

---

441 Although the first agreement made reference to 34 categories of PNR data for transfer and the new agreement makes reference to 19, the actual content of data remains the same. Some of the 34 items were simply collapsed into others, reducing the number of items, but not the amount of data.

442 DHS, US Customs and Border Protection *Privacy Impact Assessment for the Automated Targeting System* (3 August 2007), above n 396. DHS, Transportation Security Administration *Privacy Impact Assessment for the Secure Flight Program* (9 August 2007), above n 415.

443 DHS, Office of the Secretary, Privacy Act 1974 (US), above n 2; US Customs and Border Protection, Automated Targeting System, System of Records (6 August 2007), above n 360. DHS, Transportation Security Administration, Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records (23 August 2007) 72 Federal Register 163 <www.edocket.access.gpo.gov>. DHS, Transportation Security Administration, Privacy Act of 1974: Implementation of Exemptions and System of Records; Secure Flight Records (9 November 2007), above n 410.

444 "US Changes the Privacy Rules to Exemption Access to Personal Data" *Statewatch* (September 2007) < www.statewatch.org>.

was continuing. Recommendations included: updating the FAQs and Privacy Statement to reflect the current EU/US PNR agreement (and not the 2004 agreement); improving the timeliness of responses to, and decreasing backlog of, Privacy Act and Freedom of Information Act requests; improving staff training so that Privacy Act exemptions are not inconsistently applied and search requests for information held by CBP are conducted consistently; and finally, improving record retrieval and release so that only records of those requesting them are released (not the entire group of which the requestor was a part).[445] But as clearly stated in the "areas for improvement" (and in a pointed challenge by The Identity Project to the representation that no complaints were received since 2005), compliance is still a way off.[446]

In what appeared to be a rebuttal to The Identity Project's challenges to asserted compliance, DHS Chief Privacy Officer Hugo Teufel III reiterated that while improvement could be achieved, CBP's hard work resulted in compliance with the EU/US agreement. While CBP's ongoing commitment to improve the way it handles data is commendable, its current handling of problems can only be described as compliance failings, resulting from premature deployment of the system. An agency's hard work does not compliance make. As for whether delaying the system's deployment would have been the right move or whether that would have created a tangible security risk, we will never know. What we do know is that by deploying it before it was ready, sacrifices to privacy were, and continue to be, made. Why the EU did not participate in what was supposed to be a joint review, Teufel says he does not know.[447]

The future for PNR data is far from resolved. There is still no Framework Decision (to approximate or align Member State laws) and no Directive that applies to the processing of personal data in pillar two or three in relation to third-party nations. While Framework Decision 2008/977 (see above) pertains to cross-border exchanges of data in third pillar matters, it does not apply to exchanges with non-EU members. The only overarching data protection legislation in the third pillar is Convention 108 from the 1980s. The Convention has not been updated to take into account new technologies, (or implementations of old ones, like data mining).

Technically, the agreement with the US, and others the EU has since entered into with other countries, are not even in force. (The EU also entered into a PNR Agreement with Canada in 2005, which is due to expire on 22 September 2009. Its 2008 PNR Agreement with Australia does not expire until 2015.) These agreements are only "provisionally applicable and will enter into force as

---

445 DHS Privacy Office *A Report Concerning Passenger Name Record Information* (18 December 2008), above n 422.

446 "DHS Admits Problems in Disclosing Travel Surveillance Records" (24 December 2008) *The Identity Project* <www.papersplease.org>.

447 DHS Chief Privacy Officer Hugo Teufel III "What the Passenger Name Record Report Really Says" (31 December 2008) *DHS Leadership Journal Archive* <www.dhs.gov>.

soon as all the Member States have finalised their domestic consultation procedures."[448] Practically speaking, however, all these agreements are in operation. But there is no guarantee that they won't resurface before the European Court of Justice. With the European Parliament's adoption of a Resolution expressing regret at the signing of the new EU/US PNR agreement, and its reservation of the right to challenge the legitimacy of the EU/Australia PNR agreement[449] (again, it was not consulted in those negotiations), it could happen at any time.

Other issues on the horizon include a proposed Framework Decision on EU PNR.[450] As stated above, one reason to adopt a Framework Decision is to align different Member States' laws. On the issue of PNR data, only a handful of Member States (the UK, France and Denmark) have enacted national legislation regulating its use.[451] But others are considering it (for example, Sweden and Belgium). Based largely on the EU/US model, the proposed Framework Decision is eliciting the same concerns now that the EU/US Agreement did earlier. Some Member States (and EU bodies) want to enact it, while others (the same data privacy advocates in the first debate, namely the European Parliament and European Data Protection Supervisor) are unconvinced of its effectiveness as a tool to combat terrorism, while its potential to violate fundamental rights is very real.[452] (See below.)

One proponent of an expansive EU PNR proposal is the UK. Like the US, the UK wants to use PNR data for purposes other than tracking terrorists, for example, for serious crime detection and immigration management. The UK currently uses PNR data to combat illegal immigration and serious crimes under its national e-Borders programme and is concerned that if a restricted EU PNR Framework Decision is adopted solely to combat terrorism, this will limit the uses to which PNR data can be put in the UK, which would have an impact on its e-Borders programme.[453]

---

448 See the Hague Programme review set out in a Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Justice, freedom and Security in Europe since 2005: An Evaluation of The Hague Programme and Action Plan – An extended Report on the evaluation of the Hague Programme {COM(2009) 263 final} {SEC(2009) 765 final} {SEC(2009) 767 final} <www.eur-lex.europa.eu>.

449 "Legitimacy of PNR Challenged Again" (14 October 2008) <www.libertysecurity.org>.

450 Commission Proposal 2007/654 for a Council Framework Decision on the use of Passenger Name Record (PNR) for Law Enforcement Purposes (6 November 2007) <www.ec.europa.eu>.

451 Evelien Brouwer's Study for the European Parliament *Towards a European PNR System? Questions on the Added Value and the Protection of Fundamental Rights* (11 March 2009) at 4 <www.ceps.eu>.

452 Ibid, 6-10. Paul de Hert and Rocco Bellanova's Study for the European Parliament *Data Protection from a Transatlantic Perspective: The EU and US Move Towards an International Data Protection Agreement?* 35 - 38 (19 November 2008) <www.ceps.eu>.

453 "Dispute between UK Government and EU Over the Use of PNR" (27 August 2008) *European Digital Rights* <www.edri.org>.

In this unstable environment, another concern is that without a Framework Decision in place, bilateral agreements will be negotiated, further weakening any chances of a unified approach regarding PNR data. The US has already started negotiating agreements with some EU Member States.[454]

What is the future of PNR data regulation? If nothing else, a top priority must be to fill the gaping hole in European data privacy instruments in relation to the second and third pillars. Without that, as data privacy advocates learned in the EU/US PNR negotiations, what might start as an effort to protect data may ultimately backfire. The process highlighted more than ever the need for a new EU structure. Fortunately, a proposal is already on the table.

If the Lisbon Treaty is enacted, and the pillar structure is abolished, the new data protection provisions in the Treaty on the Functioning of the European Union will ensure that no sector is left unregulated. Not all areas will be subject to the new general provisions on data protection. There are some specific rules and declarations that apply to former pillars two and three, but at least regulation in all areas is ensured.[455] Moreover, with increased voting rights, Parliament will not so easily be cut out of any future proposals on personal data privacy, at least regarding matters falling under former pillar three.

However, to the extent that future data exchange agreements fall under former pillar two (common foreign and security policy), Parliament could still be relegated to onlooker status. This is possible in light of the Court of Justice's 2006 ruling that the exchange of PNR data between the EU and US did not fall under pillar one, but pillars two *and* three.[456] Under the Lisbon Treaty, specific rules regarding the processing of data in the CFSP area will be adopted according to a Council decision if the processing involves Member States. Parliament will not be involved. But if future processing involves EU institutions (and not Member States), then Parliament will still have a role in the decision-making.[457]

---

454 Peter Hobbing *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, above n 382, at 330. See also Evelien Brouwer's Study for the European Parliament *Towards a European PNR System?*, above n 451, at 15.

455 For information on how the new structure would work see arts 16 and 39 of the Treaty on the Functioning of the European Union, above n 163. See also Alfonso Scirocco "The Lisbon Treaty and the Protection of Personal Data in the European Union," above n 126.

456 Judgment of the Court (Grand Chamber) in Joined Cases C-317/04 and C-318/04 paras 56-59 and 68 (30 May 2006), above n 436.

457 See Treaty on European Union (TEU), above n 123, art 39 and Treaty on the Functioning of the European Union (TFEU), above n 163, art 16. See also Scirocco "The Lisbon Treaty and the Protection of Personal Data in the European Union," above n 126, and "Observatory on the Exchange of Data on Passengers (PNR) with USA" <www.statewatch.org>.

Until the Lisbon Treaty comes into effect, ad hoc efforts to regulate data protection in the third pillar may continue. Examples include the Schengen I and II, Europol and Eurojust Agreements.[458] Although these efforts often use Convention 108 as a springboard to create sector-specific regulation and are comprehensive in their own right, they have nevertheless added to the confusion regarding data protection law in the third pillar. One creative hybrid approach is the transposition of ad hoc efforts into EU law. One such example is the Prüm Treaty. Initially entered into by seven states in 2005 to increase cross-border co-operation through exchange of "DNA data, fingerprints, vehicle registrations, and personal and non-personal data related to cross-border police cooperation … [,]"[459] it has since become transposed into the EU legal framework.[460]

Another development toward a more unified approach of data protection is the EU/US High Level Contact Group and its endorsed list of 12 data protection principles. Set up in 2006 to discuss "a more permanent solution to data protection issues relating to the US-EU exchange of information,"[461] it is of the opinion that an international agreement encompassing these principles is in the best interests of all. One high priority concern was judicial redress. With talks ongoing, there is hope that these discussions will produce a comprehensive framework agreement on data protection. [462] Although not all are encouraged by its agenda or secret nature.[463]

2 Why care about passenger data?

For those who question why the European Parliament and the European Data Protection Supervisor (among others) seem to be more concerned about safeguarding passenger privacy than combating crime and terrorism, there are reasons in addition to those raised in the EU/US discussions. Consider the following:

---

458 See de Hert and Bellanova's Study for the European Parliament *Data Protection from a Transatlantic Perspective*, above n 452, 7-9.

459 European Parliament Programme *Public Hearing on the Prüm Decision: Striking the Balance between Data Protection and Effective Police Cooperation?* (7 May 2007) 2 <www.europarl.europa.eu>. The original seven states were Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria. Many others have since joined.

460 Council Decisions 2008/615/JHA and 2008/616/JHA (23 June 2008) <www.eur-lex.europa.eu>. For more information on the Prüm Treaty and its transposition into EU law, see Leon Hempel, Michael Carius, & Carla Ilten European Parliament Study *Exchange of Information and Data between Law Enforcement Authorities within the European Union* (April 2009) 17-22 <www.statewatch.org> (accessed 7 August 2009).

461 See Hague Programme review, above n 448.

462 Ibid.

463 For a less optimistic viewpoint, see "US-EU Agreement to Disagree" *The Identity Project* (18 December 2008) <www.papersplease.org>.

(a) Databases contain significant inaccuracies:

As set out above, the number of databases becoming globally available has mushroomed since 9/11. In the United States alone, the number of databases available just for law enforcement purposes has exploded. A synopsis of a number of error-prone databases in the US and the ramifications of their use was recently put before the US Supreme Court in an exclusion of evidence case. Although the Court ultimately ruled that evidence obtained as a result of computer error did not warrant its exclusion in that case, the 5-4 ruling was far from a reflection of unity.[464] While guidelines exist to prevent commingling private and public data (see the Fusion Center Guidelines above), the fact that PNR data is even getting near these databases that are rife with inaccuracies is cause for concern. Already the number of misidentifications or erroneous inclusions on watch lists range from inconvenient (Ted Kennedy)[465] to job threatening (Eric Sherfen, see below) to embarrassing (Nelson Mandela)[466] to violating human rights (Maher Arar, see below).[467]

(b) Lack of independent oversight can result in failure to identify and correct system inaccuracies:

This concern was raised by the Article 29 Working Party. In the United States oversight of the use of PNR from a privacy standpoint is ultimately conducted by the Privacy Officer inside the Department of Homeland Security. While the persons who have occupied that position in the past have made valiant efforts to investigate Privacy Act violations (sometimes at personal cost),[468] there is an inherent conflict of interest. Especially since the reporting requirement is to the Secretary of Homeland Security, not Congress.[469] Moreover, their effectiveness is questionable. It has been well documented that Privacy Officers have often failed to receive co-operation in ongoing investigations, not helped by

---

464 For more information on US Supreme Court case *Herring v United States of America*, see Brief of Amici Curiae, above n 310. For Court's 5-4 ruling on 14 January 2009 against the Amici, see < www.supremecourtus.gov>.

465 Jarrett Murphy "Ted Kennedy's Airport Adventure" (19 August 2004) <www.cbsnews.com>. For TSA's side of the story see <www.tsa.gov>.

466 "US Drops Mandela from Terrorist List" (2 July 2008) <www.abc.net.au>.

467 For a more comprehensive list of others either on a watch list or erroneously detained, see the American Civil Liberties Union website <www.aclu.org>.

468 The investigation of a claim that an airline was turning over millions of passenger records to TSA for a "'security project'" led to unpopularity within the Department. House of Representatives Committee on Homeland Security *The State of Homeland Security 2006: An Annual Report Card on the Department of Homeland Security* (2006), above n 369 at 59.

469 Ibid, at 58.

their lack of subpoena power.[470] That could change if a bill introduced in 2007 is passed. As of 18 January 2009, that bill appears to be stalled in the Senate Committee on Homeland Security and Governmental Affairs.[471]

Customary oversight functions provided by Parliament in the EU, and Congress in the United States, may similarly be inadequate if complete programme details are kept from them, or side-stepped completely, as in the case of the European Parliament in the EU/US PNR negotiations. One example of failure to keep Congress informed of a certain programme's details was the Total Information Awareness programme (see above). The biggest stick the US Congress carries is the power of the purse, which it used to withdraw funding from TIA.[472] But it has to know where the money is going in the first place before its power is of any use.

Finally, when the availability of civil remedies and judicial review is curtailed by the stroke of a pen (as in the case of Privacy Act exemptions for current passenger pre-screening programmes), the last opportunity for independent oversight is lost.

(c) Systems that fail to correct inaccuracies and lack oversight lose credibility:

With a significant amount of personally identifiable information contained in inaccurate databases that have no independent oversight and no judicial redress, two-thirds of the checks and balances that keep democracies functioning are missing. Executive power reigns supreme, and systems lose credibility.

(d) Systems that fail to correct inaccuracies and lack oversight are more prone to privacy and human rights violations:

Information included in PNR data could include details of race, ethnicity, religion or dress. Moreover, under the EU/US PNR agreement, access has been granted to sensitive data, albeit in exceptional cases. "Exceptional" is defined as instances "where the life of a data subject or of others could be imperilled or seriously impaired."[473] Sensitive data is deleted "within 30 days once the purpose for which it has been accessed is accomplished and its retention is not required by law."[474] In the case of an ongoing investigation, this

---

470 Ibid, at 56-60.

471 S.332: A Bill to Amend the Homeland Security Act of 2002 to Clarify the Investigative Authorities of the Privacy Officer of the Department of Homeland Security, and for other Purposes <www.statesurge.com>.

472 Roy Mark "Wyden: No Funding for Total Info Awareness Program," (16 January 2003) <www.datamation.com>.

473 Letter from Michael Chertoff to Luis Amado setting forth terms of EU/US PNR agreement (26 July 2007), above n 419, at 3.

474 Ibid.

data could remain in the system for years, even if the data subject is not a suspect, but merely a "person of interest," ie someone who might know someone.

(i) In April 2008, Erich Sherfen, an American Gulf War veteran and commercial airline pilot, was suspended from his job because he appeared to be on a government terror watch list. (Although the United States government would not confirm or deny his status on a watch list, his employer did.) Mr Sherfen has since been allowed to return to work, but has sued the government to be removed from any list on which his or his wife's names appear.[475] As a result of this incident, it became public knowledge that Mr Sherfen's wife is of Pakistani descent, and that he had converted to Islam.

