BRILL
NIJHOFF

TILBURG LAW REVIEW 20 (2015) 78-102

Tilburg Law Review
brill.com/tilr

Rethinking Privacy Beyond Borders

Developing Transnational Rights on Data Privacy

Konrad Lachmayer
Research chair holder, Institute of Legal Studies, Centre for Social Sciences, Hungarian Academy of Sciences
Senior lecturer (Privatdozent), Department of Constitutional and Administrative Law, Faculty of Law, University of Vienna Independent researcher in Vienna
konrad@lachmayer.eu

Abstract

The tensions between transnational data exchange by police authorities as well as intelligence agencies on the one hand and the need for data privacy on the other hand are increasing. The European Union follows an ambivalent approach intensifying data exchange as well as reforming data protection in the context of police and judicial cooperation in criminal matters. Based on EU constitutional law, the CJEU defends privacy rights in the EU. Beyond the European perspective, the paper argues based on a comparison of data privacy in the EU, US and Australia in favour of the establishment and strengthening of international data privacy rights. A more detailed concept of international digital rights would be necessary to address all different issues of data privacy in the context of trans-border surveillance. While intelligence agencies and police cooperation are already linked on a global level, the protection of data privacy is not organized on an international level in an equivalent way.

Keywords

state surveillance – data privacy rights – European Union – United States – Australia – police – judicial cooperation in criminal matters – data protection

* The author would like to thank Federico Fabbrini for all his support to finalise this paper; moreover, he would like to thank an anonymous reviewer for his/her remarks.

 | DOI 10.1163/22112596-02001008

1 Introduction

In 2011, a politically active Austrian student asked the Austrian Ministry of Interior if it gathered personal information about him. In accordance with Section 26 of the Austrian Data Protection Act[1] (ADPA), the student had the right to know what type of personal data was being collected. Although the ministry had different legal bases on which it could have rejected such a request[2] (e.g. for reasons of national security, police investigation etc.), it informed him that his name and further personal data were stored by the Federal Agency for Protection of the Constitution and Counter-Terrorism, which forms part of the Federal Ministry of the Interior. The storage of this personal data, however, was not linked to the political activities of the student. The reason for it dated back to a completely different story.

Some years earlier, this student had travelled from Austria to the United Kingdom, arriving at London's Stansted Airport. He was impressed by the architecture of the airport and took some photos. A police officer at the airport observed the student and stopped him. The officer informed the student that the law forbade the taking of photos at the airport. The student was obliged to delete the photos and was requested to give his name and other details to the police officer. The student subsequently forgot about the incident, which had no further effect. The UK police administration, however, entered the student's personal data into police databases. Finally, the UK police informed the Austrian Ministry of the Interior by sending a form containing the recorded data of the student. The Austrian Ministry of the Interior did not investigate the relevance of the information but stored the student's data under the category of terrorism.[3]

1 Austrian Data Protection Act, Section 26, para 1: '§ 26. (1) A controller shall provide any person or group of persons with information about the data being processed about the person or the group of persons who so request in writing and prove his/her identity in an appropriate manner. … The information shall contain the processed data, the information about their origin, the recipients or categories of recipients of transmissions, the purpose of the use of data as well as its legal basis in intelligible form. Upon request of a data subject, the names and addresses of further processors shall be disclosed in case they are charged with processing data relating to him. If no data of the person requesting information exist it is sufficient to disclose this fact (negative information)' For the entire act in English, see: <http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html> accessed 22 August 2014.

2 Ibid, s 26, para 5.

3 The case was presented on Austrian television on 15/11/2011 in ORF Report (weekly TV programme on current developments in Austria). Only one reference (in German) can be found on the internet <http://at.rechtsinfokollektiv.org/orf-report-und-interview-mit-mikl-leitner/> accessed 22 August 2014.

