THE CHALLENGE TO PRIVACY FROM EVER INCREASING STATE SURVEILLANCE: A COMPARATIVE PERSPECTIVE

KONRAD LACHMAYER* AND NORMANN WITZLEB**

I INTRODUCTION

A 'The 9/11 Effect'[1]

> Terrorism was not invented with the September 11, 2011 (9/11), terrorist attacks on the United States. Nevertheless, the coordinated attacks that killed almost 3,000 people were unprecedented as a single act of terrorism. So, too, was the global response to those events. Although individual countries had panicked and reacted to terrorism with repressive and ineffective laws and measures before, the response to 9/11 was an unprecedented global phenomenon. … All countries responded in a manner that reflected their own particular histories and legal, political, and social cultures.[2]

International terrorism poses serious threats to the societies it affects. The counter-terrorism measures adopted since 2001 have sought to limit the advance of terrorism but, in the process, also created enormous challenges for (transnational) constitutionalism. Long-held and cherished principles relating to democracy, the rule of law and the protection of a wide range of human rights have come under increasing strain. Legislative authority to shoot down hijacked aircrafts[3] or to use lethal drones against suspected terrorists[4] affect the right to

* Priv-Doz Dr Konrad Lachmayer is a Senior Lecturer at the Department of Constitutional and Administrative Law at the University of Vienna and a Senior Researcher at the Institute of Legal Studies of the Hungarian Academy of Sciences. The research for this article has been facilitated by a Monash University Faculty of Law International Collaboration Grant. A former version of this article was presented at a workshop of the International Association of Constitutional Law Research Group on Constitutional Responses to Terrorism: Konrad Lachmayer, 'Rethinking Privacy beyond Borders' (Paper presented at the Constitutionalism across Borders in the Struggle against Terrorism Workshop, Harvard Law School,7 March 2014).

** Dr Normann Witzleb is a Senior Lecturer at Monash University, Melbourne.

1 Kent Roach, *The 9/11 Effect: Comparative Counterterrorism* (Cambridge University Press, 2011).

2 Ibid 1.

3 Oliver Lepsius, 'Human Dignity and the Downing of Aircraft: The German Federal Constitutional Court Strikes Down a Prominent Anti-terrorism Provision in the New *Air-Transport Security Act*' (2006) 7 *German Law Journal* 761, 766–72.

4 See David Cole, 'How We Made Killing Easy' on NYRblog, The New York Review of Books, *NYRblog* (6 February 2013) <http://www.nybooks.com/blogs/nyrblog/2013/feb/06/drones-killing-made-easy>; Jamie L Kleidman, 'The Constitutionality of the Predator Drone Program' (2010) 4 *Vienna Journal on International Constitutional Law* 359.

life; waterboarding of prisoners and other inhumane practices contravene the prohibition of torture;[5] extraordinary renditions and black sites circumvent constitutionally protected rights and processes, including the right to freedom and security,[6] the right to a fair trial and due process for suspected terrorists;[7] ill-defined terrorism offences undermine the rule of law and personal freedom;[8] blanket suspicion of Muslims as terror sympathisers impacts on freedom of religion and leads to unfair discrimination;[9] and mass surveillance of communication sweeps away the right to privacy.

This article explores how internet surveillance in the name of counter-terrorism challenges privacy. In Part II, the article analyses the international dimension of counter-terrorism measures and the conceptualisation of data protection and privacy in the European Union ('EU'), the United States of America ('US') and Australia. Part III compares the different concepts of data protection and privacy, and explores the prospects of an international legal framework for the protection of privacy. Part IV concludes that work on international data protection and privacy standards, while urgently needed, remains a long-term vision with particularly uncertain prospects as far as anti-terrorism and national security measures are concerned.

B The Privacy Challenge

Counter-terrorism measures have broken many taboos regarding the rule of law in democratic countries. While torture, detention and interrogation target individuals in highly confronting ways, mass surveillance operates more subtly but affects the community at large. The erosion of core aspects of individual privacy can fundamentally alter the nature of human behaviour and interaction, our sense of personal freedom and the ethos of democratic societies.

The revelations in particular by the former Central Intelligence Agency ('CIA') contractor, Edward Snowden, have shown that massive surveillance of ordinary citizens on an unprecedented scale by law enforcement and national security agencies is now commonplace: it includes internet surveillance, video surveillance of public spaces, electronic eavesdropping, data retention, monitoring of bank accounts and social media, the sharing of air travel booking information, large scale intrusions into email, web chat and data held in cloud storage etc. Moreover, the different forms of data gathering can be combined

5 See Jeremy Waldron, 'Torture and Positive Law: Jurisprudence for the White House' (2005) 105 *Columbia Law Review* 1681.

6 Johan Steyn, 'Guantanamo Bay: The Legal Black Hole' (2004) 53 *International and Comparative Law Quarterly* 1.

7 Federico Fabbrini, 'The Role of the Judiciary in Times of Emergency: Judicial Review of Counter-Terrorism Measures in the United States Supreme Court and the European Court of Justice' (2009) 28 *Yearbook of European Law* 664; Christina Eckes, *EU Counterterrorist Policies and Fundamental Rights: The Case of Individual Sanctions* (Oxford University Press, 2010).

8 Roach, above n 1, 227–9.

9 See Jocelyne Cesari (ed), *Muslims in the West after 9/11: Religion, Politics and Law* (Routledge, 2010).

with sophisticated data mining,[10] dragnet investigations and big data analysis.[11] Technological developments which result in ever-increasing amounts of data logging our communications and recording our daily activities create new possibilities for covert risk profiling and discriminatory treatment that are often beyond legal challenge. In their totality, these forms of information technology-based counter-terrorism measures raise serious constitutional concerns.

The new possibilities for state surveillance to dig deep into our social interactions, behaviour, and personality do not stop at national borders. Data exchange between governments and agencies, cooperation with and inquiries at private companies, international agreements and security cooperation create new data that provide our own or foreign governments with further insight into our activities and intentions. Internet communications are subject to direct or indirect intrusion into computers, computer systems, clouds, private chat rooms, social media and email accounts.[12] Access to telecommunication networks does not only include eavesdropping on our conversations but also many informational by-products, including metadata and, in the era of smartphones, geolocation data. Wiretapping, the use of spy satellites and traditional foreign espionage supplement these sources of information.

These new surveillance practices are challenging the concept of privacy in many ways. Indeed, it can be asked how privacy can still be sensibly safeguarded in this new environment. In international human rights law, privacy enjoys significant but not unlimited protection. Article 12 of the *Universal Declaration of Human Rights* states that '[n]o 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.'[13] Likewise, the *International Covenant on Civil and Political Rights* ('*ICCPR*'),[14] the *Convention for the Protection of Human Rights and Fundamental Freedoms*, now known as the *European Convention on Human*

10 Fred H Cate, 'Government Data Mining: The Need for a Legal Framework' (2008) 43 *Harvard Civil Rights – Civil Liberties Law Review* 435.

11 Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013).

12 Regarding the changing role of the individual in international conventions relating transborder data flows, see Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013) 36–7.

13 *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948). On the continuing relevance of the Universal Declaration, see Jochen von Bernstorff, 'The Changing Fortunes of the Universal Declaration of Human Rights: Genesis and Symbolic Dimensions of the Turn to Rights in International Law' (2008) 19 *European Journal of International Law* 903.

14 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17. In relation to extraterritorial surveillance and interception of communication, there is also a jurisdictional issue of whether human rights instruments have application to foreign intelligence activities: see also Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2014) forthcoming *Harvard International Law Journal*.

Rights ('*ECHR*'),[15] and the *American Convention on Human Rights*[16] recognise respect for private life as a human right. Yet, privacy is not an absolute right. In practical terms, it is only guaranteed to the extent that it is not outweighed by countervailing public interests or by conflicting rights held by others. Under the *ECHR*, which probably contains the richest human rights jurisprudence relating to the right to privacy, conflicting human rights positions have to be resolved by reference to the principle of proportionality, under which each human right can only be limited as far as is necessary for the protection of the conflicting human rights. In the context of counter-terrorism measures, these will normally justify a curtailment of privacy for the protection of state security, public safety or public order.

While there is a shared discourse on the framework of privacy protection at an international level, international human rights instruments tend to give states a 'margin of appreciation'[17] as to how privacy is to be effected and how it is to be balanced against conflicting public interests. This has resulted in significant differences concerning the nature and precise extent of privacy protection between jurisdictions. Even among liberal Western democracies, there is no consensus regarding the status that privacy should enjoy at a constitutional level. In some countries, for example, Germany, constitutional jurisprudence plays a pivotal role in the protection of privacy. In other countries, such as Australia, privacy is not a constitutionally protected value.

Since the days of Warren and Brandeis,[18] debate on privacy has always been shaped by new technological developments. However, the contemporary dimension of intrusion goes far beyond previously existing technologies and is powerfully supported by anti-terrorism rhetoric. Cultural concepts of privacy have always varied between different states and societies in the world but the contemporary and emerging techniques of intrusion into privacy create a new global standard of possibilities. Privacy protections no longer keep up with these developments: neither nationally with the aim of limiting government usage of the new surveillance technologies nor internationally with the aim of adopting

---

15 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953), as amended by *Protocol No 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Amending the Control System of the Convention*, opened for signature 13 May 2004, CETS No 194 (entered into force 1 June 2010) art 8; see also Charter of Fundamental Rights of the European Union [2010] OJ C 83/389, arts 7–8.

16 *American Convention on Human Rights*, signed 22 November 1969, 1144 UNTS 17955 (entered into force 18 July 1978).

17 The 'margin of appreciation' is a doctrine developed by the European Court of Human Rights. The term refers to the space for manoeuvre that is accorded to national authorities in fulfilling their obligations under the European Convention on Human Rights. The margin of appreciation differs depending on the circumstances of the case and the rights and freedoms engaged. See, eg, Dean Spielmann, 'Whither the Margin of Appreciation?' (Speech delivered at the Current Legal Problems Lecture Series, University College London, 20 March 2014) <http://www.echr.coe.int/Documents/Speech_20140320_London_ENG.pdf>.

18 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 195 (referring to 'recent inventions' such as '[i]nstantaneous photographs').

universal standards of privacy protection. Safeguarding privacy in times of terrorism requires the reaffirmation of the rule of law nationally and an intercultural dialogue on privacy internationally.[19]

II COUNTER-TERRORISM MEASURES AND THEIR IMPACT ON PRIVACY – COMPARATIVE INSIGHTS

A The European Union

1 Counter-Terrorism Surveillance Measures

During the last decade, the EU intensified its counter-terrorism activities in many ways.[20] After 9/11, initiatives to improve EU police and judicial cooperation in criminal matters included a strong counter-terrorism component.[21] The terrorist attacks in Madrid[22] and London[23] provided the political impetus for further expansion of these initiatives and led most prominently to the enactment of the so-called *Data Retention Directive*.[24] Based on the EU competence of legal harmonisation in the common market,[25] the *Data Retention Directive* aimed at harmonising the obligations of providers of public electronic communications services or networks to retain certain categories of traffic and location data generated or processed by them.[26] The categories included data necessary to trace and identify the source and the destination of any electronic (tele)communication as well as the date, time, duration and type of this communication.[27] While the *Data Retention Directive* expressly excluded retention of data revealing the content of the communication,[28] it created a highly contentious basis for privacy invasion by state authorities. The CJEU struck down the *Data Retention*

19 David Cole, 'Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism', in Fergal Davis, Nicola McGarrity and George Williams (eds), *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, 2014) 95.