(ii) Maher Arar:[476]

> The purpose of the information collection is to screen passengers … to identify those persons who may pose a risk to border, aviation or public security, may be a terrorist or suspected terrorist or *affiliated with or suspected of being affiliated with terrorists, ... may be a person of interest. ...*

On September 26, 2002, Maher Arar, a 36-year-old Syrian-Canadian, was travelling home to Canada via New York, after having been on an extended three-month holiday in Tunisia with his wife and two children. He had been living in Canada since he was 17. He had a Bachelor's degree in Engineering and a Master's degree in Telecommunications from two Canadian universities.

Canadian Customs had given his name to US border agents at the request of Project A-O Canada (the investigative unit of the Royal Canadian Mounted Police (RCMP)). "Terrorism lookouts" were placed in the TEC system for both Arar and his wife. Terrorism lookouts are "used when someone is suspected of being a member, associate or sympathizer of a known terrorist organization."[477] It is not intended for persons of interest. Profiles on Dr. Mazigh and their children were also uploaded into IMS, "an automated facility for reporting and compiling intelligence information on targets '"known or suspected to be a potential border risk"'[478]

Agencies using TECS at the time included: INTERPOL; the US Bureau of Alcohol, Tobacco, Firearms and Explosives; the US Internal Revenue Service; the US Drug Enforcement

---

475 Jeanne Meserve "Name on Government Watch List Threatens Pilot's Career" (22 August 2008) < www.cnn.com>.

476 DHS, Office of the Secretary, Privacy Act of 1974 (US), above n 2; Customs and Border Protection Advanced Passenger Information System Systems of Records, above n 2. (DHS, Advanced Passenger Information System Systems of Records, 2007.) Emphasis added.

477 Justice Dennis R. O'Connor, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (18 September 2006) 19 <www.epe.lac-bac.gc.ca>.

478 Ibid, at 98.

Administration; the US State Department; the US Coast Guard and, when engaged in a joint investigation, the CIA and FBI.[479] Because the United States did not participate in the ensuing investigation into Arar's case, it is unknown what information was actually entered into TECS.

An hour before his arrival in New York, the FBI contacted Project A-O Canada to alert the Canadians of his impending arrival and the US plan to interrogate him and refuse him entry into the United States. When Arar arrived, he was detained and interrogated about alleged links to Al Qaeda. The information available to US border agents at the time was that:

(1) Arar had met Almalki, a Muslim-Canadian suspected of being associated with Al Qaeda, at a café in Ottawa just after 9/11; they had talked outside in the rain for 20 minutes, and proceeded to a computer equipment store;[480]

(2) He had associated with Almalki on occasion and had three business dealings with him;[481]

(3) Almalki was listed as the emergency contact on Arar's rental application;[482]

(4) Arar knew a second Muslim-Canadian who was the subject of the same investigation;[483]

(5) In the Canadian investigation file, Arar was listed as a "suspect or target";[484]

(6) He was listed as the principal subject of an investigation, whose name was included in a list of names of persons believed to be serious terrorist threats, described by some as "heavy hitters";[485]

(7) He had been in the Washington DC metropolitan area on 9/11;[486]

(8) He had an "important connection" to, and was a business associate or close associate of, Almalki. (Almalki was listed in a diagram entitled "Bin Laden's Associates: Al Qaeda Organization in Ottawa" and Arar was linked to Almalki in that diagram);[487]

(9) Arar had travelled especially from Quebec to meet Almalki at the café in Ottawa;[488]

---

479 Ibid, at 116, 117.

480 Ibid, at 78.

481 Ibid, at 113, 156.

482 Ibid, at 115-116.

483 Ibid, at 116.

484 Ibid, at 113, 126.

485 Ibid, at 113, 126.

486 Ibid, at 28, 144.

487 Ibid, at 25, 113.

(10) Arar was an "Islamic Extremist … suspected of being linked to the Al Qaeda terrorist movement." (Arar's wife, Dr Mazigh, was also included in this description);[489]

(11) He was linked to certain other individuals who were suspects in the investigation;[490]

(12) He had declined an interview with Project A-O Canada earlier in the year; and[491]

(13) Had left the country suddenly after refusing to grant an interview.[492]

Out of the 13 "facts" listed above, only four were substantiated: Arar admitted to knowing Almalki, meeting him at a café in Ottawa (he did not travel to Ottawa from Quebec, he lived in Ottawa), and talking with him outside in the rain for 20 minutes,[493] then proceeding to a computer equipment store. He also admitted to associating with Almalki on occasion, having had three business dealings with him. Finally, he admitted listing Almalki as the emergency contact on his rental application, and knowing a second Muslim-Canadian who was the subject of the same investigation.

The rest of the above information was either inaccurate or false. For example, evidence that he was linked to other suspects in the investigation was inaccurate. Arar was not in Washington, DC on 9/11 – he was in San Diego; he did not refuse an interview, rather, in accordance with his lawyer's instructions, he requested that certain interview conditions be met, to which the Canadians did not agree, so no interview took place; and he did not leave "suddenly" after "refusing" to be interviewed. He left for Tunisia five months later.[494]

All of the above information was provided by Project A-O Canada to American agencies when it turned over the contents of its entire investigation database contained on three compact disks. On the heels of 9/11, the Canadians were investigating sleeper terrorist cells in Ottawa and the possibility of a second wave of attacks. Project A-O Canada turned over its files contrary to policy, and without screening the information or report notes. There was, however, evidence that Project A-O Canada did later inform the American agencies that it did not have enough information to link Arar to Al Qaeda.[495] And the investigation file would have contained information that surveillance

---

488 Ibid, at 124.

489 Ibid, at 86, 113.

490 Ibid, at 25.

491 Ibid, at 28, 126, 144.

492 Ibid, at 28, 144.

493 On the Maher Arar support website, reference is made to a three-hour meeting. See <www.bcrevolution.ca >.

494 Justice O'Connor *Report of the Events Relating to Maher Arar*, above n 477, at 28, 126, 144.

495 Ibid, at 16, 101, 148.

on Arar was eventually discontinued, and that although warrants were sought to search various suspects' homes, Arar's home was not among them.[496] Whether or not the Americans saw this mitigating information is unknown.

After a 12-day detention in the US, Arar was flown to Syria, where he was chained, interrogated, beaten and tortured. He endured detention in a cell of "grave-like" proportions for ten months. Over one year later, in late 2003, he was allowed to return to Canada. Upon inquiry by the Canadian government, Arar was cleared of all allegations of terrorism. In his summary conclusions, Justice O'Connor found that the RCMP had passed on information to United States authorities "that was inaccurate, portrayed him in an unfairly negative fashion and overstated his importance in the RCMP investigation."[497]

The Canadian government paid Mr Arar compensation over C$10 million, the highest amount ever paid in a Canadian human rights case. Almalki and the second Muslim-Canadian involved in the underlying investigation were never charged with offences.

Among the report's 23 recommendations were that national security investigation training be given to the RCMP, that a new system be created regarding "lookout" alerts involving Canadian citizens, and that the Canadian Security Intelligence Service (CSIS) and the RCMP be banned from sharing information internationally that could lead to torture.[498]

While the four true facts are the reason Arar was put under surveillance in the first place, none of the other allegations were ever proven. Unconvinced of his innocence, the United States continues to record Mr Arar on its No-fly list.[499]

In the US removal order deporting Arar to Syria, mention was made of classified information in an addendum that was not made available to Justice O'Connor.[500] We will never know the extent to which the US had additional information upon which to deport Arar, although Justice O'Connor, upon a thorough two-year review of Canadian evidence (some classified), found it difficult to believe that the US decision was based on anything other than the Canadian information: "It is

---

496 Ibid, at 79.

497 Ibid, at 13.

498 Ibid, at 364-369.

499 House of Lords European Union Committee *21st Report of Session 2006-07: The EU/US Passenger Name Record (PNR) Agreement: Report with Evidence* (The Stationery Office Limited, London, 2007) at 12-13 < www.statewatch.org>.

500 Ibid, at 156.

interesting that, as late as October 7, the very day the order finding Mr Arar a member of Al Qaeda was made, the FBI was still looking for evidence to link him to a terrorist group."[501]

Arar is currently suing the US government for violating his constitutional right to due process, and his right to choose deportation to a country other than one where he would endure torture, in accordance with his rights under domestic and international law. *Arar v Ashcroft* defendants include former Attorney General John Ashcroft, current FBI Director Robert Mueller, and former Secretary of Homeland Security Tom Ridge, as well as a number of US immigration officials.[502]

(e) Systems that fail to correct inaccuracies and lack oversight can also lead to intentional abuses:

In the United States in 2006, there were reports of Air Marshals having to fulfil Surveillance Detection Report (SDR) quotas of one report per month. Failure to meet their quota impacted air marshals' salaries and promotions.[503] Surveillance Detection Reports are one criterion in getting people named on terror watch lists. In response to an ACLU inquiry, the DHS found that in 2007 no one had been added to a watch list solely as a result of an SDR being filed. It added somewhat unconvincingly that it was "unlikely that an SDR, by itself, will be sufficient to add an individual to a watch list."[504] SDRs appear to be still in use.[505] Whether or not quotas are, is uncertain.

3 Intercepting communications

(a) United States – warrantless wiretapping and the Fourth Amendment

Among the legal instruments enacted in the United States immediately after 9/11, was a joint Congressional resolution approved on 18 September 2001, called the Authorization for Use of Military Force Joint Resolution (AUMF).[506] This resolution authorised the President "to use all necessary and appropriate force against those nations, organizations, or persons *he determines planned, authorized, committed or aided* the terrorist attacks ..., or harboured such organizations or

---

501 Ibid, at 154. For more information on the Maher Arar case, see also Scott Shane "Torture Victim Had No Terror Link, Canada Told U.S." (25 September 2006) *The New York Times* <www.nytimes.com> and the Maher Arar support website <www.bcrevolution.ca>.

502 Dina Temple-Raston "Court Weighs 'Extraordinary Rendition' Case" (5 January 2009) *National Public Radio* <www.npr.org>. See also Centre for Constitutional Rights <www.ccrjustice.org>.

503 "Marshals: Innocent People Placed On 'Watch List' To Meet Quota: Marshals Say They Must File One Surveillance Detection Report, Or SDR, Per Month" (21 July 2006) <www.thedenverchannel.com>.

504 Hugo Teufel III, Chief Privacy Officer, DHS letter to ACLU (6 October 2006). <www.dhs.gov>.

505 See DHS Federal Emergency Management Agency (FEMA) website regarding Datamaxx Group Tactical Information Sharing Solution product and SDRs at <www.rkb.us>.

506 Authorization for Use of Military Force Joint Resolution Pub Law No 107-40, 115 Stat 224 (2001), s 2(a).

persons ..."[507] (Emphasis added.) The Department of Justice under President Bush interpreted the above passage to mean that Congress authorised the President to "determine" the persons or groups responsible for those attacks ..."[508] (Emphasis added.) The reason behind this tortured reading would soon become apparent.

Laws that were enacted post 9/11 include the well-known "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act",[509] and the Homeland Security Act of 2002.[510] The Protect America Act was enacted in 2007,[511] and although it is no longer in force, it played a significant role in post-9/11 interception of communications by the United States government.

The USA PATRIOT Act, as it is commonly referred to, was introduced on 23 October 2001 and signed into law just three days later. It amended over a dozen statutes, including all three framework interception statutes: The Wiretap Statute (Title III),[512] the Electronic Communications Privacy Act (ECPA)[513] (including the Stored Communications Act (SCA)[514] within the ECPA), and the Foreign Intelligence Surveillance Act (FISA),[515] granting law enforcement and intelligence increased access to electronic communications and other sensitive records, including financial and credit records.[516] Among other things, it also increased the government's ability to detain and deport foreigners

---

507 Ibid.

508 US Department of Justice *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* 12 (January 19, 2006).

509 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub L No 107-56, 115 Stat 272 (2001) (codified in scattered titles of the US Code).

510 Homeland Security Act of 2002, Pub L No 107-296, 116 Stat 2135 (2002). Provisions of the Stored Communications Act amended by this Act are codified at 18 USC § 2702(b)(8) (Supp 2005).

511 Protect America Act of 2007, Pub L No 110-55, 121 Stat 552 (2007).

512 Title III of the Omnibus Crime Control and Safe Streets Act of 1968 42 USC § 3711 or the Wire and Electronic Communications Interception and Interception of Oral Communications (Wiretap Act) 18 USC §2510-2522, has been amended by: (1) the Electronic Communications Privacy Act (ECPA) of 1986, (2) the Communications Assistance to Law Enforcement Act (CALEA) in 1994, (3) the USA PATRIOT Act in 2001, (4) the USA PATRIOT Reauthorization Acts in 2006, and (5) the Foreign Intelligence Surveillance Amendments Act (FAA) of 2008 HR 6304.

513 Wire and Electronic Communications Interception and Interception of Oral Communications Act of 1986 (Wiretap Act) 18 US Code § 2510-2522.

514 Stored Wire and Electronic Communications and Transactional Records Access Act of 1986 18 USC § 2701-2712.

515 Foreign Intelligence Surveillance Act of 1978 50 USC § 1801-1871.

516 Mary Minow "Features – Library Records Post-Patriot Act (Federal Law)" (16 September 2002) < www.llrx.com>.

suspected of terrorist activity, removed the distinction between criminal investigations and surveillance insofar as foreign intelligence is concerned, and expanded the authority of the Treasury Secretary to freeze financial assets of suspected terrorist groups or individuals.

Enacted with sunset provisions beginning on 31 December 2005, the USA PATRIOT Act has been reauthorised twice, most recently on 2 March 2006. Provisions of the Act that are due to expire at the end of 2009 are the authority to use "roving" wiretaps (the ability to use one warrant to track a person regardless of the device or location being intercepted), to compel third parties to disclose business records without notifying the suspect (for example, banks, landlords and telecommunications companies), and to allow for secret surveillance orders against people who do not have connections to a terror group or foreign nation, denoted the "lone wolf" provision.[517] However, a bill was recently introduced in Congress to retain these provisions until 2019.[518]

The Homeland Security Act, which also amended the SCA, consolidated 22 federal agencies, bringing nine of them, including Customs, Secret Service, FBI's National Infrastructure Protection Center, and the former Immigration and Naturalization Service, under the roof of the newly created Department of Homeland Security.[519] Excluded were the remaining functions of the FBI, and the entire CIA. This Act expanded the ability of government entities to acquire subscriber information and the contents of communications by lowering the threshold from "reasonable belief" to "good faith belief" for Internet service providers to voluntarily disclose information in cases of emergency involving death or serious injury.[520] In the initial budget it also allocated US$500 million to research new technologies such as data mining in order to access and analyse volumes of data. (The supplemental 2003 budget allocated a further US$700 million "to help protect urban areas and critical infrastructure."[521])

---

517 USA PATRIOT Act, above n 509 ss 206 and 215, and Intelligence Reform and Terrorism Prevention Act of 2004 s 6001 <www.travel.state.gov>. See also Eric Rosenbach and Aki Peritz *Confrontation or Collaboration? Congress and the Intelligence Community* (Cambridge, Mass: The Belfer Center, Harvard University, June 2009) <www.belfercenter.ksg.harvard.edu> (last accessed 22 July 2009).

518 The Safe and Secure America Act of 2009 HR 1467, introduced 12 March 2009, extends the use of roving wiretaps for intelligence investigations, and allows the FBI to apply to the Foreign Intelligence Surveillance Court for a grant of access to tangible items (books, records, etc.) in foreign and clandestine intelligence, and international terrorism cases <www.thomas.loc.gov>.

519 Brian K Landsberg (ed) Macmillan-Thomson Gale "Department of Homeland Security Act 2002" *Major Acts of Congress* 2004 *eNotes.com* 2006 <www.enotes.com>.

520 "Monitoring of Email and Web Usage by Government and Law Enforcement Officials" (9 July 2009) *CIA Memory Hole* <www.ciamemoryhole.blogspot.com> (accessed 23 July 2009). See also Declan McCullagh "Bush Signs Homeland Security Bill" (25 November 2002) <www.news.cnet.com>.

521 Landsberg, above n 519.

The Protect America Act (PAA), which amended FISA, provided for the collection of international communications (including those of American citizens reasonably believed to be outside the United States) without a court order for up to one year. The Inspectors-General of the intelligence community recently acknowledged that PAA granted even broader surveillance powers than the secret presidential directive that authorised a questionable surveillance programme (the Terrorist Surveillance Programme (TSP), part of an overarching programme called the President's Surveillance Programme (PSP), for which they struggled to find a legal basis until the programme was revised in 2004).[522] (See below).