Obviously, the student was surprised to get this information and a debate on the legality of the processed data was begun. At exactly the same time, the Austrian parliament introduced – based on a draft from the Ministry of the Interior – further powers for police and intelligence agencies to observe suspicious individuals regarding terrorism activities.[4]

The example gives us several important insights. First, the violation of the data privacy of innocent individuals in national security is quite significant. There are various reasons why national security agencies are made aware of individuals. The reasons can be more or less valid; the threat posed by a person can be real or fictitious. However, the persons concerned are usually not informed and often have no possibility to get access to the personal data being held. Second, this case illustrates the importance of the right to access. If such a right exists and the authority does not reject relevant information, a proportionate protection of the individuals is possible. Effective legal protection for individuals is based on rights and access to courts.[5] Third, transnational data exchange is increasing in counter-terrorism activities carried out by the nation states. It is easy to imagine how much more difficult it would have been for the student to gain access to his information in another country. Language problems and the knowledge about the legal system are just two examples for problems, which can occur. Thus, it is necessary to develop adequate strategies to enable data protection rights beyond borders.

The case of the Austrian student also exemplifies the problem of international data flows in the context of national security, counter-terrorism and state surveillance. The exchange of personal data between agencies of different states typically only depends on the different agencies granting approval to exchange information. However, the person concerned will never be informed.

4 Austrian Security Police Act, s 21, para 3 and the relevant amendment by Parliament, available in German at <http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01520/fname_235567.pdf> accessed 22 August 2014. Before the relevant amendment the Austrian police and intelligence agencies were only allowed to observe certain groups without any urgent suspicion. The new amendment allowed police and intelligence agencies to observe not only certain radical groups but also individual extremists within the full range of police powers. The official argumentation referred to the Norway attacks by Anders Breivik in 2011. The problem with the Austrian provision, however, is its very vague wording, which enables the police to observe on a very low level of evidence.

5 It is especially important that the person concerned knows if any information at all is stored. The problem is that the stored information is often considered secret and thus the right to access is rejected. See Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60, Art. 17.

In the case of the Austrian student, he only filed a request with the Ministry of the Interior because of his political activities as a student representative. Because of a heated debate on the data gathering of the police in the context of student organisations, a greater number of students started to file requests to see if the police had processed their data. The interesting result in the concrete case was that no data was stored with regard to the student's political activities but solely in connection with the incident at Stansted Airport.

Although there is a lot of exchange of counter-terrorism information going on between different countries,[6] the mechanisms to protect data often depend on the national legislation of the relevant countries especially beyond Europe. In any case, the persons concerned do not know that their personal data is already spread around the world. In the context of counter-terrorism, the exchange of data can lead to various scenarios, which can have significant effects on innocent individuals, e.g. that these persons will be observed by domestic police or foreign security agencies, that immigration is denied at the airport or, in the worst case, that they are brought to a secret detention camp.[7] However, even if none of these scenarios occurs, the storage of the personal data in the wrong context can still be understood as a permanent threat to the person concerned that at some point police authority will abuse their information for illegitimate reasons.[8]

This article proposes that we have to rethink privacy beyond borders from a rights-based perspective. The introductory example showed that effective legal control of data exchange in the context of terrorism requires rights for individuals, for them both to be made aware that data has been processed and to gain legal review by an independent authority or court. The example not only illustrates how easily innocent people can be involved in police investigations, but also shows how important it is for individuals to have the right to legally challenge the activities of intelligence agencies.

In this paper, the author will analyse the tension between transnational data exchange by police authorities as well as intelligence agencies on the one hand and the need for data privacy on the other. Section 2 starts with an analysis of the current developments in the European Union and illustrates that a

6 See the contribution of C Cocq, 'Developments of Regional Legal Framework for Intelligence and Information Sharing in the EU and ASEAN' in this Special Issue (focusing specifically on the exchange of information and intelligence).

7 D Cole, 'How We Made Killing Easy' (*The New York Review of Books*, 6 February 2013) <http://www.nybooks.com/blogs/nyrblog/2013/feb/06/drones-killing-made-easy/> accessed 22 August 2014.