20 See Cian C Murphy, *EU Counter-Terrorism Law: Pre-emption and the Rule of Law* (Hart Publishing, 2012).

21 See, eg, *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union* [2005] OJ C 53/1.

22 The Madrid train bombings took place on 11 March 2004.

23 The London bombings took place on 7 July 2005.

24 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54 ('*Data Retention Directive*'). See, eg, Theodore Konstadinides, 'Mass Surveillance and Data Protection in EU Law – The Data Retention Directive Saga' in Maria Bergström and Anna Jonsson Cornell (eds), *European Police and Criminal Law Cooperation* (Hart Publishing, 2013) 69.

25 The Court of Justice of the European Union ('CJEU') rejected an action for annulment on the basis of lack of competence. See *Ireland v European Parliament and Council of the European Union* (Court of Justice of the European Union, C-301/06, 10 February 2009).

26 *Data Retention Directive* [2006] OJ L 105/54, arts 1(1)–(2).

27 *Data Retention Directive* [2006] OJ L 105/54, art 5.

28 *Data Retention Directive* [2006] OJ L 105/54, art 5(2).

Directive in April 2014 as a disproportionate intrusion into the rights to privacy and data protection,[29] yet it continues to illustrate the status of personal data protection in Europe.

To understand its significance, it is important to recall some major elements of the *Data Retention Directive*. In its first recital the *Data Retention Directive* invoked data protection and the right to privacy; however, the *Data Retention Directive* primarily operated to limit and restrict these rights. While counter-terrorism provided the context for enacting the *Data Retention Directive*,[30] the *Data Retention Directive* itself expressed its purposes more widely. The data had to be retained, for a period between six months and two years, to 'ensure that [they] are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.'[31] In other words, the *Data Retention Directive* provided each member state with wide discretion to define the parameters for use of the retained data by its police, the judiciary or intelligence agencies, having regard to its own institutional and constitutional framework.[32] Its contested nature meant that the transposition of the *Data Retention Directive* into national law remained incomplete. When the German Constitutional Court declared the transposition of the *Data Retention Directive* into German law to be unconstitutional, the German government made no further attempt of transposition.[33] While the German Constitutional Court did not decide on compatibility of the *Data Rentention Directive* with the *German Constitution*, it held that the constitutional principle of proportionality demanded more detailed provisions regarding data security,

29 See *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung v Seitlinger* (European Court of Justice, C-293/12; C-59/14, 8 April 2014) [58].

30 See recital 10 of the *Data Retention Directive* [2006] OJ L 105/54: 'On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.'

31 *Data Retention Directive* [2006] OJ L 105/54, art 1(1).

32 The use of data was completely at the discretion of the member states. The *Data Retention Directive* only required the member states to adopt rules for data retention for telecommunication providers, but did not regulate in which form, if any, member state authorities used such data other than providing that the procedure and conditions for access

> in accordance with necessity and proportionality requirements shall be defined by each member state in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Data Retention Directive [2006] OJ L 105/54, art 4.

33 Bundesverfassungsgericht [German Constitutional Court], 1 BvR 256/08, 2 March 2010 reported in (2010) BVerfGE 125, 260. See also Christian DeSimone, 'Pitting Karlsruhe against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive' (2010) 11 *German Law Journal* 291.

transparency and legal protection in the German Act transposing the *Data Retention Directive*.[34]

The majority of member states have limited the purpose of data retention to serious crime, but in 2011 there were eight member states which allowed its use in relation to all criminal offences and for crime prevention, or on general grounds of national or state and/or public security.[35] The *Data Retention Directive* was not unusual in this regard.[36] New police and judicial powers have often been introduced as counter-terrorism measures but have then been made available to all (or at least many others) forms of criminal activities, especially organised crime. Once anti-terrorism has been used as the political justification for introducing a particular measure, there is a temptation for police and other agencies to lobby for an expansion of the new powers to deal with other forms of criminality.

The *Data Retention Directive* was just one, but a prominent, example of EU counter-terrorism policy.[37] Other activities related to counter-terrorism and the use of personal data include the establishment and development of Europol,[38] the establishment of EU Intelligence Analysis Centre,[39] the Schengen Information System,[40] the *Prüm Convention*,[41] European Criminal Records Information

34 See with regard to legal challenges in other countries Chris Jones and Ben Hayes, 'The EU Data Retention Directive: A Case Study in the Legitimacy and Effectiveness of EU Counter-Terrorism Policy' (Report No D2.4, Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness, 7 November 2013) 22 <http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf>.

35 *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)* [2011] COM(2011) 225, 6.

36 See Maria Tzanou, 'The EU as an Emerging "Surveillance Society": The Function Creep Case Study and Challenges to Privacy and Data Protection' (2010) 4 *Vienna Journal on International Constitutional Law* 407.

37 Francesca Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) 8 *Chicago Journal of International Law* 233.

38 See *Council Decision of 6 April 2009 Establishing the European Police Office (Europol) (2009/371/JHA)* [2009] OJ L 121/37; see also *Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and Repealing Decisions 2009/371/JHA and 2005/681/JHA*, Communication [2013] COM(2013) 173.

39 Rhodri Jeffreys-Jones, *In Spies We Trust: The Story of Western Intelligence* (Oxford University Press, 2013) 212–29.

40 See Jens-Peter Schneider, 'European Information Systems and Data Protection as Elements of the European Administrative Union' in Dieter Dörr and Russell L Weaver (eds), *The Right to Privacy in the Light of Media Convergence: Perspectives from Three Continents* (De Gruyter, 2012) 374, 380–2.

41 See *Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the Stepping Up of Cross-Border Cooperation, Particularly in Combating Terrorism, Cross-Border Crime and Illegal Migration*, signed 27 May 2005, 2617 UNTS 46562 (entered into force 1 November 2006) ('*Prüm Convention*'); see also the implementation of the *Prüm Convention* into the EU legal framework by *Council Decision (2008/615/JHA) on the Stepping Up of Cross-Border Cooperation, Particularly in Combating Terrorism and Cross-border Crime* [2008] OJ L 210/1 ('*Council Decision (2008/615/JHA)*').

System,[42] and the attempts to establish a 'principle of availability' in police cooperation[43] and to enact an EU Passenger Name Record ('EU PNR') directive.[44]

All these counter-terrorism measures have had a dimension extending beyond the EU. The *Data Retention Directive* did not focus on EU citizens but on all communications which utilised telecommunication infrastructure located in the EU.[45] This affected all persons using the internet within the EU, but also persons outside the EU who used telecommunication providers and their services on EU territory or by EU providers. Moreover, the storage of data leads to communication data with regard to persons outside the Union, for example, if somebody inside the EU contacts a person, an email address or a website outside the EU.

European counter-terrorism measures are enforced within the EU but they are intended to gain as much data as possible, also beyond the EU territory. The international reach, which is characteristic of the 'new' forms of terrorism, requires cross-border strategies also for the fight against it. The EU is therefore part of international agreements to foster cooperation against international terrorism: the prominent examples are the *Terrorist Finance Tracking Program Agreement* ('*TFTP Agreement*')[46] and the *Passenger Name Record Agreements* ('*PNR Agreements*')[47] with the US or Australia. Other initiatives, like the efforts for an EU-PNR directive[48] or Europol's cooperation agreements with non-EU

42 See *Council Framework Decision 2009/315/JHA on the Organisation and Content of the Exchange of Information Extracted from the Criminal Record between Member States* [2009] OJ L 93/23; *Council Decision 2009/316/JHA of 6 April 2009 on the Establishment of the European Criminal Records Information System (ECRIS) in Application of Article 11 of Framework Decision 2009/315/JHA* [2009] OJ L 93/33.

43 See *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union* [2005] OJ C 53/1.

44 See *Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime* [2011] COM(2011) 32.

45 *Data Retention Directive* [2006] OJ L 105/54, art 3(2):

> The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned.

46 *Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program* [2010] OJ L 195/5; see also Ariadna Ripoll Servent and Alex MacKenzie, 'The European Parliament as a "Norm Taker"? EU-US Relations after the SWIFT Agreement' (2012) 17(2/1) *European Foreign Affairs Review* 71.

47 *Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security* [2012] OJ L 215/5; *Agreement between the European Union and Australia on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs and Border Protection Service* [2012] OJ L 186/4.

48 See European Commission, above n 44.

countries,[49] also show the intention of the EU to cooperate on information sharing internationally.[50]

2 Data Protection and Counter-Terrorism

The centrepiece of EU regulation in the field of data protection is *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* ('*Directive 95/46/EC*').[51] Like all directives, it is addressed to the member states and required transposition into national law through the enactment of data protection legislation in each member state. Even though the directive established minimum standards of data protection in all EU member states,[52] its scope of application has expressly been limited to exclude data protection in the context of public and state security, defence, as well as criminal law. Post 2001, member states relatively quickly agreed on the necessity of EU-wide counter-terrorism measures but the negotiations for a more general EU data protection framework in the field of police cooperation were a relatively lengthy process. However, in 2008, the EU adopted *Council Framework Decision 2008/977/JHA of 27 November 2009 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters*,[53] which is still in force.

This *Framework Decision* requires member states to 'protect the fundamental rights and freedoms of natural persons' when their personal data are processed 'for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[54] In article 13, the *Framework Decision* imposes conditions on the data transfer by national authorities to third states and international bodies. These conditions include that the transfer must be necessary for criminal law enforcement; must only be to competent authorities; and that the recipient state or international body ensures an adequate standard of data protection. However, the exclusion of some of the most important forms of cooperation, like the Schengen Information System, Europol or the *Prüm Convention*,[55] has significantly limited the protections provided by the *Framework Decision*.[56] In relation to exchange of information for

---

49 See Europol, *External Cooperation* (2014) <https://www.europol.europa.eu/content/page/external-cooperation-31>.

50 The EU, however, also took over international security strategies of the US, see Javier Argomaniz, 'When the EU Is the "Norm-Taker": The Passenger Name Records Agreement and the EU's Internalisation of US Border Security Norms' (2009) 31 *Journal of European Integration* 119.

51 [1995] OJ L 281/31.

52 See Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2nd ed, 2007).

53 [2008] OJ L 350/60 ('*Framework Decision*').

54 *Framework Decision* [2008] OJ L 350/60, art 1(2).