Although PAA expired on 16 February 2008, it was repealed on 10 July 2008 by the FISA Amendments Act of 2008 (FAA) (see below). But that was not the end of PAA. Many of its provisions were reinvigorated in FAA, albeit with more checks and opportunities for judicial review. (For example, under that Act, the Inspectors-General of five intelligence agencies were required to conduct a comprehensive review of TSP.)[523]

These new laws, enacted to combat terrorism, soon proved to have other, unintended consequences: spying on unsuspecting, innocent Americans. One person targeted by the government's expansive new mandate was Brandon Mayfield.

In 2004, Brandon Mayfield, an American lawyer, had his home searched, his telephone calls intercepted, and was detained for 14 days as a suspect in the Madrid train bombings earlier that year. This, despite the fact that he had not left the United States since 1994, did not have a criminal record, and fingerprints that the FBI incorrectly identified as his were confirmed by Spanish authorities not to be his. Mayfield was also a practicing Muslim, to which he attributes the government's zeal in pursuing him even without evidence.[524]

He brought an action challenging, among other things, the constitutionality of the USA PATRIOT Act (and its amendments to FISA), and the underlying authority for the government's actions. The government ultimately settled with Mayfield (after it lost three motions to dismiss) for US$2 million and an apology. The settlement did not preclude Mayfield challenging the constitutionality of the Act, with recovery limited to injunctive relief. On those grounds, he sued. In September 2007, Judge Ann Aiken of the Oregon District Court ruled in his favour, holding that the

---

522 Offices of Inspectors-General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and the Office of the Director of National Intelligence *Unclassified Report on the President's Surveillance Program* (10 July 2009) 22 <www.judiciary.house.gov>.

523 Daniel Ray "H.R. 6304 – FISA Amendments Act of 2008: New Law Expands Government Surveillance Powers" (12 July 2008) *Jolt Digest: An online companion to the Harvard Journal of Law & Technology* < www.jolt.law.harvard.edu>.

524 *Mayfield v United States of America* Civil Case no 04-1427-AA (J Aiken, Oregon District Court, 26 September 2007) 6-10 <www.ord.uscourts.gov>.

part of the Act that allowed surveillance and searches of Americans without probable cause violated the Fourth Amendment:[525]

> Prior to the Patriot Act, FISA may have had as its 'general programmatic purpose … to protect the nation against terrorism and espionage threats directed by foreign powers.' … After the Patriot Act, however, FISA surveillance, including the surveillance at bar, may have as its 'programmatic purpose' the generation of evidence for law enforcement purposes – which is forbidden without criminal probable cause and a warrant. …
>
> Moreover, the constitutionally required interplay between Executive action, Judicial decision, and Congressional enactment, has been eliminated by the FISA amendments. … These constitutional checks and balances effectively curtail overzealous executive, legislative, or judicial activity regardless of the catalyst for overzealousness. The Constitution contains bedrock principles that the framers believed essential. Those principles should not be easily altered by the expediencies of the moment. …
>
> *In place of the Fourth Amendment, the people are expected to defer to the Executive Branch and its representation that it will authorize such surveillance only when appropriate.* The defendant here [the US government] is asking this court to, in essence, amend the Bill of Rights, by giving it an interpretation that would deprive it of any real meaning. This court declines to do so.
>
> Judge Aiken's decision is on appeal.[526]

In addition to the odd individual being singled out by the government's increased surveillance and wiretapping powers, there was another programme underway that was catching the personal data of not just a few individuals, a few hundred, or even a few thousand, but millions of them. After 9/11, the National Security Agency (NSA) made a concerted effort to access telecommunications users' data without a warrant, with the complicity of a number of telecommunications companies. Interception was only part of the equation. The data still needed to be collected in a call database to be analysed or "mined."

Analysing dynamic information on the Web, unlike telephone records, requires more sophisticated technology than the performance of simple keyword searches on data in a database.[527] Data mining was the technology of choice.

---

525 Ibid, at 42-43. See also Susan Jo Keller "Judge Rules Provisions in Patriot Act to Be Illegal" (27 September 2007) *The New York Times* <www.nytimes.com>. (Emphasis added.)

526 David Kravets "Bush Administration Appeals Patriot Act Ruling" (8 February 2008) <www.wired.com>. For more information see David Holley "Lawyer Unjustly Jailed Working Toward 'Normal'" (26 March 2009) <www.eastcountynews.com>. See also a short video presentation of Mayfield's lawyer (famous advocate Gerry Spence) for interesting details of the case <www.brandon-mayfield.love.com>.

527 Jiawei Han and Kevin Chen-Chuan Chang "Data Mining for Web Intelligence" (Nov 2002) *Computer*, vol 35, no 11, at 64-70 <www2.computer.org>.

The related technology of keyword searches to analyse data has been around since at least the late 1970s. As early as 1978, the NSA's ECHELON programme (pursuant to a signals intelligence (SIGINT) agreement signed in 1948 between the UK and the United States: The UKUSA Agreement)[528] was designed to connect computers around the world so that they functioned as one. It was capable of intercepting telecommunications via satellite and conducting keyword searches on intercepted data:[529]

> The electronic signals that ECHELON satellites and listening posts capture are separated into two streams, depending upon whether the communications are sent with or without encryption. … Scrambled signals are converted into their original language, and then … are checked by a piece of software called Dictionary. There are actually several localised 'dictionaries.' The UK version, for example, is packed with names and slang used by the Irish Republican Army. Messages with trigger words are dispatched to their respective agencies.

According to Mike Frost, a former employee of the Communication Security Establishment (CSE) (Canada's equivalent of the American NSA), "ECHELON covers everything that's radiated worldwide at any given instant. … Everything from … data transfers to cell phones to portable phones to baby monitors to ATMs…."[530] Apparently these actions and communications radiate invisible electronic signals, and every one of them can be collected and analysed.[531]

To this day, the UK, Canada, United States, Australia and New Zealand all participate in the programme.[532] Although the United States government has never acknowledged it, there is overwhelming evidence of its existence.[533] It has also been recently revealed as the likely programme used to intercept communications in the controversial TSP programme.[534]

---

528 European Parliament Final Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system) (2001/2098 (INI)) at 59-61 < www.europarl.europa.eu>.

529 Ibid, at 71-72. See also Jason Leopold "Revisiting ECHELON: The NSA's Clandestine Data Mining Programme" (15 July 2009) *The Public Record* <www.pubrecord.org> (accessed 27 July 2009).

530 Interview with Mike Frost, former Canadian spy (Steve Kroft, "60 Minutes" television, 27 February 2000).

531 Ibid.

532 Duncan Campbell "Somebody's Listening …" (12 August 1988) *New Statesman* <www.cryptome.info>; Nicky Hager *Secret Power: New Zealand's Role in the International Spy Network* (Craig Potton Publishing, Nelson, New Zealand, 1996) at chapter 2 <www.fas.org>; European Parliament Report on the Existence of ECHELON, above n 528.

533 (1) Duncan Campbell "Somebody's Listening …," above n 532. *Note*: Two entities found Duncan Campbell's claims that the United States was using ECHELON for corporate espionage were unsubstantiated. See 21 December 2005 letter from Marc Rotenberg of the Electronic Privacy Information Center <www.cryptome.org>. See also European Parliament Resolution on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI)) of September 2001 recital R <www.europarl.europa.eu>; (2) Nicky Hager *Secret Power:*

The legal authority for the NSA's wiretapping programme is a secret presidential directive.[535] The Bush Administration did contend later, after the programme became known, that the AUMF Resolution, together with the President's inherent authority under Article II of the Constitution as Commander-in-Chief, gave him the power to conduct warrantless electronic surveillance, irrespective of the FISA requirement to obtain a court order from the secret Foreign Intelligence Surveillance Court in cases of warrantless wiretapping.[536] (Why the government later amended FISA to encompass this activity if it had inherent authority under the AUMF Resolution and Article II of the Constitution to conduct warrantless wiretapping in the first place is unclear.)

Publicly called the Terrorist Surveillance Program, the programme enabled the NSA to intercept over 300 terabytes[537] of data.[538] That is approximately one Encyclopaedia Britannica every four seconds.[539] Only one telecommunications company (telco) was identified as refusing to comply with a NSA request.[540] But this was not the first time the NSA had engaged in warrantless wiretapping.

New Zealand's Role in the International Spy Network, above n 532, at chapter 2; (3) Duncan Campbell "Australia First to Admit 'We're Part of a Global Surveillance System: Echelon Outed by the Head of Australia's Defence Signals Directorate (DSD), Martin Brady'" (28 May 1999) *Telepolis* <www.heise.de>; (4) European Parliament Final Report on the Existence of ECHELON, above n 528 and European Parliament Resolution on the Existence of ECHELON, above.

534 Jason Leopold "Revisiting ECHELON," above n 529.

535 Confirmed by the Offices of Inspectors-General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and the Office of the Director of National Intelligence *Unclassified Report on the President's Surveillance Program* 5, above n 522. See also James Risen and Eric Lichtblau "Bush Lets U.S. Spy on Callers Without Courts" (16 December 2005) *The New York Times* <www.nytimes.com>. See also Francesca Bignami "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining" 618, above n 189.

536 See Michael Hayden's testimony at his Senate confirmation hearing as CIA Director in July 2006: *Hearing of the Senate Select Committee on Intelligence on the Nomination of General Michael V. Hayden to be the Director of the Central Intelligence Agency* 109th Congress 35, 53 (2006). See also Francesca Bignami "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining" 618, above n 189.

537 One terabyte = 1,000,000,000,000 bytes or 1000 gigabytes. See Electronic Frontier Foundation FAQs < www.eff.org> (accessed 8 June 2009).

538 A later Department of Justice whistleblower has since identified TSP by its code name, "Stellar Wind". See Julian Sanchez "Behind the Legal Fight over NSA's Stellar Wind Surveillance" (16 December 2008) < www.arstechnica.com>.

539 Ibid.

540 In 2001, Qwest refused to give the NSA access to localised communications switches, which primarily carried domestic calls. There was also a reported case in 2004 of a major telecommunications company refusing to co-operate, believing the administrative subpoenas to be overly broad. That company's identity was not confirmed. See Eric Lichtblau, James Risen and Scott Shane "Wider Spying Fuels Aid Plan for

There is evidence to suggest that the NSA had engaged in this type of activity almost immediately upon President Bush assuming office. According to Bruce Afran, a lawyer representing plaintiffs in a federal lawsuit first filed in New Jersey challenging the NSA's wiretapping operations, there "was decisive evidence that within two weeks of taking office [around February 2001], the Bush administration was planning a comprehensive effort of spying on Americans' phone usage."[541] Moreover, there is also evidence that the NSA assisted in collecting telephone records in the 1990s to assist in the US "war on drugs".[542]

The data that the NSA was intercepting, collecting and mining post-9/11 included the content of telephone calls, emails, text messages and Internet communications not just of telco customers, but also of people who communicated with customers of the wiretapped telcos or whose data just happened to be carried over those networks.[543] The government's position is that it used phone numbers and e-mail addresses to analyse links between people in the United States and abroad. It did not listen to the communications. Both the Clinton and Bush administrations consistently signed off on the TSP programme.[544] With one notable exception: in 2004, FBI Director Robert Mueller III, Chief of the Justice Department's Office of Legal Counsel Jack Goldsmith, Deputy Attorney General James Comey (and possibly even Attorney General John Ashcroft, who was in hospital at the time) stated they would resign if the programme, as it was then constituted, was reauthorised over their objections. Details of the showdown, have been reported in riveting detail in *The Washington Post*.[545]

Forty-eight lawsuits (including that involving Mr Afran's clients), were filed against a number of telcos, alleging, violations of the First and Fourth Amendments, FISA, the Wiretap Act, and the

---

Telecom Industry" (16 December 2007) *The New York Times* <www.nytimes.com>. An unnamed telecommunications company also brought a case before the Foreign Intelligence Surveillance Court challenging the government's request for foreign intelligence on what appears to have been one of its customers. Unsatisfied with the Surveillance Court's ruling in the government's favour, the company appealed, only to lose once again. (See below.)

541 Lichtblau, Risen and Shane "Wider Spying Fuels Aid Plan for Telecom Industry," above n 540.

542 Ibid.

543 See the Electronic Frontier Foundation FAQs <www.eff.org> (accessed 8 June 2009).

544 Lichtblau, Risen and Shane "Wider Spying Fuels Aid Plan for Telecom Industry," above n 540.

545 For more on how the NSA Stellar Wind programme almost brought down the Justice Department and members of the Bush Administration with it, see two articles by Barton Gellman "Conflict Over Spying Led White House to Brink" (14 September 2008) <www.washingtonpost.com> and "Cheney Shielded Bush From Crisis" (15 September 2008) <www.washingtonpost.com>. The showdown between the Department of Justice, and the FBI on the one hand, and the White House on the other, has since been corroborated by the Inspectors-General *Unclassified Report on the President's Surveillance Program* 27-29, above n 522.

Stored Communications Act among other claims.[546] Not all of the lawsuits named telcos as defendants; at least four sued the Bush Administration, among other claims.[547] According to the Electronic Frontier Foundation (EFF), which filed the first of those lawsuits against AT&T in 2006,[548] the data AT&T released to the FBI and NSA was often via the retroactive use of National Security Letters (NSLs), administrative subpoenas that, unlike warrants, do not require a judge's signature.[549]

NSLs were created in the mid-1980s to help the FBI access communications and financial records in certain foreign intelligence cases.[550] There were a total of five NSL statutes as of 2008. The USA PATRIOT Act greatly expanded their reach. Among other things, it eliminated the requirement that the information being sought pertain only to a foreign agent or foreign power, merely requiring instead that the requested NSL be "relevant to an investigation to protect against international terrorism or foreign spying."[551] In subsequent audits, this NSL power was found to have been excessively, and sometimes illegally, used.[552] A bill is currently before Congress to reign in NSLs and require "specific and articulable facts" that the target be a "foreign power or agent of a foreign power" before a NSL will issue.[553]

The evidence from the lawsuit against AT&T is that all communications were split: one copy going to its intended recipient, the other to the NSA. There was no targeting of any particular individuals. Both Internet and telephone communications of all AT&T's subscribers, and people who were otherwise using the network, were duplicated without notice:[554]

---

546 See the Electronic Frontier Foundation Web page regarding NSA spying cases *EFF.org* <www.eff.org>. These lawsuits were consolidated in the Northern District Court of California before Judge Vaughn Walker on 15 February 2007: *In Re National Security Agency Telecommunications Records Litigation* (Northern District of California) Multidistrict Litigation (MDL) Docket no 06-1791 (VRW). The EFF and the American Civil Liberties Union are co-coordinating counsel.

547 *Shubert v Bush* (No C 07-0693), *Center for Constitutional Rights v Bush* (no C 07-1115), *Guzzi v Bush* (No C 06-6225), and *Al-Haramain Islamic Foundation, Inc. v Bush* (no C 07-0109), all consolidated with the cases against the telcos in the Northern District Court of California, see above n 546.

548 *Hepting v AT&T*, (Northern District of California Case no C-06-0672-VRW), filed on 31 January 2006.

549 See <www.eff.org>.

550 Charles Doyle *CRS Report for Congress National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments* <www.fas.org> (updated 28 March 2008).

551 Ibid.

552 Julian Sanchez "New Bill Would Tighten Rules for National Security Letters" (31 March 2009) < www.arstechnica.com>.

553 Ibid.

554 EFF letter dated October 12, 2007 to Chairman Dingell of the U.S. House Committee on Energy and Commerce, Chairman Markey of the Subcommittee on Telecommunications and the Internet, and Chairman

> To divert the communications, AT&T connected the fiber-optic cables entering the WorldNet Internet room to a 'splitter cabinet.' The splitter cabinet splits the light signals from the WorldNet Internet service into two, making two identical copies of the material carried on the light signal. The splitter cabinet directed one portion of the light signal through fiber optic cables into the NSA's secret room while allowing the other portion to travel its normal course to its intended destination. The split cables carried domestic and international communications of AT&T customers, as well as communications from users of other non AT&T networks that pass through the ... facility.