8 One might think of all the historical examples of authoritarian regimes.

rights-based approach can overcome the ambivalent dynamics of counter-terrorism and police cooperation regarding data privacy. Section 3 opens up the European perspective towards a broader comparative overview of data protection in the United States (US) and Australia. Section 4 finally suggests an international rights-based approach to tackle the problem of data privacy in transnational counter-terrorism activities and concludes that more distinct rights of individuals have to be developed with regard to data privacy on a national and international level.

2 European Data Privacy at a Crossroads

2.1 *Introduction*

Recent European developments on data privacy reflect, on the one hand, the ambivalence of the last 20 years of legal evolution in counter-terrorism and, on the other hand, the increasing emphasis on surveillance.[9]

The starting point for understanding the challenges for data protection with regard to surveillance of public authorities is the constitutional framework. From a rights-based perspective, the EU offers strong protection. Article 7 of the EU Charter of Fundamental Rights (CFR) provides for the right to respect for private and family life, home and communications. This echoes the protection of the right to privacy, which is guaranteed by Article 8 of the European Convention on Human Rights (ECHR). Moreover, Article 7 CFR grants a particular right to the protection of personal data.[10] In the case law of the Court of Justice of the European Union (CJEU) the right to data protection was already secured before the Lisbon Treaty, which declared the Charter as binding norm of EU constitutional law.[11]

The strong human rights approach towards data protection is limited by the competences of the EU regarding intelligence agencies. Article 4.2 of the Treaty on the European Union (TEU) states that the Union shall respect the essential State functions (of the Member States), 'including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security'.

9 See the contribution of V Mitsilegas, 'The Transformation of Privacy in an Era of Pre-Emptive Surveillance' in this special issue, focusing on 'surveillance emphasis'.

10 Consolidated Version of the Treaty on the Functioning of the European Union (Lisbon Treaty) [2008] OJ C 115/47, Art. 16.1: 'Everyone has the right to the protection of personal data concerning them'.

11 See G González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

The EU's competence in the policy field of Freedom, Security and Justice, which includes police and judicial cooperation in criminal matters, reiterates that the creation of the area of Freedom, Security and Justice 'shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security'.[12] The EU has adopted legislation to foster 'police and judicial cooperation in criminal matters'[13] regarding counter-terrorism. A grey zone is gaping between the competences of the Union and the Member States, which includes intelligence agencies and questions of national security.

Based on the above-discussed constitutional framework of the Union, this section examines the latest case law of the CJEU and the on-going policy-making discussion on the reform of the EU data protection legislation to emphasize the ambivalence of the state of data protection in the EU.

In recent cases regarding the Data Retention Directive[14] and the rights to 'erasure' of results in search engines, the CJEU proved that the court is able to further develop data protection on the foundation of a rights-based approach. Grounding its reasoning in the rule of law and a strong understanding of data privacy, the Court strengthened privacy rights.

While the Court fosters data privacy in the EU legal system, the Council of Ministers of the Interior of the Union is currently discussing the next five years of police and judicial cooperation in criminal matters (the so-called 'post Stockholm process'[15]). Although the consideration of data protection is regularly mentioned, the debate mainly focuses on the development of new tools of cooperation, which typically includes further use of personal data. Most recent developments in Police and Judicial Cooperation in Criminal matters (PJCC) include the introduction of a European Investigation Order, the establishment of the Schengen Information System II and a revised version of the legal basis for the European Police Office: the Europol Regulation. All this new legislation will be introduced more closely in the next chapters.

In order to understand European data privacy in the context of counter-terrorism it is necessary to consider both developments: the case law of the

12 Lisbon Treaty, Art. 72.

13 Council Decision 2008/615/JHA of 23 June 2008 on the stepping-up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1.

14 Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2006] OJ L105/54.

15 See <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/future-of-home-affairs/index_en.htm> accessed 2 September 2014; Commission, 'An open and secure Europe: making it happen' (Communication) COM (2014) 154 final.

Court regarding privacy rights and the EU's counter-terrorism legislation. The compromise between data protection on the one hand and the needs to boost data flow for security purposes is epitomized by the Framework Decision on Data Protection in the area of PJCC.[16] This instrument shall be revised and substituted by a new PJCC Data Protection Directive. The analysis of the draft Directive again shows significant loopholes and challenges remaining if an effective data protection system regarding state surveillance and transborder data flows on security matters is to be established.