55 See *Prüm Convention*; see also the implementation of the *Prüm Convention* into the EU legal framework by *Council Decision (2008/615/JHA)* [2008] OJ L 210/1.

56 *Framework Decision* [2008] OJ L 350/60, recital 39.

counter-terrorism, the scope of the *Framework Decision* is further reduced by its article 1(4), which provides that the *Framework Decision* is 'without prejudice to essential national security interests and specific intelligence activities in the field of national security'. Moreover, some rights are subject to exceptions, which can make it difficult for individuals to obtain effective legal protection. For example, while article 17 guarantees the right of the individual to access processed personal data, this right can be restricted in national legislation and the reasons for restriction are formulated in very broad terms.[57]

The *Lisbon Treaty*,[58] which entered into force in 2009, completely changed the institutional arrangements for police and judicial cooperation as well as for data protection in the EU. Because of the integration of the so-called 'third pillar' (ie police and judicial cooperation in criminal matters), matters of police cooperation, including Europol, are now dealt with in articles 87–9 of the *Treaty on the Functioning of the European Union* ('*TFEU*').[59] This means that relevant measures, including instruments concerning the 'collection, storage, processing, analysis and exchange of relevant information'[60] now fall under the ordinary legislative procedure. This simplifies the process for the adoption of new counter-terrorism measures and strengthens the role of the European Parliament. As a further important change, the *Charter of Fundamental Rights* ('*CFR*') has become binding EU constitutional law. Article 8 of the *CFR* includes a right to the 'protection of personal data'.[61] This right is complemented by the provision of article 16 of the *TFEU*, which confirms this right and guarantees the competence of the Union to regulate data protection for the whole Union including its member states.

---

57 See *Framework Decision* [2008] OJ L 350/60, art 17(2), which allows restrictions which are a necessary and proportional measure:

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the data subject or the rights and freedoms of others.

58 *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, signed 13 December 2007, [2007] OJ C 306/1 (entered into force 1 December 2009) ('*Lisbon Treaty*').

59 The *TFEU* also widened the mandate of Europol: *Consolidated Version of the Treaty on the Functioning of the European Union* [2010] OJ C 83/47, art 88(1).

60 *TFEU* [2010] OJ C 83/47, art 88(2)(a).

61 *Charter of Fundamental Rights of the European Union* [2000] OJ C 364/01, art 8 ('*CFR*'):

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

This new European constitutional situation with regard to data protection after the *Lisbon Treaty* has provided the basis for developing a new data protection framework. In January 2012, the EU Commission presented proposals[62] for a regulation setting out a general EU framework for data protection (to replace *Directive 95/46/EC*)[63] and for a directive on the protection of personal data processed for the purposes of criminal law enforcement (to replace *Framework Decision 2008/977/JHA*).[64] After an extensive review by the Civil Liberties, Justice and Home Affairs Committee of the European Parliament ('LIBE Committee'), with the general aim of achieving more clarity and a more appropriate balance between the conflicting human rights positions,[65] a modified proposal is currently awaiting further parliamentary action.

The *Draft Directive*[66] is concerned with the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences.[67] This also includes offences related to terrorism. However, the *Draft Directive* is not intended to apply to the processing of personal data 'in the course of an activity which falls outside the scope of Union law, in particular concerning national security',[68] or to data processed 'by the Union institutions, bodies, offices and agencies', such as Europol or Eurojust.[69] The *Draft Directive* therefore still suffers from some of the deficiencies of the framework decision it would replace, but it would nonetheless be a major step towards fostering a European approach to data protection with regard to counter-terrorism activities.

---

62 Summarised by Viviane Reding, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2 *International Data Privacy Law* 119.

63 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* [2012] COM(2012) 11. In contrast to a directive, a regulation is directly applicable in the member states, without the need for national transposition: *TFEU* [2010] OJ C 83/47, art 288.

64 *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data* [2012] COM(2012) 10 ('*Draft Directive*').

65 Eg, the LIBE Committee introduced new provisions with regard to further processing for incompatible purposes (article 7a), the processing of genetic data (article 8a), general principles for data subject rights (article 10a), a data protection impact assessment (article 25a), joint operations (article 48a), and transmission of personal data to other authorities or private parties in the Union (article 55a): Committee on Civil Liberties, Justice and Home Affairs, European Parliament, *Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),* A7-0402/2013.

66 For a comparison between the *Framework Decision* [2008] OJ L 350/60 and the *Draft Directive* [2012] COM(2012) 10, see Reding, above n 62, 122–3.

67 *Draft Directive* [2012] COM(2012) 10, art 1(1).

68 *Draft Directive* [2012] COM(2012) 10, art 2(3)(a). Matters relating to national security and intelligence agencies are not included in the competences of the European Union.

69 *Draft Directive* [2012] COM(2012) 10, art 2(2)(b), recital 15.

Any reform of the EU data protection framework now also needs to have regard to the statements contained in the decision of the CJEU on the *Data Retention Directive*. In this important decision, the Court held that the *Data Retention Directive* was invalid because it constituted a disproportionate interference with the right to respect for private life and with the right to the protection of personal data, as enshrined in articles 7 and 8 of the *CFR* respectively.[70] The Court held that the EU legislator had failed to establish 'clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards' against abuse and unlawful access of the data retained.[71] The *Data Retention Directive* was held to apply too broadly because it did 'not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.'[72] The *Data Retention Directive* further failed to 'lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences'.[73] Many of the deficiencies of the *Data Retention Directive*, including the vague definition of the purpose and limits of data retention, can be attributed to competence issues. At the time of its enactment in 2006, a framework decision concerning police and judicial cooperation in criminal matters would have required unanimity of Council. When this was unattainable, the *Data Retention Directive* was based on the 'harmonisation competence' of the internal market, which allowed its enactment with a qualified majority but did not enable it to address issues of police and judicial cooperation in criminal matters.

While the decision of the CJEU does not preclude the enactment of a new directive on data retention, now based on the broader competence of the *Lisbon Treaty*, such an initiative is currently unlikely. In any event, it would need to carefully consider the Court's statements relating to the definition of the purpose and limits of data retention, as well as of the substantive and procedural safeguards that would apply to access and subsequent use of the data by competent national authorities. In the meantime, each member state is called upon to determine the scope and limits of data retention in its national laws, having regard to its specific constitutional framework.[74]

The preceding discussion of the EU instruments in the field of data protection demonstrates the significance of the multiple constitutional protections existing in this area – specifically, the right to the protection of personal data in article 8

70 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung v Seitlinger* (European Court of Justice, C-293/12; C-59/14, 8 April 2014) [69].

71 Ibid [54].

72 Ibid [58].

73 Ibid [60].

74 Most recently the Austrian Constitutional Court declared the Austrian statutory provisions on data retention to be 'an excessive interference' with the right to data protection and declared them to be void and unconstitutional: Verfassungsgerichtshof [Austrian Constitutional Court], G 47/2012, 27 June 2014.

of the *CFR* and, more generally, the right to respect for one's private life in article 7 of the *CFR* and article 8 of the *ECHR*.[75] The strength of these constitutional protections has been confirmed in the CJEU's judgment on the *Data Retention Directive*. The proposed new data protection framework of the EU is expected to build upon these foundations and to create an effective approach towards the collection, storage and use of personal data by police and criminal authorities. However, the activities of intelligence agencies and their use of personal data will remain within the domestic sphere of the member states and, thus, be outside the purview of the EU's data protection regime.

3 International Dimension

The new EU data protection framework for police and judicial cooperation also provides general principles for the international transfer of personal data (article 33 of the *Draft Directive*). Personal data can be transferred to third countries or international organisations if this is necessary for criminal law enforcement and provided that there is either an adequacy decision of the European Commission (article 34 of the *Draft Directive*) or that appropriate safeguards (article 35 of the *Draft Directive*) are in place. In addition to these formal avenues, article 36 of the *Draft Directive* allows derogations from articles 34 and 35 to transfer personal data to a third country in exceptional circumstances, for example, if 'the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country',[76] which may cover cases of a specific terror threat. The transfer is also possible if, more broadly, it is 'necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[77] The European Parliament adopted amendments to the *Draft Directive* proposed by the LIBE Committee, which provided further safeguards including a prohibition on the 'frequent massive transfer of data' and strict limitations on transfers on the basis of derogations.[78] The overall concept of derogation possibilities, however, has remained the same.

---

75 *CFR* [2000] OJ C 364/01, art 52(3): 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

76 See *Draft Directive* [2012] COM(2012) 10, art 36(2)(c).

77 See *Draft Directive* [2012] COM(2012) 10, art 36(2)(d).

78 See European Parliament, Legislative Resolution of 12 March 2014 on the *Draft Directive*, A7-0403/2013, Amendment 99, art 36:

> 2b. All transfers of data decided on the basis of derogations shall be duly justified and shall be limited to what is strictly necessary, and frequent massive transfers of data shall not be allowed.
>
> 2c. The decision for transfers under paragraph 2 [refers to the possibility of derogation] must be made by duly authorised staff. These transfers must be documented and the documentation must be made available to the supervisory authority on request, including the date and time of the transfer, information about the recipient authority, the justification for the transfer and the data transferred.

Notably, the EU also puts data protection policy on its foreign affairs agenda.[79] Article 38 of the *Draft Directive* tasks the Commission and the member states with improving international cooperation regarding the protection of personal data. The Union aims to 'develop effective international cooperation mechanisms to facilitate the enforcement of legislation for the protection of personal data', 'international mutual assistance in the enforcement of legislation for the protection of personal data' and to 'promote the exchange and documentation of personal data protection legislation and practice'.[80] Thus, the EU's data protection regime with regard to police and judicial cooperation does not only affect third countries who wish to cooperate with the EU but the Union seeks to export its own visions and concepts of data protection into the world.

4 Conclusion

The scourge of international terrorism provided the impetus for counter-terrorism measures at the European level, including initiatives like EU's *Data Retention Directive*, which sought to create a legal framework for storing internet and (tele)communication traffic data for law enforcement and national security purposes. The European counter-terrorism measures are not limited to EU citizens or EU territories but affect international communication with links to the territory of the Union. Moreover, these measures are not restricted to counter-terrorism but member states are free to allow their use for other law enforcement purposes, especially regarding serious crime.

Alongside the Europeanisation of information technology-based counter-terrorism measures have been attempts to foster data protection in the Union. The recent CJEU's decision on the invalidity of the *Data Retention Directive* underlines the value attached to privacy in the EU legal order. The new *Draft Directive* on data protection concerning police and judicial cooperation would definitely be a major achievement, but nevertheless has significant loopholes. It is only directed at member states and thus does not apply to Europol. Broad provisions allowing international cooperation to take place on the basis of derogation clauses mean that the *Draft Directive*'s requirements for adequacy or appropriate safeguards can be sidestepped. Lastly, and most importantly, national security and the activities of intelligence agencies are not included in the EU framework. The current and future European frameworks therefore still leave much room for national counter-terrorism activities, including mass surveillance, that do not need to abide by the EU data protection regime.