In one challenge to a government's NSL request under the Protect America Act brought by a telco before the Foreign Intelligence Surveillance Court (and then before three justices of the Foreign Intelligence Surveillance Court of Review in August 2008),[555] the Court held that an exception to the Warrant Clause of the Fourth Amendment existed, and that the unnamed plaintiff telco had to comply with government requests under PAA to intercept email and telephone communications of persons or agencies suspected of being spies or terrorists. It did not, however, rule on whether the interceptions conducted before the enactment of the PAA were legal.[556]

There were other lawsuits as well. *ACLU v NSA*[557] was brought by the ACLU on behalf of journalists, academics and lawyers who were forced to travel to meet sources and clients in person to assure confidentiality of communications. In that case, Judge Anna Diggs Taylor held that the government's TSP programme violated, among other things, the First and Fourth Amendments, FISA and the Separation of Powers doctrine, and summarily enjoined it:[558]

> The Government appears to argue here that, pursuant to the penumbra of the Constitutional language in Article II, and particularly because the President is designated Commander in Chief of the Army and Navy, he has been granted the inherent power to violate not only the laws of the Congress but the First and Fourth Amendments of the Constitution, itself. ... [T]he Office of the Chief Executive has itself been created, with its powers, by the Constitution. *There are no hereditary Kings in America* and no powers not created by the Constitution. So all 'inherent powers' must derive from that Constitution.

Stupak of the Subcommittee on Oversight and Investigation. The letter refers to the declaration of Mark Klein, overseer of AT&T's World Internet room.

555 The ruling was made public in January 2009.

556 See *In Re: Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act No 08-01* United States Foreign Intelligence Surveillance Court of Review 17 (22 August 2008) < www.fas.org>. See also James Risen and Eric Lichtblau "Court Affirms Wiretapping without Warrants" (15 January 2009) *The New York Times* <www.nytimes.com>.

557 *ACLU v NSA* 438 F Supp 2d 754 (Eastern District of Michigan) (2006).

558 Ibid, at 40-41. Emphasis added.

…

Not only FISA, but the Constitution itself has been violated by the Executive's TSP.

Although the court dismissed those claims barred by the state-secrets privilege (ie, data mining), the court held that plaintiffs had standing to sue on their claims regarding the unconstitutionality of the interception programme (that is, TSP).

In a divided opinion[559] of the Sixth Circuit Court of Appeals, Judge Taylor's decision was vacated and remanded for dismissal on the ground that the plaintiffs lacked standing to sue.[560] The US Supreme Court denied cert.[561]

In the wake of all these lawsuits, Congress passed, and former President Bush signed into law, the FISA Amendments Act of 2008.[562] This law granted the telcos retroactive immunity from liability in the warrantless wiretapping on certification by the Attorney General that the telco's actions were "in connection with an intelligence activity involving communications that" were: (1) authorised by the President between 11 September 2001 and 17 January 2007; (2) "designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States;" and (3) requested by the Attorney General or intelligence agency head on the representation that the request was authorised by the President and was legal.[563] The Attorney General has since made the requisite certifications.

Besides granting telcos retroactive immunity for their role in intercepting communications, the FAA improved upon many of the Protect America Act provisions, for example, by requiring a court order to eavesdrop on Americans overseas, and instructing the Foreign Intelligence Surveillance Court to review statutory compliance de novo. But it does continue to permit the interception of foreign communications received in the United States without a warrant.[564] Although the TSP

---

559 Three separate opinions (the opinion of the court, a concurring opinion, and one dissent) were delivered by the three-judge panel.

560 *ACLU v NSA* 467 F 3d 590 (6th Circuit Court of Appeals) (2006) <www.ca6.uscourts.gov>.

561 "Supreme Court Denies Cert in *ACLU v NSA*" (19 February 2008) <www.techlawjournal.com>.

562 FISA Amendments Act of 2008, Pub L 110-261, 122 Stat 2436 (2008). FAA is an amendment to the Foreign Intelligence Surveillance Act of 1978. It repealed the already lapsed Protect America Act of 2007, bringing the NSA interception programme under the Foreign Intelligence Surveillance Act.

563 Pub L No 110-261, § 802(a)(4)(A)-(B), 122 Stat. 2469 (July 10, 2008).

564 Daniel Ray "H.R. 6304 – FISA Amendments Act of 2008: New Law Expands Government Surveillance Powers," above n 523.

programme was not reauthorised beyond 1 February 2007, it is continuing under the supervision of the Foreign Intelligence Surveillance Court.[565]

Undaunted in the face of this retroactive immunity legislation (which effectively resulted in the dismissal of all the lawsuits against the telcos), the EFF persisted in arguing that the immunity provision is unconstitutional, earlier rulings against the Government from Chief Judge Vaughn Walker of the Northern District Court of California perhaps spurring them on.[566] The case is currently on appeal.[567]

In a second lawsuit, the EFF is suing the US government on behalf of AT&T customers to stop any ongoing surveillance on the grounds alleged in its first case against the telcos (ie that this surveillance violates the Constitution, FISA, the Wiretap Act and the Stored Communications Act).[568] President Obama is adopting the same line of defence as the Bush administration, ie that the retroactive immunity legislation is constitutional. This despite the fact that Obama's new Attorney General, Eric Holder, is on record as stating that he did not believe he would ever "see that a president would act in direct defiance of federal law by authorizing warrantless NSA surveillance of American citizens."[569]

And the lawsuits continue, including another filed by ACLU on 10 July 2008 (the same day former President Bush signed the FAA into law), for declaratory and injunctive relief on the unconstitutionality of FAA.

In addition, there is the *Al-Haramain* case against the Bush administration, which President Obama has now inherited**.** Based on claims that two American lawyers for a Saudi charity were illegally spied upon, this case is moving forward without the classified evidence mistakenly produced by (and since returned to) the government showing intercepted telephone calls between

---

565 Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and the Office of the Director of National Intelligence *Unclassified Report on the President's Surveillance Program,* above n 522, at 8, 30. See also the National Research Council Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals *Protecting Individual Privacy in the Struggle against Terrorism: A Framework for Assessment* 230 (The National Academies Press, Washington, DC, 2008).

566 See the EFF Web page regarding Judge Walker's rulings in the *Hepting v AT&T* case at <www.eff.org>.

567 David Kravets "Obama Claims Immunity, as New Spy Case Takes Center Stage" (15 July 2009) < www.wired.com> (accessed 23 July 2009).

568 *Jewel v NSA* (ND CA Case no C 08 4373 CRB) filed 18 September 2008 <www.eff.org> (accessed 9 October 2008). Defendants include the NSA, former President Bush, Vice President Cheney, and Attorneys General Alberto Gonzales and Michael Mukasey.

569 David Kravets "Obama Sides With Bush in Spy Case" (22 January 2009) <www.blog.wired.com>; Transcript Senate Confirmation Hearings: Eric Holder, Day One (16 January 2009) *The New York Times* 34 <www.nytimes.com>.

one of the charity's officers in Saudi Arabia and its American lawyers. The Treasury Department has declared the charity a "Specially Designated Global Terrorist" (SDGT) entity with "'direct links'" to Osama bin Laden.[570]

Two EFF officials were indicted on multiple charges, including conspiracy to defraud the US. One is a long-time resident of Oregon and of Iranian descent; the other, a municipal government official, lives and works in Saudi Arabia. Evidence supporting the government's case includes postings on the charity's website promoting violent jihad, transfer of funds specifically designated to support "'our Muslim brothers in Chechnya,'" and conversion of those funds into traveller's cheques and a cashier's cheque that were later transported out of the US without the requisite disclosure to the government. (Declaring all fund transfers out of and into the US in excess of US$10,000 is required by law.)[571] In defence of the charity, its former director stated that control of donations after they arrive in an area of conflict such as Bosnia and Chechnya is near impossible: "If you give a sack of flour to a needy family, you cannot guarantee that some of their mujahideen sons will not eat some of the bread made of that flour."[572]

(b) United Kingdom – prying eyes are everywhere

As illustrated above, the United States is not alone in its interception practices. In addition to participating in ECHELON internationally, the UK has a series of programmes in place domestically. Many stem from one piece of legislation: the Regulation of Investigatory Powers Act 2000 (RIPA).[573]

Among other things, RIPA regulates government interception, access, acquisition and disclosure of communications data. It allows the UK Home Secretary to issue interception warrants for the purpose of examining the contents of communications transmitted via the postal service or a telecommunications network "in the course of their transmission… ."[574] (Emphasis added.) Relevant grounds are national security, to prevent or detect serious crime, to safeguard the UK's economic well-being or in the case of proportionate conduct justifying the issuance of a warrant to give "effect to the provisions of any international mutual assistance agreement."[575] RIPA has had a rocky road.

---

570 Patrick Radden Keefe "State Secrets: A Government Misstep in a Wiretapping Case" (28 April 2008) < www.newyorker.com>.

571 See the Nine Eleven for Answers (NEFA) Foundation website at <www.nefafoundation.org>.

572 Ibid.

573 The Regulation of Investigatory Powers At 2000 (UK), Interception with a Warrant s 5(3)(a)-(d).

574 Ibid.

575 Ibid.

Lack of detail in the Act as initially introduced provoked sufficient consternation in the House of Lords that it was agreed, pursuant to section 71 of the Act, that a Code of Practice regarding the Acquisition and Disclosure of Communications Data be implemented. After the first version of this new Code of Practice was denounced by privacy advocates, a revised version was finally agreed upon in 2007[576] and it came into force on 1 October 2007.[577]

Among other things, this Code sets out who may self-authorise access to communications data, ie access without a warrant.[578] In 2008, 474 local bodies, including intelligence agencies, plus another 110 entities (such as regulatory agencies and commissions) had this authority.[579]

RIPA also allows government to demand decryption of encrypted electronic data or surrender of the encryption key in cases involving national security, the "economic well-being of the United Kingdom," or "to prevent or detect crime."[580] Recently tested in court, RIPA has so far withstood a challenge to the right to withhold an encryption key on the grounds of self-incrimination.[581]

RIPA has not lost its nickname as the "Snooper's Charter." In addition to continuing criticism for requiring ISPs to provide interception capability in their networks, it has been assailed for its inadequate oversight procedures.[582] One reason is undoubtedly because oversight primarily involves the review of internal processes.[583] Moreover, while a member of the public who believes their data has been acquired illegally by a public entity can file a complaint with the Investigatory Powers

---

576 "Regulation of Investigatory Powers Act 2000: An Act Making Provisions for Covert Surveillance and Access to Communications Records by Public Bodies" (19 January 2009) <www.guardian.co.uk>.

577 The Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order (2007) (UK). For more information, see an Explanatory Memo at <www.opsi.gov.uk>.

578 Home Office Acquisition and Disclosure of Communications Data Code of Practice Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000 (UK). Lawful interceptions without a warrant are set out in RIPA, above n 572, ss 1(5)(c), 2(7), 2(8), 3(1) and 3(2).

579 The London School of Economics and Political Science *Briefing on the Interception and Modernisation Programme* (response to 27 April 2009 consultation document *Protecting the Public in a Changing Communication Environment* 8 <www.lse.ac.uk> (accessed 2 August 2009).

580 RIPA, above n 572, Investigation of Electronic Data Protected by Encryption etc.: Power to Require Disclosure s 49(3) Notices Requiring Disclosure.

581 John Ozimek "RIPA Ruling Closes Encryption Key Loophole: No Pleas Against Self-incrimination Allowed" (14 October 2008) <www.theregister.co.uk>.

582 "Regulation of Investigatory Powers Act 2000: An Act Making Provisions for Covert Surveillance," above n 574.

583 *Information Commissioner's Response to "Protecting the Public in a Changing Communication Environment": A Consultation by the Home Office* (15 July 2009) paras 2.9 and 2.10 <www.ico.gov.uk> (accessed 2 August 2009).

Tribunal,[584] there is no equivalent provision for investigation of a private entity not subject to RIPA, and no remedy available other than criminal prosecution.[585]

Reports (albeit edited ones) are available regarding RIPA's implementation. In a recent report of the Chief Surveillance Commissioner, problems he encountered included overbroad interceptions (interceptions were being conducted along the lines of what was requested, and not what was authorised[586]), and misuse by public authorities. Some of these were not new revelations.

As the press reported in 2008, RIPA had been used to combat minor societal ills like littering and "dog fouling."[587] The Home Office took notice and announced that it would review how RIPA was being used.[588] But that review appears to have focused more on increasing surveillance powers than on restraining them. For example, one Home Office proposal was to collect and analyse third-party data crossing ISP networks "largely relating to communications services provided from overseas providers…"[589] To do that would inevitably require adding more sophisticated (that is, expensive) equipment to capture all of this traffic. The only entity with pockets that deep is government – not a viable option in the eyes of privacy and civil liberties advocates.

(c) Australia – innocents are not immune

Among the interception legislation enacted in Australia post-9/11 were amendments to the Telecommunications (Interception and Access) Act 1979 (Commonwealth) (TIA).[590] Except where authorised, the 1979 Act prohibits the interception of communications passing over a network as well as stored communications (for example, email, and stored voice mail messages). In amending the TIA, the Telecommunication (Interception) Amendment Act 2006[591] created a new type of

---

584 Home Office *Protecting the Public in a Changing Communication Environment* (April 2009) < www.homeoffice.gov.uk> (accessed 2 August 2009).

585 *Information Commissioner's Response to "Protecting the Public in a Changing Communication Environment": A Consultation by the Home Office*, above n 581, para 2.10.

586 Guy Herbert "Watching the Watchers" (22 July 2009) <www.guardian.co.uk> (accessed 2 August 2009).

587 Tom Whitehead "Town Halls Ordered to Stop Using Terror Laws to Catch Dog-foulers" (19 November 2008) <www.telegraph.co.uk>.

588 David Meyer "Home Office to Review DNA Database, RIPA" (16 December 2008) < www.news.zdnet.co.uk>.

589 Home Office *Protecting the Public in a Changing Communication Environment*, above n 582, at 4. For a response critical of the Home Office proposal, see The London School of Economics and Political Science *Briefing on the Interception and Modernisation Programme*, above n 577. See also the concerns raised by the Information Commissioner, *Information Commissioner's Response to "Protecting the Public in a Changing Communication Environment": A Consultation by the Home Office,* above n 581.

590 Telecommunications (Interception and Access) Act 1979 (Cth).

591 Telecommunication (Interception) Amendment Act 2006 (Cth).

warrant, called a "stored communications warrant," covering access to stored communications held by a telco or ISP. As with the rest of the world, new laws were being passed to keep pace with advances in technology.[592]

Two other highly controversial amendments were added by the 2006 Amendment Act: "B-party" and "Equipment-based" warrants. B-party warrants are issued against non-suspects who, although innocent, may be in contact with a suspect. Equipment-based warrants track a user regardless of which device they are using. Both were controversial because of their potential to violate innocent users' privacy rights.

In early 2008, additional proposed amendments to the TIA that would have allowed for "roving" search warrants (granting law enforcement and security forces access to multiple devices that are not listed on a warrant) were dropped by the government, due to significant opposition from the privacy lobby. However, a concessionary proposal was introduced to make the Act more flexible, enabling law enforcement agencies to add other devices to the same warrant later.[593]

Interception warrants for both real-time and stored communications are available in criminal investigations or for national security purposes. With national security warrants, the ASIO may obtain a warrant from the Attorney-General if "the person is engaged in, or *reasonably suspected ... of being engaged in, or of being likely to engage in*, activities prejudicial to security; and … the interception … will, or is likely to, assist the [ASIO] in carrying out its function of obtaining intelligence relevant to security…"[594]

A further amendment was recently passed making the ASIO's spying powers subject to independent review. Modelled on the UK's Independent Reviewer of Terrorism Laws, its mandate will be to ensure that Australia's anti-terrorism laws abide by international human rights law principles, and that the laws continue to be necessary.[595] Among other proposed changes to its counter-terrorism laws, Australia has recently asked for comment on giving the police emergency powers to conduct warrantless searches.[596]

---

592 See the Electronic Frontiers Australia website regarding Telecommunications Privacy Laws at < www.efa.org.au>.

593 Gary Hughes "Mobiles to Become Tracking Devices" (23 July 2007) <www.australianit.news.com.au>; Brett Winterford "Government Yields on Device Spying Bill" (13 May 2008) <www.zdnet.com.au>.

594 Telecommunication (Interception) Amendment Act 2006, above n 589, s 5 Subsection 9(A)1. (Emphasis added.)

595 Lynch and Garrity "At Last, an Independent Reviewer of Terrorism Laws," above n 231. See also Brett Winterford "Government Yields on Device Spying Bill," above n 591.