79 On the EU strategies to extend the scope of application of the EU's *Data Protection Directive*, see Lokke Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1 *International Data Privacy Law* 28.

80 See *Draft Directive* [2012] COM(2012) 10, art 38(1).

B The United States

1 Counter-Terrorism Surveillance Measures

The US response to 9/11 dramatically altered many aspects of US law, both domestically and regarding its international legal relations. This includes most prominently the treatment of terror suspects in Guantánamo and elsewhere with all its implications ('enemy combatants', 'military trials', 'black sites'),[81] but also the *USA PATRIOT Act*[82] ('*Patriot Act*') and the massive surveillance of domestic and internationals by the National Security Agency ('NSA').[83] The analysis of more than 10 years of US surveillance shows that the legal response to terrorism has the following characteristics: measures have been based on the exercise of legislative as well as executive powers; there is a sharp cleavage between the constitutional protections afforded to US citizens and the significantly lesser protections enjoyed by foreigners;[84] and there has been reliance on a variety of extra-legalistic concepts to avoid legal obligations that would otherwise apply.[85]

The most prominent reaction to 9/11 with regard to surveillance was the *Patriot Act*. As Banks has noted, the

> Patriot Act is hardly a code for fighting the war on terrorism, nor one for saving the US homeland from another attack. Instead, it is an amalgam of often unrelated pieces of authority, most of which simply amend existing laws, and the larger share of which are unremarkable complements to existing authority.[86]

The *Patriot Act* provided the Federal Bureau of Investigation ('FBI') with greater powers in the conduct of national security investigations. Independently of courts, the FBI can issue National Security Letters to obtain simplified access to various information sources, such as the internet, libraries, bank accounts, car dealers, post offices, casinos.[87] The *Patriot Act* also provides the basis for the bulk collection by the NSA of telephone call records or metadata. This program, which records the calling and receiving phone number, as well as time and date of most US phone calls but not their contents, has been periodically approved by a special secret court, the Foreign Intelligence Surveillance Court ('FISC') pursuant to section 215 of the *Patriot Act*.[88]

---

81 William C Banks, 'The United States a Decade after 9/11' in Victor V Ramraj et al (eds), *Global Anti-terrorism Law and Policy* (Cambridge University Press, 2nd ed, 2012) 449, 453–60; Roach, above n 1.

82 The title of this 2001 Act (Pub L No 107-56, 115 Stat 272) is a 'backronym' that stands for *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.*

83 Roach, above n 1, 184–6.

84 Milanovic, above n 14.

85 Roach, above n 1, 163.

86 Banks, 'The United States a Decade after 9/11', above n 81, 470.

87 Andrew E Nieland, 'National Security Letters and the Amended *Patriot Act*' (2007) 92 *Cornell Law Review* 1201.

88 This program has come under sharp criticism by the Privacy and Civil Liberties Oversight Board, an independent agency appointed by the US President and approved by Congress, which calls for its abolition: David Medine et al, 'Report on the Telephone Records Program Conducted under Section 215 of the *USA PATRIOT Act* and on the Operations of the Foreign Intelligence Surveillance Court' (Report, Privacy and Civil Liberties Oversight Board, 23 January 2014).

Under another program, the US government collects in the so-called 'PRISM' database, the content of electronic communications, including phone calls and emails, where the targets are reasonably believed to be non-US persons located outside the US. Amendments of the *Foreign Intelligence Surveillance Act* ('*FISA*') opened up the possibility of undertaking such electronic surveillance by authorisation of the Director of National Intelligence.[89] This surveillance program, which had been established on administrative authorisation, was legitimised by section 702 of the *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*.[90] *FISA* procedures bypassed traditional approaches towards criminal investigations (warrant process) and fostered increased cooperation between intelligence agencies and law enforcement.[91]

The *Patriot Act* and *FISA* are the most relevant federal Acts but different levels of administration, including the US President, the US government, law enforcement and intelligence agencies have introduced numerous further surveillance programs.[92] The US model of surveillance has therefore been described as an executive model of counter-terrorism.[93] The government enabled various counter-terrorism surveillance programs without congressional approval, with legislation also often strengthening the surveillance powers of the administration. Temporary measures have often become permanent and the complexity of the rules has been steadily increasing. The strengthening of administrative powers goes along with closer cooperation between intelligence agencies and law enforcement agencies and the weakening of judicial controls. More recently, Congress has begun to engage in more intense scrutiny of the intelligence services and their surveillance programs. The *USA Freedom Act*,[94] which has passed the House of Representatives and is currently before the Senate, seeks to restrict the surveillance activities under *FISA*, in particular the bulk collection of telephony metadata, and imposes further requirements on police authorities regarding the use of personal data, but also extends the *Patriot Act* until 2017.

Many forms of surveillance target international communication inside and outside US territory. The US has concluded various international agreements regarding surveillance. The *UKUSA Agreement*, a treaty between Australia, Canada, New Zealand, the UK and the US for joint cooperation in signals

89 50 USC §§ 1801–85.

90 Pub L No 110-261, 122 Stat 2436.

91 David Cole, 'English Lessons: A Comparative Analysis of UK and US Responses to Terrorism' (2009) 62 *Current Legal Problems* 136.

92 William C Banks, 'The Death of FISA' (2007) 91 *Minnesota Law Review* 1209, 1275–6; Stephanie K Pell, 'Systematic Government Access to Private-Sector Data in the United States' (2012) 2 *International Data Privacy* Law 245, 249–54; Cate, above n 10, 444–51.

93 Daphne Barak-Erez, 'Terrorism Law between the Executive and Legislative Models' (2009) 57 *American Journal of Comparative Law* 877.

94 Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act, HR Res 3361, 113th Congress (2014) ('*USA Freedom Act*').

intelligence (also known as 'Five Eyes'), or the *TFTP Agreement*[95] are prominent examples. The possibilities of the US regarding international surveillance are enormous and, as the Snowden revelations have confirmed, the potential is used extensively. As US companies play a crucial role in internet communication, surveillance inside the US territory opens up manifold possibilities regarding international communication networks. While US surveillance has broad international reach,[96] the level of protection afforded to foreigners against excessive or unwarranted surveillance is very low. Under the US constitutional system, civil liberties are generally assumed to depend on citizenship, providing foreigners with very limited protection.[97] This also applies to the protection of privacy under the Fourth Amendment.[98] The constitutional assessment of anti-terrorism measures therefore draws a sharp distinction between surveillance involving US persons and surveillance on non-US persons.[99] However, in practice, the US counter-terrorism programs initiated by the administration have often not been able to uphold this distinction. Much surveillance is sweeping and affects all kinds of personal information, frequently affecting foreigners as well as US persons alike.

The political debate on the US surveillance program in the US is likely to remain focused on US interests. Foreigners not permanently residing in the US can only expect a reprieve from continued US intrusion if the surveillance, by chance or by necessity, also affects the legal rights of US citizens or residents, or if the international diplomatic process brings home to the US administration that a particular form of surveillance does more harm than good to US interests. However, the recent scandals involving US interception of telecommunications by foreign heads of state including German Chancellor Angela Merkel[100] and the US administration's response to them, demonstrate that even powerful allies encounter difficulties in seeking assurances that they be exempt from surveillance.

---

95 *Terrorist Finance Tracking Program Agreement* [2010] OJ L 195/5.

96 Gehan Gunasekara, 'The "Final" Privacy Frontier? Regulating Transborder Data Flows' (2007) 17 *International Journal of Law and Information Technology* 147, 161–2.

97 On the constitutional right to habeas corpus of non-US nationals imprisoned in Guantanamo, see, eg, *Boumediene v Bush*, 553 US 723 (2008).

98 *United States v Verdugo-Urquidez*, 494 US 259 (1990).

99 This differentiation between US persons and non-US persons also underlies the constitutional analysis by the Privacy and Civil Liberties Oversight Board: see David Medine et al, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the *Foreign Intelligence Surveillance Act*' (Report, Privacy and Civil Liberties Oversight Board, 2 July 2014) <http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf>.

100 See, eg, Philip Sherwell, 'Barack Obama "Approved Tapping Angela Merkel's Phone 3 Years Ago"', *The Telegraph* (online), 27 October 2013 <http://www.telegraph.co.uk/news/worldnews/europe/germany/10407282/Barack-Obama-approved-tapping-Angela-Merkels-phone-3-years-ago.html>.

2 Privacy and Counter-Terrorism

The US concept of privacy has a number of legal dimensions: first, the *US Constitution* provides some privacy guarantees, especially in the Fourth Amendment,[101] which protects individuals against unreasonable searches and seizures. The case law of the US Supreme Court ('Supreme Court') developed certain standards of constitutional protection of privacy, which are, however, very ambivalent. The courts have also developed a common law right to privacy, including a right to be left alone, allowing suits for damages and injunctions through a private cause of action. Private law protection of privacy is relatively weak because freedom of speech, the value with which privacy is often in conflict, enjoys a high degree of constitutional protection in the First Amendment.

In federal data protection legislation, the *Privacy Act 1974* ('*Privacy Act*') is of particular note.[102] It imposes standards that bind a federal agency in its collection, use, maintenance and disclosure of personally identifiable information. It creates statutory privacy rights for US citizens and legal permanent residents but does not cover visitors or aliens. Non-US persons can nonetheless benefit from the protections of the *Privacy Act*, when agencies, such as the US Department of Homeland Security, apply its provisions to data repositories that contain personal information of US persons and non-US persons.[103] A further limitation of the *Privacy Act* is that it does not apply to records created or held by the intelligence agencies. As a result many new surveillance possibilities established for anti-terrorism purposes stand outside or displace the *Privacy Act*.[104]

The most relevant restriction on surveillance is the Fourth Amendment to the *US Constitution*. In the landmark decision of *Katz v United States*,[105] the Supreme Court provided some protection for individual privacy against state surveillance, but the judgment did not lead to the development of broadly-based privacy jurisprudence.[106] The Supreme Court held that the government intrudes upon a person's 'reasonable expectation of privacy', and violates an individual's rights under the Fourth Amendment, if it overhears that person's private conversations by means of a listening device attached to the outside of a public phone booth. Yet, subsequent case law demonstrates that the protection under the Fourth Amendment is incomplete in an important respect: any personal information,

---

101 Stephen J Schulhofer, *More Essential Than Ever: The Fourth Amendment in the Twenty-First Century* (Oxford University Press, 2012) 144–68.

102 5 USC § 552a. See Andrew Charlesworth, 'Clash of the Data Titans? US and EU Data Privacy Regulation' (2000) 6 *European Public Law* 253, 259–60.

103 Hugo Teufel III, 'Privacy Policy Guidance Memorandum' (Memorandum No 2007-1, US Department of Homeland Security, 7 January 2009) <https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf>.