596 Attorney-General for Australia *National Security Legislation Discussion Paper* (12 August 2009) < www.attorneygeneral.gov.au> (accessed 23 August 2009). For response to the above discussion paper, see < www.amnesty.org.au> (accessed 23 August 2009).

The issue of compelling assistance to access communications in a computer that is on warrant premises is set out in section 3LA of the Crimes Act 1914. A court order is required before a suspect, computer owner/lessee, or employee may be compelled to assist, and is obtainable on reasonable suspicion that evidential material is on the computer.[597] Unlike the UK's RIPA, it does not directly refer to compelling disclosure of a decryption key itself, nor does it mention compliance for national security purposes. But like New Zealand's comparable provision (see below), it is probably broad enough to cover mandatory disclosure of encryption keys.

(d) New Zealand – far away, but still connected

Among the legislation that New Zealand enacted post-9/11 were the Terrorism Suppression Act 2002, the Government Communications Security Bureau Act 2003 (GCSB Act), and the Telecommunications (Interception Capability) Act 2004. Pre-existing acts were also amended regarding access to computers and encrypted data (see below).

As mentioned above, New Zealand's Terrorism Suppression Act 2002 had a tortured path into law, having been introduced before 9/11 and then enduring significant revision to incorporate New Zealand's obligations under UN Security Resolution 1373.[598] Its most recent amendment, in 2007,[599] received significant attention for a number of reasons.

Under the 2007 amendment it is a criminal offence to make property or financial services available to a designated terrorist entity, participate, harbour or conceal a terrorist, or make a credible threat. Of concern was the fact that anyone who tried to assist someone erroneously designated a terrorist would themselves run foul of the Act.[600]

The amendment also gave Customs authority to detain and seize property without a warrant if it suspected that the property was owned or controlled, directly or indirectly, by a designated terrorist entity.[601] And it created a duty (for anyone, but primarily banks) to report to the Commissioner of Police regarding similar suspicions.[602] Unlike other countries (the US, UK and Australia) the Act

---

597 Crimes Act 1914 (Cth) s 3LA.

598 Alex Conte *Counter-Terrorism and Human Rights in New Zealand*, above n 272, at 94.

599 Terrorism Suppression Amendment Act 2007. The Counter-Terrorism Bill 2003 amended the Terrorism Suppression Act 2002 in 2003 (Terrorism Suppression Amendment Act 2003) and there was an additional amendment in 2005 (Terrorism Suppression Amendment Act 2005). For more information on the Act and its amendments, see Alex Conte *Counter-Terrorism and Human Rights in New Zealand,* above n 272, at 114.

600 Terrorism Suppression Act 2002 (as amended), above n 271, ss 10, 12, 13, 13A, 25.

601 Ibid, ss 47A-47G.

602 Ibid, ss 43-47.

did not give police additional powers of arrest or detention.[603] (But the detention powers under the Immigration Act of 1987 are in the process of being amended, increasing initial detention from 72 to 96 hours without a warrant.[604])

Also controversial was the fact that under the 2007 amendment, the High Court lost its ability to review terrorist designations every three years (the Prime Minister alone now conducts the review).[605] According to Winston Peters, Foreign Affairs Minister at the time, changing the review procedure was necessary because the High Court did not have access to classified information deemed inadmissible. Speculation was that the United States was behind this amendment to facilitate unilateral action, should one be required.[606] Irrespective of the reason for the change, the effect was to eliminate oversight.

Finally, the 2007 amendment came on the heels of a terrorist raid in five cities and communities around New Zealand.[607] A raid that left many feeling uneasy.

The raid caused a mixture of emotions from anger to embarrassment and apathy. It was described in some circles as a heavy-handed police action: 300 riot police descending at dawn, breaking doors and windows, ordering families into the street at gunpoint, setting up roadblocks, boarding school buses, subjecting at least one teenage girl to an intimate body search. While few people were the actual targets (17 were arrested), the raid was not limited to them. Some Māori and Pākehā felt targeted for the wrong reasons: racism and intimidation.[608]

The Police, for its part, had done significant surveillance (including telecommunications) for almost two years and suspected that they were engaged in a raid to arrest armed "terrorists," some of whom were at a weekend "terrorist training camp". In Rūātoki, four guns and 230 rounds of ammunition were confiscated. In the end, however, the Solicitor-General could not authorise the bringing of charges under the Terrorism Suppression Act because the Act was completely unsuited to the situation at hand, or in his words: it was "incoherent and unworkable."[609] The Act applied to those who had already committed a terrorist act, not to those who may have been planning one. It wasn't the evidence that was at fault – according to the Solicitor-General some "very disturbing

---

603 See New Zealand's Immigration Act 1987 regarding numerous detention provisions.

604 Immigration Bill 2007.

605 Terrorism Suppression Act 2002 (as amended) s 35.

606 Joseph Barratt "High Court Bypassed Under New Anti-Terror Bill" (27 June 2007) <www.scoop.co.nz>.

607 Although the Act was introduced in March 2007, and the raids were on 15 October 2007, the legislation underwent its second and third readings on 24 October and 13 November 2007.

608 Danny Keenan "Searching for Terror" 17-34, and "The Terror Raids and the Criminalising of Dissent" 129-138 in Danny Keenan (ed) *Terror in Our Midst?* (Huia Publishers, Wellington, 2008).

609 Ibid, Danny Keenan "Searching for Terror" at 22.

activities" were discovered – it was the law.[610] In the end, the surveillance evidence the police had obtained under the Terrorism Suppression Act would not be admissible.[611] Sixteen people are still facing weapons, explosives, and firearms-related charges.[612]

In addition to the feelings the raid stirred nationally, it roused interest internationally. Around Christmas 2007, the UN Special Rapporteur on Counter-terrorism, the Special Rapporteur on fundamental freedoms and human rights of indigenous peoples, and the Secretary-General Special Representative on Human Rights Defenders sent a letter to the New Zealand government expressing concern over the raid and the effect on human rights, specifically the unnecessary disturbance in the Māori community of Rūātoki. They urged the government to take all steps necessary to ensure people's rights and freedoms were respected, and to make those responsible for any human rights violations accountable.[613]

Not everyone in New Zealand was incensed at the raid. Many also supported it and did not think it heavy-handed:[614]

> We are a conservative, middleclass white nation that sometimes pays lip service to liberal ideas… The wider sentiment of the 'great New Zealand public' is that the Maori should just get over it and that social change activists should just go and get jobs.

Another post-9/11 measure was the Government Communications Security Bureau Act 2003. New Zealand has a number of intelligence resources, including the NZSIS, its security intelligence agency, and the GCSB, its foreign intelligence agency.[615]

---

610 Jordan Pearson "'Anti-terror' Raids in New Zealand Remind of Old Brutalities" (17 November 2008) < www.thecommentfactory.com>.

611 Keenan, above n 606.

612 Pearson, above n 608. See also "'Anti-terror' raids in Urewera" at <www.nzhistory.net.nz>.

613 Ibid. See also "UN Orders Govt to Explain Anti-terror Raids" *New Zealand Herald* (Auckland, 17 January 2008) <www.nzherald.co.nz>.

614 Jordan Pearson "'Anti-terror' Raids in New Zealand Remind of Old Brutalities," quoting Graham Jury above n 608.

615 Although it has been predated to the late 1930s, the predecessor to the GCSB was created in 1955 as a restricted arm of the UKUSA network ie which comprises original members United States (NSA), and UK (Government Communications Headquarters (GCHQ)), and now, in addition to New Zealand's GCSB, the signals intelligence organisations of Canada (CSE), and Australia (Defence Signals Directorate (DSD)). Other intelligence groups include the Strategic Commitments and Intelligence Branch (SCI) of the New Zealand Defence Force, and a number of other groups relating to the Office of the Prime Minister and Cabinet. For more information on the SCI see <www.nzdf.mil.nz>. For more details on the roles of the groups that advise the Prime Minister and Cabinet see Weller "Change and Development in the New Zealand Security and Intelligence Services," above n 249. See also the European Parliament Final Report on the Existence of ECHELON, above n 528, at 59 and McBride "Heightened State Surveillance in New Zealand, Post-'9/11'", above n 272, at 4.

Like Australia's ASIS, New Zealand's GCSB statutory framework postdates its creation. While the GCSB came into existence on 1 September 1977, it only received a statutory framework in 2003 under the GCSB Act.[616] Its mission: to provide "New Zealand government departments with advice on all matters relating to foreign intelligence derived from the interception and exploitation of foreign communications and other signals (such as radar). These include radio, satellite and other forms of telecommunications (including facsimiles and telephones)."[617]

Interestingly, the GCSB's original purpose was not made clear to even the highest of political offices. During his time as Prime Minister from 1984 to 1989, David Lange was reported to have said that he was not advised the country was part of an international electronic spy network, even though as prime minister (and minister in charge of security and intelligence services), this information was certainly within his purview. In the foreword to Nicky Hager's 1996 book *Secret Power*,[618] he famously remarked "... it is an outrage that I and other ministers were told so little, and this raises the question of to whom those concerned saw themselves ultimately answerable."[619] As unbelievable as this may sound, his lack of knowledge was not unique. European leaders were likewise uninformed. In a European Union Resolution adopted in mid-2001, it was reported that "many senior Community figures, including European Commissioners, … gave evidence to the Temporary Committee [and] claimed to be unaware of this [same] phenomenon…."[620]

GCSB has been described as a "virtual branch of the US National Security Agency" by an independent human rights group.[621] Among links between the GCSB and NSA is ex-GCSB Director, Dr. Warren Tucker (now Director of the NZSIS), who was a former liaison officer to the NSA.[622] A report in April 1999 by the Inspector-General concluded that he was "satisfied from [his] inquiry and from [his] knowledge of the GCSB that it is not managed, controlled or influenced by the USA or other of its intelligence partners *contrary to our own national interests*."[623] (Emphasis added.) On its face, this statement does not preclude the possibility that GCSB is "managed, controlled or influenced by the USA or [others]," just that any outside influence is not contrary to New Zealand's own national interests.

---

616 Ibid, citing Nicky Hager *Secret Power: New Zealand's Role in the International Spy Network*, above n 532.

617 See the Department of the Prime Minister and Cabinet website <www.dpmc.govt.nz>.

618 Hager, above n 532, at 8.

619 Ibid.

620 European Parliament Resolution on the Existence of ECHELON, above n 533, recital C.

621 See <www.privacyinternational.org>. For additional information on the GCSB, see Hager, above n 532.

622 For more information on Dr Tucker see <www.nzsis.govt.nz>.

623 Weller "Change and Development in the New Zealand Security and Intelligence Services," above n 251, citing the Inspector-General of Intelligence and Security *Report on Inquiry into National Control of SIGINT Collection and Reporting of the Government Communications Security Bureau* (28 April 1999).

Like the NZSIS Act, the GSCB Act proclaims the Bureau's objective to protect against threats to traditional national security concerns, as well as the "interests of New Zealand's international well-being or economic well-being" but "only to the extent that they are affected by the actions or intentions of foreign organisations or foreign persons."[624] With its restricted focus on foreign intelligence, restrictions that apply to law enforcement and the NZSIS do not apply to the GCSB.

The GCSB Act sets out conditions for the issuance of interception warrants and computer access "authorisations."[625] The GCSB is only required to seek interception warrants under section 15(1) if the interception involves some physical connection or installation of an interception device "in a place for the purpose of intercepting communications that occur in the place."[626] Section 16 of the Act permits interception using an interception device without a warrant or authorisation as long as:

> (d) [T]he foreign communications do not contain private communications other than private communications that-
>
> (i) are produced, sent, or received by, or sent to, a foreign organisation or a foreign person; and
>
> (ii) *contain, or may* reasonably *be* expected *to contain, foreign intelligence*. (Emphasis added.)

Since the two GCSB bases in New Zealand, Waihopai and Tangimoana, primarily intercept electronic signals via satellite and do not need to attach listening interception devices, it is unlikely that it needs to seek interception warrants or authorisations.[627] The Transnational Issues Reporting Team analysis section of the GCSB processes "'raw" intercepted emails and other messages intercepted at Waihopai and elsewhere, translating them and producing standardised intelligence reports to send to New Zealand and overseas intelligence "end users."[628]

But concerns have been raised that while the GCSB may only target foreigners, the fact is that one leg of many communications being spied upon will inevitably consist of New Zealand individuals or organisations."[629] Since the ECHELON programme that appears to have been used in the NSA warrantless wiretapping of Americans also appears to be in use in New Zealand, there may

---

624 Government Communications Security Bureau Act (GCSB Act) (2003) s 7(2). "Foreign person" means not a New Zealand citizen or permanent resident. See GCSB Act s 4.

625 An "authorisation" is a mechanism allowing access to computer systems of foreign persons or entities. It must be issued by the Minister responsible for the GCSB on application of the GCSB Director or specified employee on justifiable evidence. See Government Communications Security Bureau Act 2003 ss 14-16 and 19.

626 GCSB Act, above n 623 s 15(1).

627 Weller "Change and Development in the New Zealand Security and Intelligence Services", above n 251.

628 "Waihopai: Our Role in International Spying" *Sunday Star Times* (Auckland, 11 May 2008) < www.stuff.co.nz>.

629 Weller, above n 251.

be some merit to this concern. Regarding the GCSB's focus, some GCSB staff have also raised the concern that the GCSB's new role after 9/11 seems to focus more on supporting the United States' "war on terror" than on monitoring terrorist activities in the immediate region.[630]

The Telecommunications (Interception Capability) Act 2004 sets out the parameters governing both New Zealand law enforcement and intelligence agencies' power to access telecommunications information, and the duties of telecommunications operators. It requires a telecommunications operator (ISP/telephone company) to decrypt customer communications if required to do so pursuant to an interception warrant, but only where the encryption product is provided by that particular operator.[631] The Act also requires operators to upgrade systems to assist law enforcement and intelligence agencies in intercepting communications.[632]

The Summary Proceedings Act 1957 section 198B (as amended in 2003) expands the power of law enforcement (but not intelligence) agencies to gain access to computer data.[633] Police may, in the process of executing a search warrant, demand that a specified person, (someone with possession or control of a computer, or an employee) provide assistance to access protected (that is, encrypted) computer data.[634]

While this Act does allow law enforcement to demand assistance to access computer data from the above specified persons, those persons do not include third party operators (such as ISPs or telecos). The Law Commission has recently recommended that section 198B be amended to include third party operators.[635] If this amendment is adopted without further qualification, it would eliminate the protection in the Telecommunications (Interception Capability) Act 2004, which limits decryption by an ISP or telco to only those communications protected by their own encryption programmes. In sum, while intelligence agencies are limited in the types of information they can ask ISPs and telephone companies to help them decrypt under the Telecommunications (Interception Capability) Act 2004, with the expansion of powers available under section 198B of the Summary Proceedings Act 1957, law enforcement is not.

---

630 "Waihopai: Our Role in International Spying," above n 627.

631 Telecommunications (Interception Capability) Act 2004 s 8(4).

632 This type of provision is not unique to New Zealand. For example, see the Communications Assistance for Law Enforcement Act (CALEA) 2004 in the United States 47 USC 1001-1010, and RIPA 2000 in the UK, above n 572.

633 Summary Proceedings Act 1957 s 198B.

634 Ibid.

635 Ibid.

Australia's equivalent provision to section 198B requires a court order before access is gained to computer data.[636] New Zealand's section 198B does not. The New Zealand Law Commission has recently reviewed the law on search and surveillance in general, and the issue of assistance in accessing a computer in particular. One recommendation was that a provision similar to Australia's be enacted. However, section 198B was enacted without the prior court order requirement before the Law Commission had completed its review.[637] There has been no recommendation that this requirement now be added to the Summary Proceedings Act.[638]

Even though section 198B is sufficiently broad to encompass the mandatory provision of encryption keys, the Law Commission has also recommended that this power be specifically enumerated. In addition, the Commission has recommended an amendment to allow the use of a multi-function surveillance device as well as multiple surveillance devices on a single warrant.[639] Based on its recommendations, search and surveillance powers are being updated in a Bill currently before Parliament.[640]

Unlike Australia, New Zealand has implemented specific provisions in both the NZSIS and GCSB Acts to minimise the impact of an interception warrant on third parties.[641] There are no comparable provisions for warrants on non-suspects.