104 If a specific Act on the use of personal data authorises this use (like *FISA*), the *Privacy Act* does not apply.

105 *Katz v United States*, 389 US 347 (1967) ('*Katz*').

106 See Thomas N McInnis, *The Evolution of the Fourth Amendment* (Lexington Books, 2009) 222–9.

which a person voluntarily communicates to a third party, such as to a bank (in *United States v Miller*)[107] or a telephone company (in *Smith v Maryland*)[108] no longer enjoys the protection of the Fourth Amendment.[109] These dicta import a significant limitation to privacy. Once a person is communicating personal data to someone else (including private business or individuals) the protection of the Fourth Amendment no longer applies. This provided the basis for section 215 of *FISA*, introduced through the *Patriot Act*, that empowers the FISC to issues orders on third parties to turn over information records that may assist investigations against international terrorism or clandestine intelligence activities.

While these various strands of constitutional, statute and case law create a patchwork of privacy protection, they constantly need to be adapted in light of technological developments that create new threats to privacy. In *United States v Jones*,[110] the Supreme Court recently decided on the reach of Fourth Amendment in the context of new tracking technologies. Jones was a suspected drug dealer and the police decided to attach a Global Positioning System ('GPS') tracking tool to his car, while it was parked in a public place. The Supreme Court found that this police conduct constituted an unconstitutional 'search' of the car, and was in violation of the Fourth Amendment. Instead of using the *Katz* test, the decision was based on a property-based conception of Fourth Amendment rights and held that the police had committed a trespass on the car. In their opinions, the Justices also put into doubt the principle that an individual has no reasonable expectation of privacy in information voluntarily disclosed to a third party.[111] But, for now, the extent to which this newer jurisprudence affects the longstanding decisions in *Miller* and *Smith* remains unclear.

In the very recent case of *Riley v California*,[112] the US Supreme Court recognised the significance of mobile phones as repositories of personal information and held that the Fourth Amendment prohibited the search of a cellphone without a warrant. Together with *Jones*, this decision shows the US Supreme Court's willingness to keep the privacy protections provided for in the *US Constitution* relevant to the contemporary technological context.

3 Conclusion

The US has dramatically extended its national and international surveillance activities since 9/11. The US administrative and extra-legal approach made it

107 *United States v Miller*, 425 US 435 (1976) ('*Miller*').
108 *Smith v Maryland*, 442 US 735 (1979).
109 McInnis, above n 106, 232–8.
110 *United States v Jones*, 132 S Ct 945 (2012) ('*Jones*').
111 See especially ibid 957 (Sotomayor J), 962–3 (Alito J). See also Federico Fabbrini and Mathias Vermeulen, 'GPS Surveillance and Human Rights Review: The European Court of Human Rights and the United States Supreme Court in Comparative Perspective' in Fergal Davis, Nicola McGarrity and George Williams (eds), *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, 2014) 134, 139–48.
112 *Riley v California*, 134 S Ct 2473 (2014).

possible to sidestep some of the constitutional restrictions that traditionally limited surveillance. The national and international criticism following the Snowden revelations of the largely unbridled development of US surveillance activities may now prompt a re-evaluation of some aspects of these activities. In January 2014, President Obama delivered a major speech calling for reforms to government surveillance programs, including those conducted by the NSA, to strengthen protections for privacy and civil liberties, improving transparency and oversight, and to rebuild trust among foreign leaders and citizens.[113] The US Congress has begun to exercise closer scrutiny and to implement law reform proposals that would improve privacy protections, including restraints on extra-legal surveillance as a counter-terrorism measure.[114]

Surveillance activities appear to be less extensive in relation to US citizens but some counter-terrorism measures are unable to differentiate according to citizenship or residence. In such cases, the Supreme Court may be called upon by US persons to develop the guarantees of the Fourth Amendment further.[115] Despite some newer developments, the protection of privacy regarding counter-terrorism activities faces many restrictions. Regarding the monitoring of US citizens, it will be the task of the Supreme Court to adapt the existing restraints, in particular the Fourth Amendment, to provide redress against new threats of undue government interference.

International surveillance by US agencies falls altogether outside US privacy protection. First of all, neither the *US Constitution* nor the US *Privacy Act* protects foreigners living abroad. International agreements between the US and the EU with regard to Passenger Name Records ('PNR'), which have established a particular regime of data protection, and a proposed data protection agreement relating to personal data shared with the US by EU countries for law enforcement purposes remain the exception. In the course of negotiations relating to this agreement, the US administration recently declared the intention to extend the protection guaranteed by the US *Privacy Act* to EU citizens.[116] Such an extension, however, would not affect the large-scale surveillance and collection activities by US intelligence agencies which will remain virtually beyond challenge by non-US citizens.

---

113 Barack Obama, 'Remarks by the President on Review of Signals Intelligence' (Speech delivered at the Department of Justice, Washington DC, 17 January 2014) <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>. See also Richard A Clarke et al, 'Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies' (Final Report, Review Group on Intelligence and Communication Technologies, 12 December 2013) <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

114 See, eg, the current *USA Freedom Act* initiative before Congress.

115 Cole, above n 19, 95–116.

116 See Ewen MacAskill, 'US to Extend Privacy Protection Rights to EU Citizens', *The Guardian* (online), 25 June 2014 <http://www.theguardian.com/world/2014/jun/25/us-privacy-protection-rights-europe>.

C Australia

1 Counter-Terrorism Surveillance Measures

While Australia has not suffered devastating terrorist attacks in its own territory,[117] the Australian Parliament established a wide spectrum of far-reaching counter-terrorism measures after 9/11. Politically inspired by counter-terrorism legislation in the US and the UK, Australia's 'hyper-legislation'[118] has created new anti-terrorism offences and provided the Australian Security Intelligence Organisation ('ASIO') and other agencies with myriad new powers.[119] These developments need to be assessed in the context of Australia's system for protection of human rights, which now stands unique among Western democracies. The absence of a constitutional Bill of Rights at the federal level means that the High Court has few powers to invalidate excessive anti-terrorism laws. Instead, it is the Australian Parliament that has primary responsibility for balancing and upholding human rights. Under Australia's bicameral parliamentary system, the chances of effective scrutiny of legislation often depend on the Senate, representing the Australian states and territories, with such scrutiny being more likely when the Senate is not controlled by the party forming the Commonwealth government. However, much of Australia's anti-terrorism legislation has been bipartisan and rushed through Parliament in a climate of fear and urgency,[120] as a result of which Senate amendments of Bills are often focused on specific issues rather than the overall trend and effect of the legislation.

The academic debate on counter-terrorism measures seems to have focused on the new offences and the expansion of coercive powers, such as questioning and detention powers, given to ASIO and other law enforcement agencies.[121] The extent to which the surveillance powers and capabilities have been enhanced has received much less attention.[122] This is despite the fact that the *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIA*') has been amended numerous times since 2001. The *TIA* regulates the circumstances in which communications – both communications passing over a telecommunications network as well as stored communications – can be accessed by law enforcement agencies.[123] In his detailed analysis 'A Decade of Australian

117 The Bali Bombings of 12 October 2002 were, however, a major turning point in Australia's efforts to foster regional cooperation on counter-terrorism.

118 This term is used as the title of the chapter on Australia in Roach, above n 1, 309–60.

119 See Nicola McGarrity and George Williams, 'From Covert to Coercive: A New Model of Surveillance by Intelligence Agencies' in Fergal Davis, Nicola McGarrity and George Williams (eds), *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, 2014) 234.

120 See Nicola McGarrity and George Williams, 'Counter-Terrorism Laws in a Nation without a Bill of Rights: The Australian Experience' (2010) 2 *City University of Hong Kong Law Review* 45.

121 See Roach, above n 1.

122 But see Niloufer Selvadurai, Peter Gillies and Rizwanul Islam, 'Maintaining an Effective Legislative Framework for Telecommunication Interception in Australia' (2009) 33 *Criminal Law Journal* 34; Simon Bronitt and James Stellios, 'Telecommunications Interception in Australia: Recent Trends and Regulatory Prospects' (2005) 29 *Telecommunications Policy* 875.

123 A communication is a conversation or a message in whatever form, including speech or data: *TIA* s 5.

Anti-terror Laws', George Williams dedicates only one paragraph to surveillance measures:

> Section 5D of the *Telecommunications (Interception and Access) Act 1979* (Cth) includes divs 72, 101, 102 and 103 of the *Criminal Code* within the definition of a 'serious offence'. This means that telecommunications warrants may be issued to assist with the investigation of terrorism offences. Warrants may also be issued in relation to non-suspects who are 'likely to communicate' with the person under investigation (known as 'B-Party' communication). Communications may be intercepted through intrusive methods such as optical surveillance and tracking devices.[124]

The *TIA* also provides a statutory basis for warrantless access to telecommunications data. Under Part IV, telecommunications providers are obliged to hand over communications metadata (not the content of the communications) to numerous Commonwealth and state government departments and agencies if the information is 'reasonably necessary' for a law enforcement purpose and the disclosure is approved by an authorised senior officer of the relevant agency. In the year 2012–13, 319 874 authorisations for access to existing information or documents were made in the enforcement of a criminal law alone.[125] As a result of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2010* (Cth) ('*TIISLA*'), the communication and sharing of intelligence between intelligence and law enforcement agencies has been further enhanced.[126] Greg Carne summarises the consequences of *TIISLA* as follows:

> [T]he changes provide security and intelligence agencies with a significantly enhanced influence or contribution, through communication, cooperation and assistance, into Commonwealth and State administration. Largely by a legislative process of ignorance, default, omission and elision, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth) signals a strong move towards a more authoritative state, with the infusion and integration of national security information, cooperation and assistance as increasingly influential in the ordinary business and functions of both Commonwealth and State government.[127]

In a 2012 discussion paper, the Attorney-General's Department acknowledged that the telecommunications interception regime is outdated and in need of 'holistic reform'.[128] The Attorney-General Department's proposals were

---

124 See George Williams, 'A Decade of Australian Anti-terror Laws' (2011) 35 *Melbourne University Law Review* 1136, 1150–1; see also David Hume and George Williams, 'Who's Listening? Intercepting the Telephone Calls, Emails and SMS's of Innocent People' (2006) 31 *Alternative Law Journal* 211; see also *Surveillance Devices Act 2004* (Cth) s 6.

125 Attorney-General's Department, '*Telecommunications (Interception and Access) Act 1979*: Annual Report 2012–13' (Report, 2013) 49.

126 Greg Carne, 'Beyond Terrorism: Enlarging the National Security Footprint through the *Telecommunication Interception and Intelligence Services Legislation Amendment Act 2011* (Cth)' (2011) 13 *Flinders Law Journal* 177.

127 Ibid 239.

128 Attorney-General's Department, 'Equipping Australia against Emerging and Evolving Threats' (Discussion Paper, July 2012) 17.

said to aim at strengthening the safeguards and privacy protections; reforming the lawful access regime for agencies; reducing complexity and modernising the cost-sharing framework.[129] In June 2013, the Parliamentary Joint Committee on Intelligence and Security tabled a report that assessed potential reform options in the context of a wider inquiry into the legislative national security framework, including the *TIA*, the *Telecommunications Act 1997* (Cth), the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth).[130] As far as the *TIA* was concerned, the report recommended the introduction of an objects clause which would express the Act's dual objectives of protecting the privacy of communications and of enabling interception and access to communications in order to investigate serious crime and threats to national security.[131] In addition to mandatory record keeping standards and improved oversight arrangements, the report also recommended that the Attorney-General's Department examine the introduction of a proportionality test into the legislation that would provide a mechanism for balancing the privacy interest affected, the public interest in the investigative activity and the availability of less invasive investigative measures.[132]

In December 2013, the Senate referred an inquiry into a comprehensive revision of the *TIA*, including the recommendations of the 2013 Report of the Parliamentary Joint Committee on Intelligence and Security, to its Legal and Constitutional Affairs References Committee.[133] While this inquiry is still underway,[134] the government has introduced a Bill to implement the (bipartisan) recommendations of the Parliamentary Joint Committee on Intelligence and Security to expand the surveillance capabilities of the Australian spy agencies.[135] Under these proposed amendments, ASIO will be given wide-ranging new powers to use computers of innocent third parties to gain access to a computer used by a suspected terrorist or criminal. Through a redefinition of the term 'computer',[136] ASIO will also be empowered to access multiple computers operating in a network on a single warrant, rather than requiring separate warrants for individual computers as at present – widening its capabilities to target information stored in the cloud or to intercept information flows between computers. In implementing these proposals, the government is heeding the calls

129 Attorney-General's Department, Submission No 218 to Parliamentary Joint Committee on Intelligence and Security*, Inquiry into Potential Reforms of National Security Legislation,* 2–3.

130 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (2013).

131 Ibid recommendation 1.

132 Ibid recommendation 2.

133 Senate Legal and Constitutional Affairs References Committee, Parliament of Australia, *Comprehensive Revision of the Telecommunications (Interception and Access) Act 1979* (2014) <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act>.

134 The Committee is due to report in August 2014.

135 See National Security Legislation Amendment Bill (No 1) 2014 (Cth).

136 National Security Legislation Amendment Bill (No 1) 2014 (Cth) cl 3, sch 2 pt 1 item 4.

of the Australian Intelligence Community[137] that increased powers are needed to effectively combat the threat of terrorism, including from Australians who are suspected of engaging in overseas terrorist activities. In light of the bipartisan support for increasing the powers of the intelligence services, these changes are certain to pass Parliament, and Australians must accept the government's assurances that the exercise of these new powers will be 'subject to appropriate safeguards and accountability mechanisms'.[138] Yet, this further expansion of surveillance powers will add to the sense of public unease about the reach of the Australian intelligence agencies into the lives of ordinary Australian citizens.[139]

2 Privacy and Counter-Terrorism

Australian data protection laws are mainly contained in the *Privacy Act 1988* (Cth) ('*Privacy Act*'), which responds, as stated in its preamble, both to Australia's obligations to protect privacy under the *International Covenant on Civil and Political Rights* as well as to the *OECD Guidelines on Privacy*. The *Privacy Act* applies to federal agencies as well as private sector organisations. In the *Privacy Act*, the term 'agency' includes the 'Australian Federal Police' (section 6(1)) and other Commonwealth bodies. However, section 7(1) provides that an act or practice 'in relation to a record that has originated with, or has been received from … an intelligence agency'[140] is not subject to the *Privacy Act*. Furthermore, section 7(1A) specifies that the disclosure of personal information by another entity to the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service or the Australian Signals Directorate is not an act or practice which falls under the *Privacy Act*. Disclosure and other data processing in the context of national security is therefore intended to be exempt from the general protections of privacy. Counter-terrorism measures are only relevant within the privacy framework if they are part of law enforcement.

---

137 The 'Australian Intelligence Community' is an informal term to describe the six Australian security and intelligence agencies: Inspector General of Intelligence and Security, *The Australian Intelligence Community*, <http://www.igis.gov.au/aic/>.

138 Parliamentary Joint Committee on Intelligence and Security, above n 130, recommendation 22. Many of the safeguards in the current legislation only apply to 'Australian persons', ie Australian citizens and permanent residents, providing more far-ranging powers to act against non-Australians: see, eg, *Intelligence Services Act 2001* (Cth) ss 8, 9, 15.

139 As part of the extensive revelations in 2013 of secret surveillance activities by the US and its close allies, a secret document leaked by Edward Snowden suggested that the Australian Defence Signals Directorate (now the Australian Signals Directorate) offered to share private information on Australian citizens to its four intelligence-sharing partners: Ewen MacAskill, James Ball and Katharine Murphy, 'Revealed: Australian Spy Agency Offered to Share Data about Ordinary Citizens', *The Guardian* (online), 2 December 2013 <http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens>.

140 These are defined in s 6 of the *Privacy Act 1988* (Cth) as '(a) the Australian Security Intelligence Organisation; (b) the Australian Secret Intelligence Service; or (c) the Office of National Assessments.'

The *Privacy Act* has recently been amended to reflect changes in modern information practices.[141] Under the revised Act, 'APP entities', which includes the public sector agencies and private sector organisations to which the *Privacy Act* applies, must handle personal information in conformity with the 'Australian Privacy Principles' ('APPs'). The APPs lay down standards relating to the collection, use, disclosure and storage of personal information. However, 'enforcement related activities' of 'enforcement bodies' are facilitated through a number of exceptions in the principles.[142] This includes that enforcement bodies may collect sensitive information without the consent of the individual concerned (APP 3.4) and that an APP entity may use or disclose personal information for a purpose other than the purpose for which it was collected (secondary purpose) if it reasonably believes this to be necessary for 'enforcement related activities conducted by, or on behalf of, an enforcement body' (APP 6.2(e)). APP 8, which imposes limitations on cross-border disclosure of personal information, also does not apply to an agency if the cross-border disclosure is 'required or authorised by or under an international agreement relating to information sharing to which Australia is a party' (APP 8.2(e)). This would include, for example, the *UKUSA Agreement*. Another exception applies if an agency reasonably believes the disclosure to be necessary for enforcement related activities by an overseas body with similar functions or powers to an Australian enforcement body (APP 8.2(f)). This exception potentially applies to all kinds of information exchanges for the purposes of counter-terrorism between Commonwealth agencies and overseas law enforcement bodies. In these cases, Australian agencies are not bound to respect the APPs.

3 Conclusion

Australians lack a constitutional right to privacy and the data protection provisions of the *Privacy Act 1988* (Cth) contain significant holes. The activities of the intelligence agencies are not subject to the Act and exceptions to the APPs give law enforcement agencies relatively free reign in designing their information handling practices as well as easier access to information held by other agencies.

---

141 For a general overview of the reforms, see Normann Witzleb, 'Halfway or Half-Hearted? An Overview of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth)' (2013) 41 *Australian Business Law Review* 55.

142 'Enforcement related activities' and 'enforcement bodies' are terms defined in s 6 of the *Privacy Act 1988* (Cth). Enforcement related activities include '(a) the prevention, detection, investigation, prosecution or punishment of: (i) criminal offences; or (ii) breaches of a law imposing a penalty or sanction; or (b) the conduct of surveillance activities, intelligence gathering activities or monitoring activities'. Enforcement bodies include the Australian Federal Police, state and territory police forces, CrimTrac (the national police information sharing body). The Australian Secret Intelligence Service are not specifically mentioned under s 6. However, they could be considered to be falling under '(f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law'. This would be on the basis that they 'may co-operate with and [assist law enforcement bodies] in the performance of [their functions]': see, eg, *Australian Security Intelligence Organisation Act 1979* (Cth) s 19(1).

The powers provided under *ASIO Act 1979* (Cth) and the *TIA* have been significantly extended since 2001 and are due for further expansion under legislative proposals recently introduced by the federal Government. Intelligence agencies and police authorities have increased their cooperation,[143] blurring the distinction between intelligence-gathering and law enforcement.[144] The recent reforms of the *Privacy Act*, including the introduction of revised Privacy Principles, have not substantially changed Australia's surveillance situation. There is widespread recognition that the *TIA*, which provides the basis for access to and interception of telecommunications data, is outdated and provides insufficient protection of individual privacy. The proposed reforms will widen the surveillance capabilities of Australia's security agencies and are intended to provide a more coherent set of safeguards and accountability mechanisms.

The Australian public knows little about the extent to which counter-terrorism measures allow surveillance and cross-border information sharing by Australian government agencies. It is therefore unsurprising that there is growing unease about the extent to which Australian intelligence agencies and law enforcement authorities engage in surveillance of ordinary citizens. The recent Snowden revelations about vast secret surveillance programs in the US, and embarrassing revelations of Australia targeting the inner circle of the Indonesian government,[145] suggest that improved technical capabilities need to be matched with more robust protocols on permitted usage. The absence of constitutional protections of the right to privacy and relatively weak data protection laws provide government with much discretion to expand the powers of agencies to encroach on the personal information of Australian citizens.

III INTERNET SURVEILLANCE, PRIVACY AND INTERNATIONAL DATA PROTECTION

A The New Dimension of Intrusion

Surveillance measures for the purposes of counter-terrorism are reaching unprecedented intensity and intrude deeply into the personal sphere of millions of citizens. Because of the globalisation of telecommunications, every person can become a potential target of monitoring and information exchanges by almost any state of the world, often without personal knowledge. While citizens may enjoy some (constitutional) protections of their right to privacy against their own state, non-citizens may often find it impossible to resist these practices.

143 See *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* (Cth).

144 Carne, above n 126, 186–93.

145 Ewen MacAskill and Lenore Taylor, 'Australia's Spy Agencies Targeted Indonesian President's Mobile Phone', *The Guardian* (online), 18 November 2013 <http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone>.

Besides its international dimension, internet surveillance often includes the following characteristics. First of all, surveillance powers are usually not restricted to terrorism. Although terrorist attacks were, and still are, in many cases the primary political reason for introducing new surveillance measures, they have been given a much broader field of application that will, as a minimum, extend to law enforcement against (trans)national serious or organised crime. Data collection is increasingly in bulk and not limited to a strict purpose; and the hurdles in the way of sharing analysed data with other agencies are being whittled away. Thus, law enforcement is increasingly led by intelligence, and intelligence agencies are contributing to law enforcement.