In addition to these Acts regarding accessing data, there is also a Code to assist foreign governments. The Telecommunications Information Privacy Code 2003 allows the collection, use and disclosure of telecommunications information that would otherwise not comply with the Privacy Act, where it is necessary to help a foreign law enforcement authority to prevent, detect, investigate and prosecute a breach of a foreign telecommunications law.

4 Stopping the Funding of Terrorism

On 23 September 2001, President Bush signed Executive Order 13224 authorising the Treasury Department to block, without notice, all property of named "foreign persons" and entities, including

---

636 Crimes Act 1914, above n 595, s 3LA.

637 Law Commission *Search and Surveillance Powers* NZLC R 97, 229-230 (Wellington, 2007). See Part Two of report at <www.lawcom.govt.nz>. For a synopsis of the Law Commission's recommendations, see "Search and Spy Laws a Mess, Says Sir Geoffrey in Long-awaited Report" (8 August 2007) < www.nzherald.co.nz>.

638 Ibid.

639 Ibid, at 328.

640 Search and Surveillance Powers Bill 2008 45-1. For a digest of the Bill see <www.parliament.nz>.

641 New Zealand Security Intelligence Service Act 1969 s 4F; Government Communications Security Bureau 2003 Act, above n 623, s 24.

Osama bin Laden and Al Qaeda, within the US or under US control. The order also authorised blocking resources of individuals or entities who:[642]

> (i) … assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, such acts of terrorism or those persons listed in the Annex … ; or
>
> (ii) [are] otherwise *associated* with those persons …. (Emphasis added.)

It would be another four months before the UN adopted a Resolution naming Osama bin Laden, Al Qaeda and others,[643] although it did adopt a Resolution five days after President Bush's Order mandating the freezing of funds of persons who "commit," "participate" or "facilitate" terrorist acts.[644]

Prohibited actions under the Executive Order also included "US persons" making donations to anyone listed in the Order.[645] The US suspected that terrorists were receiving funding through charities, which would explain the government's interception of communications of the Al-Haramain charity and its subsequent designation as a Specially Designated Global Terrorist (SDGT) (see above).[646]

The Order also directed the Secretaries of Treasury and State (and other appropriate agencies) to co-operate with other countries "including through technical assistance" and to share intelligence to counter terrorist acts.[647] This language, together with the economic sanction power available to the President in a national security emergency under the International Economic Emergency Powers Act 1977 (IEEPA) (as later expanded by the USA PATRIOT Act),[648] and Executive Orders issued by President Clinton in the mid-1990s to block funds of those endangering the Middle East peace process, would lay the groundwork for another US "programme."[649] It would also land the United States in another confrontation with European lawmakers, although it would be years before this programme came to their attention through yet another leak to the press.

---

642 Executive Order 13224 Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism (23 September 2001) 66 Federal Register 49079, s 1(d) < www.fas.org>.

643 UN Security Council Resolution 1390, above n 281.

644 UN Security Council Resolution 1373, above n 280.

645 Executive Order 13224, above n 641, s 4.

646 See the NEFA Foundation website, above n 570.

647 Executive Order 13224, above n 641, s 6.

648 International Economic Emergency Powers Act 50 USC §1701-1707.

649 Nina J Crimm "High Alert: The Government's War on the Financing of Terrorism and its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy" (2004) 45 William and Mary Law Review at 1341, 1361-1363.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a Belgian worldwide financial messaging service that facilitates international money transfers among 7,800 financial institutions in more than 200 countries.[650] To accomplish these transfers requires information about the sender and recipient banks, the names of the sender and recipient, the amount to be transferred, the method of transfer, and the date and time of transfer. Sensitive data, such as the names of the sender and recipient and the amount to be transferred, is encrypted. The Treasury Department had subpoenaed SWIFT for records in the past, but production had been stymied primarily due to technical irregularities in the subpoena requests.

Immediately after 9/11, SWIFT received 64 administrative subpoenas from Treasury (reminiscent of NSLs issued in the NSA wiretapping case), many of which were sweeping requests for information on all transactions relevant to "terrorism" (as broadly defined by Treasury) in certain jurisdictions and at certain times. After negotiating with Treasury on the terms of the release of the data (including redefining the term "terrorism"), SWIFT complied, and handed over data from its mirror server in the United States. The data was not real-time, but approximately three weeks old. It was placed into a "black box" designed and held by the Treasury Department, and was searched using software that it developed. Data in the black box could only be accessed by Treasury, FBI, CIA, or other agencies, if relevant to a terrorist investigation and if overseen by a Belgian employee.[651]

SWIFT is a secure network with reliable information not otherwise available in systems where pseudonyms are more easily used (for example, email). Moreover, information can be used in "link analysis" "to identify any person with whom a suspected terrorist had financial dealings – *even those with no connection to terrorism***.** That information is then mapped and analysed to detect patterns, shifts in strategy, specific 'hotspot' accounts, and locations that have become new havens for terrorist activity."[652] (Emphasis added.)

Although SWIFT is unable to state categorically how much information was placed into the black box, in 2005 alone over 2.5 billion messages are estimated to have been placed inside.[653] In 2003, two years after what many had thought would be a temporary programme, the services of an independent auditor were hired at Belgium's request. Prior to that time, no independent oversight of the programme had occurred.[654] Barring four members of Congress (the chairs and ranking

---

650 See Web page regarding SWIFT Programme at <www.epic.org>.

651 "Belgian Prime Minister Condemns SWIFT Data Transfers to U.S. as 'Illegal'" < www.privacyinternational.org> (accessed 9 June 2009).

652 Josh Meyer and Greg Miller "U.S. Secretly Tracks Global Bank Data" (23 June 2006) *Los Angeles Times* < www.articles.latimes.com>.

653 Ibid.

654 See the June 2006 Web page regarding SWIFT Programme at <www.epic.org>, above n 651.

members of the House and Senate Intelligence Committees), and members of the Sept. 11 commission, who received classified briefings, Congress was not told of the programme until five years after its commencement, just as it was about to hit the press.[655] By comparison, the NSA's warantless wiretapping programme was reportedly shared with only "key lawmakers" and the presiding judge of the Foreign Intelligence Surveillance Court.[656]

Like the transfer of EU PNR data, the legality of the transfer of the SWIFT data was questionable under European law. Not until 2006 was this activity made public through three US newspaper articles.[657] The resulting investigation lead EU authorities to conclude that the data transfers had violated Belgian and EU data protection laws.[658]

One year later, in June 2007, SWIFT agreed to participate in the Safe Harbor Principles negotiated by the EU and US in 2000. This ensured that the transfer of data under the Treasury Department's "Terrorist Finance Tracking Program" (TFTP, also known as the SWIFT programme) would meet Belgian and EU standards. In a set of "Representations" (reminiscent of the US PNR Undertakings), the US Treasury Department provided the following:[659]

(1) TFTP does not involve data mining, but discrete searches for information "related to an identified pre-existing terrorism investigation";

---

655 Ibid. See also Eric Lichtblau and James Risen "Bank Data Is Sifted by U.S. in Secret to Block Terror" (23 June 2006) *New York Times* <www.nytimes.com>. Meyer and Miller "U.S. Secretly Tracks Global Bank Data," above n 653. See also the June 2006 Web page on the SWIFT Programme at <www.epic.org>, above n 651.

656 Meyer and Miller "U.S. Secretly Tracks Global Bank Data," above n 653. See also <www.epic.org>, above n 651.

657 Glenn R Simpson "Treasury Tracks Financial Data in Secret Program" (23 June 2006) *Wall Street Journal*; Lichtblau and Risen "Bank Data Is Sifted by U.S. in Secret to Block Terror," above n 656; Meyer and Miller "U.S. Secretly Tracks Global Bank Data," above n 653. See also Web page on SWIFT Programme at <www.epic.org>, above n 651; and Patrick M Connorton "Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide" (2007) 76 Fordham Law Review at 1.

658 Royaume de Belgique Commission de Protection de la Vie Privée Opinion no 37/2006 (27 September 2006) <www.steptoe.com>; Article 29 Data Protection Working Party *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (22 November 2006) <www.ec.europa.eu>. *EDPS Opinion on the Role of the European Central Bank in the SWIFT case* (1 February 2007) <www.edps.europa.eu>. See also "European Central Bank Found Accountable in the SWIFT Case" (14 February 2007) at <www.edri.org>.

659 Processing of EU Originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – SWIFT *Official Journal of the European Union* C 166/18 (20 July 2007) <www.eur-lex.europa.eu>.

(2) independent oversight to be conducted by SWIFT, an independent auditing firm and independent US authorities, including Congress and the Privacy and Civil Liberties Oversight Board;

(3) sharing with other US and foreign law enforcement and intelligence agencies only for related purposes;

(4) records are exempt from the Freedom of Information Act;

(5) administrative redress to be available through the Treasury Department as well as judicial review, regardless of nationality of data subject;

(6) to endeavour at least on an annual basis to delete unnecessary non-extracted data not later than five years after receipt; data regarding designated individuals to be retained in perpetuity; records on closed files to be deleted one year from the date the investigation is completed; other agencies' retention periods for onward data transfers apply; and

(7) "Eminent European" to be appointed to confirm the programme is implemented in accordance with US representations.

In a December 2008 review, the Belgian Data Protection Supervisor found SWIFT in compliance with Belgian data protection law.[660] In light of the ECJ's ruling that the EU Directive was an inappropriate legal basis for the PNR agreement between the EU and the US, whether or not the US Representations and SWIFT's joining the "safe harbour" provide an adequate legal basis remains in doubt. The Safe Harbor Principles were developed in accordance with the EU Directive, that is, pillar one matters. Clearly, using financial data strictly for counter-terrorism purposes is anything but a pillar one matter. Like PNR, it logically falls more squarely within pillars two or three. Whether or not the EU will challenge the legal basis of the SWIFT Programme remains to be seen, but challenges are already brewing in the United States.

Since 2001, 500 individuals and groups have been designated Specially Designated Global Terrorists. None has been successfully challenged in court. In recent years, the US government has successfully shut down eight Islamic charities domestically (and frozen the assets of hundreds more internationally)[661] under powers granted to Treasury in Executive Order 13224 and the IEEPA. These include the Global Relief Foundation, Holy Land Foundation, Al-Haramain Foundation, and

---

660 "SWIFT Respects Data Protection Legislation: Decision by the Belgian Data Protection Commission regarding SWIFT" (10 December 2008) Press Release <www.swift.com>. Commission de la Protection de la Vie Privée Decision (8 December 2008) <www.privacycommission.be>.

661 Patrick Radden Keefe "State Secrets: A Government Misstep in a Wiretapping Case," above n 569. William Fisher "Politics-US: Court Reins in Terror Finance Policy" (20 August 2009) <www.ipsnews.net> (accessed 21 August 2009).

KindHearts for Charitable Humanitarian Development, Inc.[662] With the exception of KindHearts, they have all been designated as SDGTs by the US Treasury Department. By comparison, the UN has only designated Al-Haramain (and its worldwide branches) and the Global Relief Foundations on its Consolidated List.[663]

In January 2002, Global Relief sued the Treasury Department to enjoin the blocking order and to release its assets, which the District Court declined to do. On 31 December 2002, the US Seventh Circuit Court of Appeals affirmed the trial court's ruling.[664]

As for the Holy Land Foundation, after the first trial was declared a mistrial, five leaders of the charity were convicted in the US in November 2008 on 108 counts in relation to supporting Palestinian militant group Hamas.[665] Al-Haramain is currently in litigation with the US government over its warrantless wiretapping programme (see above), and KindHearts has just won a notable victory.

In a lawsuit brought by the ACLU on behalf of KindHearts, a federal court recently ruled that Treasury's actions in freezing the charity's assets for three-and–a-half years (while it investigated whether to designate the charity as a SDGT for allegedly supporting designated terrorist group Hamas) violated KindHearts' rights under the Fourth and Fifth Amendments. Those violations included proceeding without a warrant, failing to provide the charity with information on the allegations against it, and failing to give it notice of a hearing. In essence, the charity had lost its presumption of innocence. (It was also encumbered by not being able to use frozen funds to pay for its own defence.) A hearing has been set for September 2009 to determine how to proceed.[666] Inasmuch as there is US Supreme Court precedent supporting failure to give notice and failure to provide pre-seizure hearings in cases where to do so would allow the enemy to hide assets, whether the US will appeal, and whether this ruling would stand on appeal, remains to be seen.[667]

(For post-9/11 international instruments implemented by the UN, European institutions and various countries, see Table 2.)

---

662 See the Treasury Department website <www.ustreas.gov>.

663 See UN Consolidated List, above n 372.

664 *Global Relief Foundation, Inc v Paul H O'Neill, Secretary of the Treasury, et al* 315 F 3d 748 (7th Circuit Court of Appeals, 2003).

665 Gretel C Kovach "Five Convicted in Terrorism Financing Trial" *The New York Times* <www.nytimes.com> (accessed 21 August 2008).

666 Fisher "Politics-US: Court Reins in Terror Finance Policy," above n 662.

667 *Global Relief Foundation, Inc v Paul H O'Neill,* above n 663.

X DO ANY OF THESE PROGRAMMES STOP TERRORISM?

In 2008, almost 50,000 people were killed or injured in terrorist attacks (down from 67,000 in 2007). Most of the attacks occurred in Iraq, Pakistan and Afghanistan. And as in previous years, substantially more than half of the attacks were perpetrated on Muslims. Approximately 65 percent of the victims were civilians.[668] Given the threat that terrorism continues to pose, no one can seriously dispute the need for effective tools in order for law enforcement and intelligence agencies to do their jobs. The question is: do these tools work?

There are some answers.

A The Case "For"

> "I can say unequivocally that we have gotten information through this program [TSP] that would not otherwise have been available."[669]

Despite positive assertions from senior intelligence agency officials, very few details have been released on the effectiveness of the PNR, TSP, and SWIFT programmes, but there are a few that have been reported in the press or in court documents. The programme with the most information on arrest and conviction rates is SWIFT:

- Hambali, the Bali bombings mastermind, arrested August 2003 (along with two of his lieutenants). Hambali is being detained at Guantanamo, and has yet to face trial;[670]
- Uzair Paracha, Brooklyn man convicted in 2005 on a terrorism-related charge of agreeing to launder $200,000 through a Karachi bank;[671]
- Five officers of the Holy Land Foundation (see above); and
- Abu Hamza al-Masri. Abu Hamza was convicted in England on a number of counts, including soliciting murder. He is serving a seven-year sentence. An Imam, his sermons stirred hatred of Jews and advocated a duty of Muslims to kill "non-believers." He was also wanted in the US for conspiring to set up a training camp in Oregon, and for his involvement with the Islamic Army of Aden, the terrorist organisation credited with the bombing of the USS Cole in Yemen.

---

668 National Counterterrorism Center *2008 Report on Terrorism* (30 April 2009) at 11-12 <www.wits.nctc.gov >. See also National Counterterrorism Center *2007 Report on Terrorism* (30 April 2008) at 11 < www.wits.nctc.gov>.

669 NSA Director General Michael Hayden, quoted in *The New York Times*, 17 January 2006. See also Lowell Bergman, Eric Lichtblau, Scott Shane, Don Van Natta Jr and William K Rashbaum "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends" *New York Times* (17 January 2006) <www.nytimes.com>.

670 "Bush Tells of al-Qaida Plot to Fly Jet Into Tallest Building in Los Angeles" (9 February 2006) < www.buzzle.com>; Lichtblau and Risen "Bank Data Is Sifted by U.S. in Secret to Block Terror", above n 656. Joe Boyle "Hambali and the Guantanamo Problem" (4 March 2009) <www.news.bbc.co.uk>.

671 Lichtblau and Risen "Bank Data Is Sifted by U.S. in Secret to Block Terror," above n 656.

General claims of SWIFT effectiveness are more prevalent. For example, we know that SWIFT has lead investigators to "a key facilitator of terrorism in Iraq."[672] And that SWIFT information was helpful in providing information on the 2005 London bombings.[673] We also know that "… as of January 2006, the U.K. ha[d] seized and/or frozen the assets of over 100 organizations and 200 individuals, in an amount exceeding one hundred million dollars, 'the bulk of [which] have now been unfrozen and made available to the current government of Afghanistan.'"[674]

SWIFT data has only been "marginally successful"[675] in tracking Al Qaeda, which uses more informal means of transferring money. Out of the 165 terrorism cases filed in the United States,[676] 18 involved SWIFT data.[677] Of those, only seven have been convicted: Paracha, the five officers of the Holy Land Foundation, and Abu Hamza. (Hambali has yet to face charges.) Three of them (Paracha, Abu Hamza and Hambali) all had links to Al Qaeda.