Second, intrusion is also more encompassing because modern technologies allow monitoring of the whole or significant sections of society. Surveillance is no longer dependent on suspicion of criminal (or terrorist) behaviour. Societies under surveillance lose freedom. If surveillance is covert and the use of the data obtained remains unknown, all but the most oblivious will act on the assumption that their behaviour is observed and that, at some point in the future, the results of surveillance may be used against them.[146]

A third dimension of the new intrusion is its permanence. There is no prospect that the current level of surveillance will be scaled back. Counter-terrorism provides the basis for preventive measures without the existence of a concrete danger. As the potential of a terrorist threat always exists and the list of terrorist attacks is getting longer (from 9/11 to Bali, and Madrid to London, from Boston to the next terrorist attack), the move towards surveillance seems irreversible. Technological advances make data storage and data retention ever cheaper, adding a further dimension of permanence. Even where the erasure of data is provided for, there is no reason for confidence that deletion really occurs or that, accidentally and deliberately, data will not be retained and, once it is retained, that it will not be accessed for some future use.[147]

Finally, the spectre of total surveillance no longer appears impossible because technology provides ever-expanding potential for data sharing, data matching and data meshing. Data processors can be public or private, and the state increasingly coopts private business into its surveillance agenda. Anyone with whom we communicate, or whose infrastructure we use, can be turned into a potential contributor to state surveillance. Information resulting from internet surveillance can be combined with personal information held by private enterprises,[148] such as bank accounts, travel itineraries, social networks, or with data held in government repositories of tax, social security and other state-held

146 Cate, above n 10, 477–9.

147 On the need for erasure, see Victor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2011).

148 Pell, above n 92.

information.[149] Personal movements can be tracked through a combination of video surveillance[150] and geolocation data.[151] This increase in surveillance possibilities is further expanded by advances in analysing capabilities of personal information.[152] Big data applications raise the prospect of mining information to predict future behaviour or psychological preferences of which a target person might not even be aware.[153]

The new dimension of international surveillance networks potentially includes everybody and leads to a permanent and dramatically accelerating loss of privacy. These surveillance networks target as many different aspects of human behaviour as possible and seek to use ever-improving tools of analysis. The data collected by these networks is subject to exponential growth, as more information is gained, analytical tools are improving and the storage capacities are expanding. The anti-terrorism narrative, on which these programs are often based, tends to make them politically immune. However, a constitutional response to this form of counter-terrorism measure needs to reassert the value and possibilities of protection of privacy and personal data.

B The International Privacy Challenge

Victor V Ramraj argues that a 'global perspective [of anti-terrorism laws] enriches our understanding of law and is imperative in the formulation of sophisticated and effective policies' yet requires a 'nuanced and sophisticated approach, one that is mindful of local differences and particularities that transform the way legal norms are understood, articulated, implemented and resisted in different parts of the world.'[154] This insight does not only apply to counter-terrorism measures, which reflect the history, politics and (constitutional) law of a society, but equally to an evaluation of the need for privacy.

The difficulty for privacy advocates is that there is no universally shared understanding of privacy. Different legal cultures and jurisdictions have adopted different approaches to privacy and data protection, each

149 Calling for greater sensitivity towards data held by public authorities, see Cecilia Magnusson Sjöberg, 'Administrative Data Protection in Global Networks' in Anna-Sara Lind and Jane Reichel (eds), *Administrative Law beyond the State: Nordic Perspectives* (Martinus Nijhoff Publishers, Liber AB, 2013) 143–61.

150 See Mathias Klang, 'Privacy, Surveillance and Identity' in Mathias Klang and Andrew Murray (eds), *Human Rights in the Digital Age* (Cavendish Publishing, 2005) 175–89.

151 See Fabbrini and Vermeulen, above n 111.

152 See Mayer-Schönberger and Cukier, above n 11.

153 See Omer Tene, 'Privacy: The New Generations' (2011) 1 *International Data Privacy Law* 15, who is arguing for a new generation of governance beyond the private/public and the personal/non-personal data dichotomy.

154 Victor V Ramraj, 'The Impossibility of Global Anti-terrorism Law?' in Victor V Ramraj et al (eds), *Global Anti-terrorism Law and Policy* (Cambridge University Press, 2nd ed, 2012) 66.

reflecting their unique historical, political and legal development.[155] While the EU follows a constitutional and rights-based approach with highly specific legislative requirements,[156] Australia relies solely on statutory protections without constitutional reinforcement or a rights-based framework. The US approach includes elements of the two extreme positions.[157] It relies on a strong constitutional framework which focuses on the protection of privacy against the state and a patchwork of norms to protect privacy in private and business relationships. However, in a globalised world of communication and informational networks that are subject to transnational surveillance measures, it becomes increasingly difficult to rely on purely domestic notions, and national protections, of privacy.[158]

In the wake of 9/11, and following the lead of the US, Western democracies around the globe massively expanded the powers of law enforcement and national security agencies, without creating sufficient oversight to control the use of these powers. If we take a closer look at the conflict between privacy and counter-terrorism, national security and intelligence agencies measures, the EU (for reasons of competences), the US (for reasons of wide executive powers) and Australia (for lacking an effective human rights framework) are essentially not all that different. The data privacy obligations of intelligence agencies are not properly addressed in any of the three legal orders.

The exemptions in general data protections laws are far-reaching and impose few obstacles to privacy-invasive practices. In the EU, each member state retains the power to define the powers of its intelligence agencies and how these agencies are controlled. In many countries, including Germany, Australia and the US, parliamentary control of intelligence agencies plays an important role even though it is, in practice, often lacking in effectiveness. In the US, the Congressional response to the Snowden revelations will be crucial; the extension of Fourth Amendment protections by the courts remains another possibility to foster data privacy. Only jurisdictions with privacy clauses, be they express or implied, in their constitutions or bills of rights subscribe to the idea that there are absolute limits beyond which state intrusion into personal privacy is prohibited. The CJEU judgment on the *Data Retention Directive* provides EU lawmakers with guidance on these limits. In the US, Congress will determine the future legislative framework for national intelligence services, while the US Supreme Court will have the responsibility to provide judicial protection against undue

155 See, eg, regarding US, Germany, France, Australia, South Korea, Hong Kong and Hungary: James B Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation* (Edward Elgar Publishing, 2008).

156 Despite this European overlay, there remain significant constitutional and cultural differences between the various European countries.

157 For a very illuminating discussion on the differences between the continental European and the US approach: James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 *Yale Law Journal* 1151.

158 See Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 *International Journal of Law and Information Technology* 142, 156–63, 174–5.

interferences. In Australia, the courts only have very limited powers to invalidate certain forms of surveillance if they are in compliance with enacted legislation.

The cooperation of law enforcement and national security agencies with regard to counter-terrorism deserves particular attention. The EU developed certain privacy standards regarding police cooperation and Europol but retained many exemptions in the current *Draft Directive*. The Australian *TIA*, as well as planned reforms to this statute, opened up the possibilities for further and cooperative surveillance measures between law enforcement authorities and intelligence agencies. The US has traditionally limited the possibilities of law enforcement authorities regarding the intrusion in the private sphere and there are some signs that the surveillance program affecting US citizens will be reviewed, but surveillance of non-US persons continues virtually unabated.

This short comparative overview provided some insight into the diverse understandings of privacy and data protection in different constitutional systems.[159] It demonstrated that constitutional systems face significant challenges in establishing a framework that appropriately balances the interest in public safety and freedom from terrorism with the legitimate expectations of ordinary citizens that their privacy will be respected.

C A Charter for Data Protection Rights: Approaches toward International Data Protection

Simon Chesterman proposes in his book 'One Nation under Surveillance' that the establishment of a new social contract has become necessary in surveillance societies.[160] It is certainly true that the relations between state, society and the individual have to be renegotiated in this new era of almost limitless gathering of private information. However, to be effective, such a compact needs to take account of the international dimension of surveillance and societies. Societies are no longer built within one nation, one state, one constitution. Globalisation, and especially the internet,[161] has created global communities and the need to consider regulation in transnational, even virtual dimensions.[162] The proper balancing of counter-terrorism, including state surveillance, with privacy can benefit from comparative constitutionalism but

159 Stephanie Schiedermair, 'Data Protection – Is There a Bridge across the Atlantic?' in Dieter Dörr and Russell L Weaver (eds), *The Right to Privacy in the Light of Media Convergence: Perspectives from Three Continents* (De Gruyter, 2012) 357; see also Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014); David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131, 169.

160 Simon Chesterman, *One Nation under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford University Press, 2011).

161 On the forms of state regulation of the internet, see Maier, above n 158, 170–3.

162 Konrad Lachmayer, 'Constitutional Reasoning as Legitimacy of Constitutional Comparison' (2013) 14 *German Law Journal* 1463, 1471, 1479–80, 1487.

needs to bear in mind the fragmented structure of international (constitutional) law.[163]

The new global challenges to privacy, which have far-reaching consequences for communities as well as individuals, can no longer solely be solved at a national level. Despite recent efforts of regulators to enhance the coordination of their enforcement activities,[164] domestic data protections laws and national regulators appear increasingly ill-equipped to deal with the international dimension of state surveillance and massive cross-border sharing of personal data. The cross-border dimension of modern surveillance, and its justification with national security imperatives, also make it virtually impossible for individuals to challenge covert and firmly entrenched programs of state surveillance.[165] It is likely that real change can only be affected at an international level through negotiation between states who act to defend their citizens' privacy as a matter of national sovereignty.

There are already some examples of international cooperation and agreements relating to the exchange of personal data. The US and Europe have entered into the *TFTP Agreement*[166] and the *PNR Agreement*;[167] the EU and Australia also have a *PNR Agreement*;[168] and Australia, Canada, New Zealand, the UK and the US are parties to the *UKUSA Agreement*.[169] These agreements illustrate that countries or regions can reach agreements on information sharing arrangements in specific contexts, without the need to surrender their own understanding of privacy and data protection to the interests of another. These measures coincide with a rise in the number of other international initiatives with regard to privacy and data protection.[170]

It is, however, a much more challenging undertaking to find common ground on general standards of privacy protection, rather than on specific issues, and to

---

163 Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press, 2012).

164 'Resolution on International Enforcement Coordination' (Resolution adopted at 35th International Conference of Data Protection and Privacy Commissioners, Warsaw, 23–26 September 2013).

165 Global civil society plays an important role in addressing security issues, see Ian Loader and Neil Walker, *Civilizing Security* (Cambridge University Press, 2007) 254–6. For a domestic (Canadian) example of social response, see Vanessa MacDonnell, 'Internet Surveillance and Popular Constitutionalism' in Fergal Davis, Nicola McGarrity and George Williams (eds), *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, 2014) 313.

166 *Terrorist Finance Tracking Program Agreement* [2010] OJ L 195/5. The US and the EU are also currently engaged in negotiations towards an umbrella agreement to govern data exchange for law enforcement purposes: see Viviane Reding, *EU-US Justice Ministerial in Athens: Vice-President Reding Welcomes US Announcement on Data Protection Umbrella Agreement* (25 June 2014) European Commission <http://ec.europa.eu/commission_2010-2014/reding/multimedia/news/2014/06/20140625_en.htm>.

167 *TFTP Agreement* [2012] OJ L 215/5.

168 *PNR Agreement* [2012] OJ L 186/4.

169 UK Government, *Newly Released GCHQ Files: UKUSA Agreement* (June 2010) The National Archives <http://www.nationalarchives.gov.uk/ukusa/>.

170 See Kuner, above n 12.

do so not in bi- or multilateral agreements but on a truly global scale.[171] Considering the widely diverging approaches to privacy rights among liberal Western democracies, as demonstrated by the EU, Australia and the US, the chances of finding a global consensus on privacy seem remote.[172] There is, however, scope for privacy issues to be considered in the context of international agreements on online security or internet governance, which usually rank more highly in the policy agendas of governments.[173]

It is unlikely that the EU initiatives to establish a new data protection framework could serve as a global blueprint. While the Union aims to export its ideas and concept of data protection, the new *Draft Framework* is perceived internationally as complex and burdensome. The demand for an adequate level of protection in countries to which data should be exported can operate as a lever to raise the levels of domestic data protection in other countries. However, if the limited success of the current adequacy framework in article 29 of the EU *Data Protection Directive* is a guide to the future, it must be doubted that the EU will successfully export its high standards of data protection to other countries around the world.[174]

A more likely candidate for global privacy standards is the Council of Europe (COE)'s *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* ('*Convention 108*'). Dating from 1981, *Convention 108* is ratified by nearly all of the member states of the Council of Europe (with the significant exception of Turkey) but non-European countries are also able to accede. As the first non-European country, Uruguay recently ratified *Convention 108*.[175] A process of modernisation currently underway is likely to make *Convention 108* more attractive to countries seeking to demonstrate their commitment to meeting global privacy standards.[176] *Convention 108*, however, offers two important exceptions. First, article 3 paragraph 2 of *Convention 108* gives a member state the possibility to declare 'that it will not apply this convention to certain categories of automated personal data files'. Such declarations with regard to national or state security were made by a number of countries, including Ireland, Latvia, Serbia, Montenegro, Macedonia, Malta and

171 See Bygrave, above n 159; Gunasekara, above n 96, 176–8.

172 See, eg, with regard to other countries, Graham Greenleaf, 'Promises and Illusions of Data Protection in Indian Law' (2011) 1 *International Data Privacy Law* 47; Mario Viola de Azevedo Cunha and Danilo Doneda, 'Privacy, Security and New Technologies: A Brazilian Approach to Privacy Issues in the Public Security Field' in Mario Viola de Azevedo Cunha et al (eds), *New Technologies and Human Rights: Challenges to Regulation* (Ashgate Publishing, 2013) 217–28.

173 See Clarke et al, above n 113, in particular recommendations 31 and 33.

174 For a critical analysis of the EU's approaches, see Lingjie Kong, 'Data Protection and Transborder Data Flow in the European and Global Context' (2010) 21 *European Journal of International Law* 441, 444–6.

175 See Graham Greenleaf, 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of *Convention 108*?' (2012) 2 *International Data Privacy Law* 68, 81–91.

176 For further discussion, see Graham Greenleaf, 'A World Data Privacy Treaty? "Globalisation" and "Modernisation" of Council of Europe *Convention 108*' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 92.

Romania. Furthermore, article 9 of *Convention 108* allows derogation from the core provisions of *Convention 108* 'when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of […] protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences'.[177] This exemption of article 9, however, requires proportionality. Although the existing *Convention 108* thus provides significant scope for exempting state surveillance for counter-terrorism, it has established itself as an important repository of general international data protection standards. The current process of modernisation and review of *Convention 108* is likely to enhance these standards and broaden their application.[178] This makes it likely that *Convention 108* will remain a more likely model for non-COE members to follow than the highly technical and more demanding provisions of the proposed new EU *Data Protection Framework*.

Another important international treaty arising from the Council of Europe in the field of counter-terrorism is the *Convention on Cybercrime* ('*Convention 185*'). *Convention 185* has been ratified by most European countries,[179] but also by a number of non-COE countries including Australia, Japan, Panama and the US. Apart from providing for the penalisation of computer-related offences, which become increasingly relevant in the context of counter-terrorism, *Convention 185* seeks to establish common procedural standards to fight cybercrime, including for example, in relation to 'Search and Seizure of Stored Computer Data' (article 19), 'Real-Time Collection of Traffic Data' (article 20) or the 'Interception of Content Data' (article 21). Lastly *Convention 185* creates a legal framework for international cooperation and mutual assistance for the purposes of the investigation and prosecution of cybercrime. Such measures will often involve the sharing of personal information, yet *Convention 185* does not provide any specific data protection standards that need to be observed in cooperation and mutual assistance matters.[180] It is therefore of limited use with regards to establishing the appropriate balance between law enforcement and data protection.[181]

---

177 Russia explicitly makes use of the derogation possibility of article 9 of *Convention 108* (Russian Declaration contained in the instrument of ratification deposited on 15 May 2013: 'The Russian Federation declares that in accordance with subparagraph 'a' of paragraph 2 of Article 9 of the Convention, it retains the right to limit the right of the data subject to access personal data on himself for the purposes of protecting State security and public order.').

178 The draft of the modernisation of *Convention 108* includes the proposal to delete the possibility of declaration regarding article 3.

179 Significant exceptions include Greece, Ireland, Poland, Russia, Sweden and Turkey.

180 Instead, article 15 of *Convention 185* provides in general terms that, in procedural matters, the applicable conditions and safeguards to protect human rights must be observed. Similarly, but with express reference to privacy, see African Union Commission, Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, Draft Convention No 01/09/2012 (1 September 2012).

181 See the already critical opinion of the EU's Article 29 Data Protection Working Party: Stefano Rodota, 'Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-Crime' (Opinion No 4/2001, Article 29 Working Party, 22 March 2001).

Further international data privacy instruments or declarations like the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[182] the *APEC Privacy Framework*,[183] the *Madrid Privacy Declaration*[184] or the UN General Assembly Resolution on *The Right to Privacy in the Digital Age* also need to be mentioned.[185] The protection of respect for privacy in article 17 of the *ICCPR* could also serve as a starting point for work on an international data privacy framework.[186] A resolution of the 35th International Conference of Data Protection and Privacy Commissioners recognised the 'pressing need for a binding international agreement on data protection' and urged national governments to advocate the adoption of an additional protocol to article 17 of the *ICCPR* to create globally applicable data protection standards.[187] Expressing its deep concern about mass scale surveillance, interception and collection of personal information, the UN General Assembly Resolution on the *Right to Privacy in the Digital Age* of 2013 put the issue on the agenda of the Human Rights Council and called upon states to review their surveillance practices and oversight mechanisms.[188] It is an encouraging sign that unbridled state surveillance is increasingly acknowledged as an international human rights issue.

IV CONCLUSION

There is growing recognition that data privacy can no longer be effectively guaranteed in the absence of internationally agreed standards and procedures. However, the international regulation of transborder data flows faces significant hurdles because the cultural and constitutional approaches towards (data) privacy differ dramatically between jurisdictions. While some regions, such as the EU,

182 See further Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2011) 1 *International Data Privacy Law* 6.

183 See also Graham Greenleaf, 'Five Years of the APEC Privacy Framework: Failure or Promise?' (2009) 25 *Computer Law and Security Review* 28.

184 *The Madrid Privacy Declaration* arose from the 31st International Conference of Privacy and Data Protection Commissioners in Madrid and has been signed by more than 100 civil society organisations and privacy experts. More information about the Declaration, including translations, is available at: The Public Voice, *Madrid Privacy Declaration* (3 November 2009) <http://thepublicvoice.org/madrid-declaration/>.

185 GA Res 167, UN GAOR, 3rd Comm, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013).

186 For a comparison with *ECHR* art 8, see Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *International Journal of Law and Information Technology* 247, 252–4.

187 'Resolution on Anchoring Data Protection and the Protection of Privacy in International Law' (Resolution adopted at the 35th International Conference of Data Protection and Privacy Commissioners, Warsaw, 23–26 September 2013).

188 GA Res 167, UN GAOR, 3rd Comm, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014, adopted 18 December 2013).

regard privacy protection as a question of human rights and are currently in the process of enhancing their privacy standards even further, other countries have barely begun to acknowledge the importance of personal privacy protection. Australia and the US adopt positions in the middle ground. Their regulation is relatively 'light touch' because of a concern that excessive privacy protection has the potential to impose a significant regulatory burden on their businesses.

Agreement on global privacy standards currently appears to be a distant vision. However, the increasing globalisation of data flows makes such an agreement ever more urgent and may prompt further efforts by governments. The most likely candidate for a world data privacy treaty is currently *Convention 108* of the Council of Europe, as it already has a significant number of European members and strikes a compromise between the high standards of data privacy within the EU and the less stringent standards in many other parts of the world. An unresolved question is whether such an international instrument would provide individuals with rights that could also be enforced internationally.

Since 2001, government surveillance has emerged as one of the most significant threats to personal privacy. In the ongoing debate on surveillance, it has become increasingly apparent that intelligence agencies and law enforcement bodies are using the concern for national security to develop systems of mass surveillance that deeply affect the lives and freedoms of ordinary citizens. While the EU, the US and Australia adopt very different approaches to data privacy, they coincide in largely exempting national security agencies from compliance with general data protection laws. The conferral of new powers on national intelligence agencies for the purposes of counter-terrorism has further exposed the flaws of regulatory systems that provide insufficient protection of privacy in the context of state surveillance. In Australia, the US and some member states of the EU, legislators have begun the difficult task of assessing how oversight of surveillance activities can be improved without sacrificing counter-terrrorism capabilities.

Surveillance as a counter-terrorism measure does not stop at national borders. The international phenomenon of terrorism requires international responses. Countries acquire increasingly sophisticated technology that can reach deeply into foreign communications and monitor data traffic without the knowledge or consent of governments or citizens affected by such measures. In other cases, governments enter into bilateral or multilateral cooperation arrangements. While agreements on information sharing require the parties to find a compromise on the appropriate level of data privacy in cross-border data flows, there is some, albeit limited, scope for national parliaments and popular constitutionalism to influence the extent and content of such international counter-terrorism cooperation.

The international regulation of surveillance activities by counter-terrorism and intelligence agencies thus faces complex hurdles. It must contend with firmly entrenched differences in relation to the relative value and significance of privacy in various world regions and legal cultures. These differences are accentuated in the conflict between privacy and protection from the threat of international terrorism. Even if global agreement on general privacy standards could be

achieved, it is not likely that surveillance for the purposes of national security would be covered in an international treaty. Such activities are usually exempt from general privacy regulation in domestic law, and there is no indication that governments would agree to give up any of their policy discretion in such a core area of national sovereignty. The prospects for enhanced protection of individual privacy against further encroachment by national security agencies are therefore dim. However, the significance of privacy for personal freedom requires the sustained efforts of civil society and privacy advocates to take on this difficult mission.