According to Treasury, SWIFT data has also been helpful in tracking middle-tier terrorists and financiers in addition to militant groups, including Hezbollah, Hamas and Palestinian Islamic Jihad. One of the reasons for the programme's success is immediate subpoena compliance. Although the data is not received in real-time, it is a vast improvement on waiting for foreign banks, who either do not comply with requests for information at all, or respond too late for the information to be of use.[678]

In addition to SWIFT subpoenas, others have been issued to Western Union (an electronic money-transfer service) with equal success. In one instance, data obtained from Western Union "help[ed] Israel disrupt about a half-dozen possible terrorist plots there..."[679]

As far as the success rate for the TSP programme, that is harder to gauge. Even former DHS Secretary Michael Chertoff conceded "I don't know that it's ever possible to attribute one strand of

---

672 Simpson "Treasury Tracks Financial Data In Secret Program," above n 657.

673 AFP "London Bombing Suspects Face Grilling" (30 July 2005) *ABC News* <www.abc.net.au>; Metropolitan Police Service Bulletin "Five Jailed for Assisting Terrorists" *MPS* Web page (4 February2008) <www.met.police.uk>; Simpson "Treasury Tracks Financial Data In Secret Program," above n 658.

674 Beckman *Comparative Legal Approaches to Homeland Security and Anti-terrorism* citing the Economic and Social Research Council, above n 70, at 60. Whether terrorist designations resulting in the freezing of funds were accurately applied is beyond the scope of this paper.

675 Meyer and Miller "U.S. Secretly Tracks Global Bank Data," above n 652.

676 Depending on the website accessed, the list of US terrorist cases varies from between 135 to 165. See the *NEFAFoundation* website, above n 571.

677 Processing of EU Originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – SWIFT 166/23, above n 660.

678 Meyer and Miller "U.S. Secretly Tracks Global Bank Data," above n 652.

679 Lichtblau and Risen "Bank Data Is Sifted by U.S. in Secret to Block Terror," above n 655.

intelligence from a particular program."[680] Without referring specifically to the TSP programme, he continued "whatever you can do technologically to find out what is being said by a known terrorist to other people, … that is without a doubt one of the critical tools we've used time and again."[681]

It is believed that the NSA's TSP programme contributed to the arrest of two Muslim immigrants in Albany, New York in August 2004. In October 2006 Yassin Aref, an Imam at a local mosque and Iraqi refugee, and Mohammed Hossain, were convicted (among other things) of money laundering and conspiring to aid a terrorist group. Hossain, an American citizen and former Bangladeshi immigrant, agreed to borrow money to improve his pizza business, having been informed that the money came from the sale of a missile launcher to be used against a Pakistani diplomat in New York. Unaware that they were dealing with a government informant,[682] they were both sentenced to 15 years in prison, and their convictions were upheld on appeal in July 2008.[683]

The US government has indicated that the TSP programme may also have helped in the investigations of people in Portland and Minneapolis affiliated with Al Qaeda. In Minneapolis in 2004, Canadian citizen Mohammed Abdullah Warsame was charged with supporting terrorism. In Portland, six people were convicted of numerous crimes, including "money laundering and conspiracy to wage war against the United States."[684]

In 2003 Iyman Faris was convicted of plotting to destroy the Brooklyn Bridge in New York, and sentenced to 20 years in federal prison.[685] Initial reports attributed his capture to the NSA's warrantless wiretapping programme, but these attributions have been contested.[686]

Historically, ECHELON was also suspected of being responsible for the capture of notorious terrorist Carlos the Jackal, as well as one of the two Libyans convicted of blowing up Pan-Am Flight 103 over Scotland in 1988, killing all 259 aboard and 11 more people on the ground.[687]

---

680 Bergman, Lichtblau, Shane, Van Natta Jr and Rashbaum "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," above n 669.

681 Ibid.

682 Michael Wilson and Dennis Gaffney "2 Albany Men Are Convicted In Missile Sting" (11 October 2006) *The New York Times* <www.nytimes.com>.

683 See the *NEFAFoundation* website, above n 571.

684 Bergman, Lichtblau, Shane, Van Natta Jr and Rashbaum "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," above n 669.

685 Contributors Kelli Arena and Producer Terry Frieden "Ohio Trucker Joined al Qaeda Jihad" (20 June 2003) *CNN.com* <www.edition.cnn.com>.

686 Bergman, Lichtblau, Shane, Van Natta Jr and Rashbaum, above n 669.

687 Interview with Mike Frost, former Canadian spy (Steve Kroft, "60 Minutes" television , 27 February 2000), above n 530.

In Australia in 1995, telephone and text message interception (along with video surveillance and undercover work) netted the capture of 17 terrorist suspects (all Australian residents of Algerian, Moroccan, Pakistani and Lebanese ethnicity) plotting to explode major targets in two Australian cities. The law credited with enabling their capture had been enacted just one week before.[688] And very recently, Australia arrested four Australian citizens (of Somali and Lebanese descent) plotting a suicide mission to attack military barracks near Sydney with semi-automatic weapons. Physical and electronic evidence was used in that joint police and ASIO surveillance operation.[689]

Reports on arrests based on PNR data have been more cryptic still. There have been many general claims of success, but few specific ones, especially with regard to terrorism. In a presentation to the European Parliament in 2007, former DHS Secretary Michael Chertoff, gave eight examples of successful PNR use in the United States.[690] Most of the identified persons were denied entry because of other criminal reasons (drug smuggling, document fraud), or because they had a high-risk profile. For example, one was a flight instructor with links to individuals regarded as "security risks and immigration violators." Another was identified through a telephone number known to be used by terrorist suspects. One said he was visiting a group suspected of having financial ties to Al Qaeda and had images of armed men, one labelled "'Mujahadin.'" The most credible evidence of PNR success is that of a terrorist denied entry to the US in June 2003: through the use of PNR data and fingerprints, he was later identified as a suicide bomber in Iraq, where he killed 132 people.[691]

In other countries, it is much the same story. In the UK, an e-Borders programme representative reported in 2007 that 18 people had been prevented from boarding and one "suspected facilitator" was arrested. What the suspect was allegedly facilitating is unclear.[692] But it doesn't appear to have been terrorism. As reported in a 2006-2007 House of Lords report, "no examples were given to us of the use of PNR data in the fight against terrorism."[693] Since its inception in November 2004, the e-

688 Richard Esposito "Australian Terror Network Operating for More Than Three Years" (8 November 2005) < www.abcnews.go.com>.

689 "Suicide Attack Plot Alleged: 5 Held" (4 August 2009) *ABCNews* <www.abc.net.au> (last accessed 23 August 2009). See also Meraiah Foley "Australia Officials Say Terror Suspects Plotted to Kill Until Killed" (4 August 2009) *New York Times* <www.nytimes.com>.

690 Letter from Michael Chertoff to Members of the European Parliament (14 May 2007) <www.dhs.gov>.

691 Ibid.

692 See Report on Article 29 Working Party Workshop on an EU Approach towards a New Passenger Data Agreement, above n 353.

693 House of Lords European Union Committee *21st Report of Session 2006-07: The EU/US Passenger Name Record (PNR) Agreement,* above n 499, at 11, para 20.

Borders programme has resulted in 900 arrests for crimes including murder, rape, drug and tobacco smuggling and passport offences, but no terrorism-related offences.[694]

On the other hand, Australia reported that PNR data helped identify 21 out of 161 matters as terrorism-related in 2007-2008. The rest involved drug trafficking, objectionable material, or "persons of interest" regarding serious crimes.[695] No additional specific information was provided.

B The Case "Against"

> Total Information Awareness project was a thoughtless and overblown approach that somehow assumed that magic algorithms could be applied that would extract [meaning] from this enormous mass of private-sector data added to public data—that somehow up would pop the bearded face of Osama bin Laden.[696]

Dr Westin's criticism of the theory that technology is the guaranteed solution to terrorism has support. Jeff Jonas and Jim Harper, distinguished technicians from IBM and the Cato Institute, contend that traditional investigative techniques and better communication and collaboration would have revealed the 9/11 terrorists, and could have captured subsequent terrorists.[697] The problem with predictive data mining technology (used in commerce to identify and target consumers with specific products) is that it is not well suited to discovering potential terrorists for two primary reasons: (1) the lack of patterns in terrorist attacks means that algorithms used to predict the next attack cannot succeed; and (2) the number of false-positives generated is so high as to make the programme cumbersome, expensive and ineffective.[698] They are not alone in their opinion.

Predictive data mining requires a data set. While there are vast databases available against which to run predictive data mining algorithms, there is a high risk of data being taken out of context or used to discriminate, as some of the above examples have illustrated.[699]

---

694 Ibid, at 40, para 155.

695 Agreement between Australian and the European Union on the Processing and Transfer of European Union Sourced Passenger Record Data, Report 95: Treaties Tabled on 4 June, 17 June, 25 June and 26 August 2008 para 7.5.

696 Interview with Dr Alan F Westin, author and privacy expert (Sarah D Scalet, 15 June 2003) transcript provided by *CIO* "Privacy Q&A: Alan Westin On Protecting Corporate Data" <www.cio.com>.

697 Specifically the authors refer to the capture of 9/11 highjackers al-Mihdhar and Nawaf al-Hazmi. Jeff Jonas and Jim Harper "Effective Counterterrorism and the Limited Role of Predictive Data Mining" (11 December 2006) *Cato Institute Policy Analysis* no 584 <www.cato.org>.

698 Ibid.

699 Anita Ramasastry "Lost in Translation? Data Mining, National Security and the 'Adverse Inference Problem'" (2006) 22 *Santa Clara Computer & High Tech Law Journal* 757, at 777.

In August 2008, the US Congressional Research Service prepared an updated report on data mining, ascribing its limitations to data or personnel error rather than to technology.[700] For example, while data mining may correctly show suspicious patterns of behaviour, including buying tickets last-minute, this pattern may have more to do with financial reasons than terrorism.[701] The report also found that the NSA may now be at risk of being drowned in too much data to be effective.[702]

In October 2008, the National Research Council created the Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals to review the effectiveness and the legality of "data mining, information fusion, and behavioural surveillance technologies."[703] Funded by DHS, its conclusion on the effectiveness of data mining in identifying terrorists was that the utility of pattern-based data and information fusion depended on the availability of a useful data set comprising characteristics of a certain group of people.

In an experiment conducted in Germany (before it was ruled unconstitutional) the data of 8.3 million individuals was analysed using former terrorist profiles (ie, young men, current or former students, Islamic, from one of 26 Muslim countries and German residents). When checked against other databases of information (for example, people with pilot licences), close to 1,700 persons were identified. After a year of investigating these people further, not a single "sleeper" terrorist was identified.[704]

The Committee found that the utility of pattern-based data mining is "very unclear."[705] In conclusion, it held that "[a]utomated identification of terrorists through data mining (or any other known methodology) is neither feasible as an objective nor desirable as a goal of technology development efforts."[706]

On 4 February 2009, the UN's Special Rapporteur issued a report on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[707] Noting with concern that "the line between … strategic intelligence and probative evidence has become blurred"

---

700 Seifert CRS Report for Congress *Data Mining and Homeland Security: An Overview*, above n 321, at 3.

701 Ibid.

702 Seifert CRS Report for Congress *Data Mining and Homeland Security: An Overview*, above n 321, at 26.

703 National Research Council Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals *Protecting Individual Privacy in the Struggle against Terrorism*, above n 565.

704 Ibid, at 215.

705 Ibid, at 24.

706 Ibid, at 3-4.

707 Martin Scheinin *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* A/HRC/10/3 (4 February 2009) <www.ohchr.org>.

in the name of "national security imperatives",[708] he found that "[t]he collection and sharing of 'signal' intelligence [for example, ECHELON-derived intelligence] has led to several violations of the right to privacy and the principle of non-discrimination…."[709] One example of this was provided by former Canadian spy, Mike Frost, who recounted the story of a woman talking on the phone to a friend about how her son "bombed" at his play the night before. This conversation was picked up by ECHELON and her name and telephone number were added to the database of suspected terrorists.[710]

On the use of data mining, the inherent over-inclusiveness of such programmes requires extra vigilance to ensure that racial or ethnic profiling (and its repercussions on travel, employment, and banking, for example) does not occur. Of significant concern in that regard was the use of "sentiment analysis", a new application that forms profiles based on authored opinions on the Internet, and which is currently in use in the US, Canada, China, Germany, Israel, Singapore and Taiwan.[711]

To combat these risks, the Special Rapporteur made a number of recommendations including: the adoption of data protection legislation along the lines of the UN Guidelines, a domestic legal basis for intelligence services' use and storage of data (subject to review and audit processes), clarification of private companies' responsibilities and liability in their data transfers to government agencies, parliamentary oversight and broad investigative powers, delineation of intelligence versus law enforcement duties, a minimum of restrictions on transparency for national security purposes, and detailed provisions regarding each investigative technique.[712]

Finally, the US Intelligence Community Inspector Generals prepared their own Report[713] on the failings of the President's Surveillance Programme (which includes TSP). Released on 10 July 2009, the unclassified version of the report found that only a portion of the intelligence derived from the TSP programme was used in preparing threat assessments, since other sources of intelligence were available that were more detailed and timely.[714] Also, overly restrictive access to information about the programme limited the effectiveness of the Foreign Intelligence Surveillance Court and the

---

708 Ibid, at 8, para 29. An example of a system using detailed investigative techniques is Dutch intelligence.

709 Ibid, at 2, Summary.

710 Interview with Mike Frost, former Canadian spy (Steve Kroft, "60 Minutes" television, 27 February 2000), above n 530.

711 Martin Scheinin *Report of the Special Rapporteur* at 9, para 33, citing The Economist (25 September 2008), above 706.

712 Ibid, at 8 para 27; 10 para 35; 24 paras 65-68; 25 paras 70, 73; 26 para 75.

713 Offices of Inspectors General *Unclassified Report on the President's Surveillance Program*, above n 522.

714 Ibid, at 9.

Justice Department's Office of Intelligence Policy and Review (that is, they were not kept fully informed).[715] When interviewed, most intelligence community witnesses "had difficulty citing specific instances where PSP had directly contributed to counterterrorism successes."[716] (Although the NSA Director did cite several examples of PSP information being used in terrorist investigations, he wasn't specific.)[717] But PSP is not TSP. The actual success of TSP alone is unknown. The remaining aspects of the PSP programme remain classified.

In addition to the formal reports above, others more informal (but informed) have appeared in the press. More than a dozen (current and former) FBI agents on the receiving end of the NSA's TSP programme reported being inundated with names, telephone numbers, and email addresses that led to hundreds of agents being pulled from other assignments to investigate the thousands of monthly tips. Virtually all of the "tips" led to dead ends or to persons they already knew about. Some agents did concede, however, that they might not know the whole story on convictions obtained overseas based on the information gleaned from the TSP programme.[718] But there has been some confirmation from British counterterrorism officials on the overstated success of the programme. For example, the US government's claim that the TSP programme was essential in uncovering a 2004 plot to detonate fertiliser bombs in London has been questioned. Evidence of the plot had already been gleaned by other means, including prisoner interrogations.[719]

Other criticisms have been levelled at the process by which the US Treasury Department designates people as SGDTs. Dennis Lormel, who retired from the FBI in 2003 with considerable financial investigation experience under his belt, was assigned after 9/11 to determine how Al Qaeda was receiving funding. Lormel says that they "latched onto charities immediately".[720] But even so, he "would have been 'hard pressed' to act on some of the material that Treasury officials used. Oftentimes, I think they base their evidence on media stories or public-source information, whereas we would never use only that…"[721]

---

715 Ibid, at 18.

716 Ibid, at 36.

717 Ibid, at 35-36.

718 Bergman, Lichtblau, Shane, Van Natta Jr and Rashbaum "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," above n 669.

719 Ibid.

720 Ibid.

721 Ibid.

And finally, there is also the negative psychological fallout from these programmes. In our post-9/11 world, where many feel increasingly watched, psychiatrists have reported an increase in cases of psychosis.[722]

While some of the programmes discussed above have netted the capture of convicted terrorists, the question is: are they worth continuing in light of the risks they pose to civil liberties and human rights?

XI WHERE ARE WE HEADED?

No law or programme can provide a simple guaranteed solution when it comes to combating terrorism. We know that innocent people have been swept up in some of the current programmes and that others have been left unprosecuted. Some mistakes are bound to occur. But did the law allow some programmes to be implemented before technology, independent oversight, operating and redress procedures, and staff, were ready? Could fallout have been minimised if deployment had been deferred?

A Where We've Been

> I would always wonder, what does "suspected' mean?[723]

This is what a former prosecutor mulled over whenever he received tips from intelligence officials who, upon handing them over, "would always say that we had information whose source we can't share, but it indicates that this person has been communicating with a suspected Al Qaeda operative."[724] Investigations into terrorists have to start somewhere, and beginning with people who are *known* to affiliate with terrorists makes sense, but is our government also pursuing innocent civilians they believe *may be affiliated* with someone who *may be a suspected terrorist* more avidly than the evidence warrants?

The case of Maher Arar is an extreme example. Unfortunately, there are other cases of note:

- Ahmed Zaoui, was an Algerian citizen, former Imam, university lecturer and democratically elected leader in Algeria. In 2002, a series of misunderstandings, false reports on his association with terrorist group GIA, and convictions (in absentia) in France and Algeria (among other things), resulted in his being detained upon arrival in New Zealand for over two years (ten months of which were in solitary confinement). This, despite the fact that approximately seven months after he arrived, he was granted refugee

---

722 Kim Zetter "Surveillance Society Sparks Psychosis" (29 August 2008) <www.wired.com>.

723 Bergman, Lichtblau, Shane, Van Natta Jr and Rashbaum "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," above n 669. (Former senior prosecutor familiar with eavesdropping programmes, quoted in *The New York Times* 17 January 2006.)

724 Ibid.

status by New Zealand's Refugee Status Appeal Authority.[725] During the course of his ordeal, an Inspector-General was removed from the case for "apparent bias," and details of his case were leaked to the press resulting in sensational headlines causing additional damage to Zaoui's case and reputation for which mea culpas were later offered.[726] Changes to the detention and charging procedures in the Immigration Act 1987 are currently before Parliament (initial detention periods without a warrant are actually increasing from 72 to 96 hours);

- In 2003, Khaled el-Masri, a German citizen of Lebanese descent, car salesman, and father of six, was abducted from Macedonia to Afghanistan where he was beaten and abused for five months, and then released.[727] He had the misfortune of having the same name as someone else suspected of links to terrorists. He filed a lawsuit in the US against CIA officials and the airline companies responsible for transporting him to Afghanistan. German authorities confirmed most of el-Masri's allegations. His case was dismissed on the basis of the state secrets privilege. El-Masri is seeking extradition of the 13 CIA agents believed responsible for his ordeal.[728] Senator Ted Kennedy is behind the introduction of recent legislation to scale back the US state secrets privilege;[729]

---

725 New Zealand Refugee Status Appeal Authority Decision, Refugee Appeal no 74540 (1 August 2003) granting Zaoui refugee status two years before he was released from detention <www.humanrights.co.nz> (accessed 17 June 2009). For a chronology of events leading up to Mr Zaoui's release from prison see < www.greens.org.nz>. See also <www.tvnz.co.nz> and <www.humanrights.co.nz> (both accessed 26 June 2009). See also Gordon Campbell "Gordon Campbell: Zaoui – The Final Chapter?" (14 September 2007) < www.scoop.co.nz>.

726 *Zaoui v Greig* (31 March 2004) HC AK CIV-2004-404-000317, para 106 Salmon & Harrison JJ < www.scoop.co.nz> (accessed 28 June 2009): "… the Inspector-General's interview statements about refugees and his subsequent dealings with the Director and members of the media raise, when considered together, the real possibility of apparent bias against Mr Zaoui when undertaking his review of the Director's decision: in the first instance of undue disfavour or partiality against Mr Zaoui, and in the second of undue favour or partiality towards the Director." See also an article summarising the interview with the Inspector General: Gordon Campbell "Watching the Watchers" *New Zealand Listener* (Auckland 29 November-5 December 2003). See also Chris Barton "Prisoner of a Legal Catch-22" *The New Zealand Herald* (Auckland, 8 November 2004): "In a post-September 11 climate, the terrorist story had, as they say, legs. Media organisations including the Herald pursued it vigorously. It's now clear that many of the earlier stories got it hopelessly wrong – a consequence of using unsubstantiated internet-based reports."

727 Khaled el-Masri statement American Civil Liberties Union <www.aclu.org>.

728 Jerry Markon "Lawsuit against the CIA Is Dismissed" *The Washington Post* (19 May 2006). "German Sues for CIA Extradition" <www.news.bbc.co.uk>. For more information on extraordinary renditions see Rebecca Leung "CIA Flying Suspects To Torture? Scott Pelley Reports on the CIA'S Rendition Program" (6 March 2005) <www.cbsnews.com>.

729 US Senate State Secrets Protection Act, S 417 and HR 984. "Both Houses Of Congress Urge State Secrets Reform" (11 February 2009) American Civil Liberties Union <www.aclu.org>.

- In 2007, Dr Mohamed Haneef, an Indian doctor working in Australia, was detained in custody for 12 days and later charged in connection with a Glasgow airport bomb plot. A year earlier, Dr Haneef had given a second cousin, a doctor in England, a SIM card, which was in turn given to the doctor's brother. That brother was in the jeep that crashed into the Glasgow airport. Months earlier in England, the doctor had been exonerated of any connection to a terrorist group, but that evidence was ignored in Australia. After an inquiry was launched by the Australian government, no evidence was found against Dr Haneef. Recommendations were made to revise the legislation that led to Dr Haneef's arrest and charge.[730] They are in the process of being implemented.[731]

These are but a few of the stories that made it to the press. There are other cases, including lawsuits brought against the US government for "extraordinary renditions" and torture in other countries.[732]

And there are still other cases, not of persons getting caught in a net, but of ones falling through the cracks, despite laws and programmes enacted or created post-9/11:

- On 31 May 2005, Hamid Hayat, a US citizen of Pakistani descent, was on the No-fly list but was still permitted to board a Korean Air jet bound for California. Discovered en-route, the flight was diverted to Japan. Later investigations revealed that Hayat had attended a Jihadist training camp in Pakistan for six months. (It was also revealed that his relatives had connections to a number of Jihadist groups.);[733]
- Izhar Ul-Haque, charged in Australia with training with a Pakistan-based terrorist organisation in 2003. Illegal actions of the Australian Federal Police and ASIO (kidnapping and false imprisonment) resulted in the exclusion of evidence forcing withdrawal of the case. Some have faulted the government and its stance on the "war on terror" for emboldening law enforcement and intelligence agencies to exceed their

---

730 *Report of the Inquiry into the Case of Dr Mohamed Haneef Volume One* (November 2008) 254-255 < www.haneefcaseinquiry.gov.au>. Mark Rix "With Reckless Abandon: Haneef and Ul-Haque in Australia's 'War on Terror'" Sydney Business School University of Wollongong (2008). See also Mathias Vermeulen "Australia's New Legislative Counter Terrorism Proposals after Haneef Inquiry" (12 January 2009) *The Lift* <www.legalift.wordpress.com>.

731 *Australian Government Response to Clarke Inquiry into the Case of Dr Mohamed Haneef – December 2008* <www.ag.gov.au>.

732 The Constitution Project "9th Circuit Court of Appeals Rejects Overbroad State Secrets Claim by Federal Government" (28 April 2009) <www.constitutionproject.org>.

733 House of Representatives Committee on Homeland Security *The State of Homeland Security 2006: An Annual Report Card on the Department of Homeland Security* 10, above n 368. Whether or not his family's connections to Jihadist groups warrant significant consideration is a difficult question in light of prior cases of misidentification for this exact reason. See the Dr Haneef case above.

authority. An inquiry in this case was also launched, and ten recommendations were made on how to better manage counterterrorism operations in the future, such as improving communications and provision of additional basic equipment, including more 'secure' desktop phones;[734] and

- Mamoun Darkazanli, indicted in Spain on terrorism charges. Despite EU member states' obligations under the Framework Decision on the European Arrest Warrants enacted in 2002[735] (which abolishes formal extradition proceedings and replaces it with "a system of surrender between judicial authorities"),[736] Germany failed to surrender Darkazanli to Spain based on two findings: (1) no evidence that Darkazanli supported the 9/11 plot (meetings for which took place in Spain); (2) being a member of Al Qaeda was not illegal in Germany until 2002. Darkazanli is still on the UN's Consolidated Terrorist List.[737] (See Table 2 for more detail on the European Arrest Warrant.)

What these cases demonstrate is that laws and programmes can only go so far in protecting us against terrorism. In some cases, they go too far in their overzealousness. We will never know if some of the more extreme errors could have been avoided had the programmes been rolled out after further testing. But we can surmise that had more oversight been in place at the time, there is a good chance that programmes with the potential to violate human rights would have been challenged. If more oversight is the key, then to whom should that duty fall?

B Where We Could Be Heading

There are a number of options regarding oversight. For example, the UN. While the UN has been, and will continue to be, a world leader in the fight against terrorism, like any organisation it is not immune to failure. In addition to a 74-page consolidated list of terrorist individuals and entities, the UN also has a list of 42 persons and entities removed from the consolidated list due to error or the fact that listed persons no longer meet the requisite criteria.[738]

Should the duty fall to the world's Parliaments and Congresses? As we have seen, while they play an important role in holding executive branches to account regarding wayward programmes, these governmental bodies are not always provided with all the facts on which to make well-

---

734 Mark Rix "With Reckless Abandon: Haneef and Ul-Haque in Australia's 'War on Terror,'" above n 730.

735 Framework Decision 2002/584/JHA on the European Arrest Warrant and the Surrender Procedures between Member States (13 June 2002).

736 Ibid, at recital 5.

737 "Complete 9/11 Timeline: Mamoun Darkazanli" <www.historycommons.org>. UN Consolidated List < www.statewatch.org>. For more information on the history of Al Qaeda, see <www.globalsecurity.org>.

738 1267 Committee of the Security Council "Individuals, groups, undertakings and entities that have been removed from the Consolidated List pursuant to a decision by the 1267 Committee" <www.un.org>.

informed decisions. At times, only a few high-ranking members are informed, which provides little opportunity for debate and consensus, or they are disregarded altogether.

Are the courts the best entities to conduct supervision? While courts have recently become more willing to challenge executive assertions of a state secrets (or equivalent) privilege, in matters of national security deference to the executive branch will undoubtedly continue, as it must. But providing for in-camera review of classified evidence, and granting defendants summaries of evidence against them, would be a step in the right direction toward having more oversight of the executive branch. Some countries have already begun this process.[739]

Perhaps independent reviewers of terrorism laws and programmes could provide more oversight? While these individuals provide another dimension, their contributions may overly reflect their own leanings, and lead to bias.

What about the press? We only know of some of these programmes through its dogged determination. But the press is also susceptible to the temptation of salacious headlines, sometimes out of their own lack of diligence, sometimes after governments apparently leak information. (As in the Maher Arar and Ahmed Zaoui cases.)

That leaves the people. While there will always be individuals who courageously challenge the system when it moves too far away from the values the West holds dear, the obligation of oversight does not rest on their shoulders alone. If we do not fully exercise our duties and responsibilities as citizens, we have no one to blame but ourselves for the path taken.

XII CONCLUSION

While laws and technologies have their place in keeping us safe, they cannot succeed on their own. Some of the legal hurdles the West has overcome in protecting privacy without sacrificing national security are noteworthy, including: the US concession to EU views on privacy (Safe Harbor Principles), EU concessions to US programmes (the EU/US PNR agreement, SWIFT), the US creation of a Privacy and Civil Liberties Oversight Board,[740] and bilateral efforts, including the High Level Contact Group. The biggest cultural hurdle that comprehensive and limited privacy systems have overcome is a reconfigured concept of privacy incorporating aspects of both liberty and dignity.

But as we have seen, none of these efforts are free from inherent and ongoing challenges. For our laws and programmes to effectively protect national security without unduly sacrificing privacy, there must be robust, independent oversight.

---

739 See New Zealand's amendment to the Immigration Act 1987 and US State Secrets Protection Act.

740 While not exactly like the European Data Protection Supervisor, whose mandate it is to do more than merely advise, it is a step in the right direction.

While the duty of oversight may ultimately rest with the people, it must not rest with individual citizens alone, but with all layers of society: international organisations, representative bodies, the judiciary, independent reviewers, and the press. Like the layers of security in airports around the world, the more interlocking are those layers, the stronger we are. The challenge is not to turn into a surveillance society.

There is no doubt that we are creating societies in which we are feeling more "watched". Governments' focus on "people of interest" who are suspected of terrorist acts, or who are merely "suspected of being affiliated" with terrorists, undoubtedly contributes to this. In such an environment, anyone who fits someone else's idea of a terrorist is suspect. But racial profiling must not be incorporated into our vigilance. What affects segments of our societies ultimately affects us all. While Muslim men of a certain age and background may be coming under increased scrutiny today, tomorrow it could be pregnant women in red dresses.

As widely reported in Australia, especially after the incident involving Dr Haneef, a "corrosive effect" was felt in Muslim communities in that country. This led to the creation of a "deep cynicism"[741] across broader bands of Australian society, a troubling development inasmuch as the security of all depends on people's ability to trust and work with their government, especially in cases of counterterrorism. Alienating a sector of the community that could hold answers has become a very real risk, not just in Australia but around the world. We must be vigilant, but within limits.

In a recent speech Janet Napolitano, current US Secretary of the Department of Homeland Security, asked citizens for help in the "war on terror". While people in the community who have information can be of undeniable assistance to government, care must be taken not to become effective government informants. In her speech, Napolitano touched on this sentiment. Stressing that she was not advocating the creation of "a culture of spying on one another," she still recommended that everyone be involved, including children: "There's actually an important role we can play in educating even our very young about watching for, and knowing what to do, if you're in an airport and you see a package left with no one around…."[742] While it is one thing to teach our children about "stranger danger," we must ask ourselves if involving children in policing is not going a step too far.

Normalising terror by internalising the possibility of terrorist attacks in our daily lives, while perhaps creating more vigilance, also has the potential to create a climate of fear in which reactionary laws and premature programmes will continue to be fostered.[743] As history has taught

---

741 Mark Rix "With Reckless Abandon: Haneef and Ul-Haque in Australia's 'War on Terror'", above n 730, at 118.

742 Philip Dru "US Enlists Citizens in Anti-terrorism Strategy" (30 July 2009) New World Order Truth < www.nwotruth.com> (accessed 25 August 2009).

743 For an interesting perspective on this phenomenon see Danny Keenan "The Logic of Terror" in Danny Keenan (ed) *Terror in Our Midst?,* above n 608, at 165-180.

us, when many early programmes that overstepped the bounds of privacy were reconsidered in the light of day, or after the perceived threat passed, they were frequently revised or funding was withdrawn (TIA and CAPPS II, for example). To avoid this occurring again, risking violating civil liberties and human rights, not to mention losing millions of dollars in misspent funds, it is incumbent on all of us to continue to be involved in the oversight of these programmes before they are activated.

This does not mean we ought not to invest in technology. But we invest in responsible, effective technology, that incorporates privacy protections at the outset, not after it has been deployed.[744]

Caution must also be exercised in developing new technologies so as not to rely on them overly and thereby create a false sense of security. They will never be a simple remedy for all our problems. This too, was a lesson hard-learned. In the days before 9/11, recommendations had been made to train airport screening staff. But because there had not been an incident of terrorism involving an American carrier in approximately ten years, there was a sense that "checkpoint screening was working."[745] Put in contemporary perspective, over-reliance on imprecise watch lists can actually lead to less effective vigilance and corresponding security. Watch lists are just one of several layers of security, they are not foolproof.

While the challenges ahead of us are varied, we have the wherewithal to create effective systems of protection and prevail over those who would do us harm. We just can't afford to let fear trump long-held democratic ideals. If we do, we run the risk of repeating history. And history's mistakes are best left remembered, but buried.

In the words of Benjamin Franklin:[746] "Any society that would give up a little liberty to gain a little security will deserve neither and lose both."

---

744 KA Taipale "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data" (December 2003) Columbia Science and Technology Law Review vol 5 no 2.

745 The Aviation Security System and the 9/11 Attacks, Staff Statement no 3, 7 <www.9-11commission.gov>.

746 Pennsylvania Assembly: Reply to the Governor, 11 November 1755.