As argued, European data protection will develop between these different elements of European integration. The increasing importance of CJEU creates a possibility for a stronger rights-based approach. The exclusion of national security questions from the competences of the European Union still has the potential to undermine the extension of data protection in the field of intelligence agencies.

2.2 *The Case Law of the European Court of Justice*

Recently, the European Court of Justice stepped into the surveillance debate with regard to state and private actors in a significant way. In particular, in the recent decision in *Digital Rights Ireland*, the CJEU invalidated the Data Retention Directive.[17] As Arianna Vedaschi and Valerio Lubello explain in another contribution to this special issue,[18] the Directive set up the most intrusive surveillance system of the EU, and epitomized the EU approach to counter-terrorism significantly by limiting data protection rights.[19]

The CJEU showed that it is possible to address questions of surveillance when a piece of legislation exists and it is brought to the courts. The court argued explicitly with the rights to private life and data protection and made use of the principle of proportionality to limit the possibility of broad

16 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.

17 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland* v *Ireland* [2014] not yet reported.

18 See the contribution of A Vedaschi and V Lubello, 'Data Retention and its Implications for the Fundamental Right to Privacy' in this Special Issue (focusing specifically on data protection).

19 See M 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; F Bignami, 'Privacy and Law Enforcement in the European Union: the Data Retention Directive' [2007–2008] 8 Chicago Journal of International Law 233.

surveillance techniques. The reaction of the European and national legislators will show if a limited approach to data retention will be re-introduced.[20]

Another important decision recently published by the CJEU refers to the right to be forgotten. Although the case – *Google Spain vs. AEPD* – dealt with the private actor Google and is related to search engines,[21] it shows the willingness of the CJEU to engage with crucial questions of data protection and to develop European standards even further. The Court opened up the terminological and territorial scope of the Data Protection Directive 95/46. Moreover, the judiciary changed the interpretation of the rights to erasure or blocking of data.[22] The Court stated that:

[T]he operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.[23]

The Court followed a rights-based approach and interpreted the rights of the Data Protection Directive 95/46 in light of Articles 7 and 8 CFR. The CJEU argued that:

[P]rocessing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet.[24]

---

20 See the contrasting developments in the UK and in Austria. The UK Parliament introduced a new statute to re-establish data retention. The Austrian government also wanted to uphold the existing data retention provisions in the Austrian Telecommunication Act; the Austrian Constitutional Court, however, declared the provision as void. See with regard to the UK the Data Retention and Investigatory Powers Act 2014; regarding Austria see: <http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/press_releasedataretention.pdf> accessed 22 August 2014.

21 Case C-131/12 *Google Spain* v. *AEPD* [2014] not yet reported.

22 See Council Directive (EC) 95/46/EC 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 [1995] OJ L 281/31 (Data Protection Directive) Art. 12 (b).

23 *Google Spain* (n 21) para 88.

24 *Google Spain* (n 21), para 80.

In conclusion, the recent case law of the CJEU can be understood as a major step towards a rights-based approach regarding surveillance and counter-terrorism. The court is about to develop certain limits to data-related counter-terrorism measures and is at the same time strengthening the rights to privacy of the individuals in the digital world. Moreover, the CJEU proved that the Court is able to tackle the constitutional questions of counter-terrorism and surveillance.

2.3 *Post-Stockholm Process*

Besides the privacy-oriented case law of the CJEU, it is also necessary to take into account EU legislative developments, which follow an ambivalent approach towards privacy rights. Although certain rights are mentioned, the increase of data exchange decreases data privacy of the individual. The EU is steadily strengthening police and judicial cooperation in criminal matters, including counter-terrorism measures. The Union's approach in this field is based on five-year policy programmes, which were started at the end of the 1990s with the Tampere Programme and were followed up by the Hague Programme.[25] The current programme in the area of Freedom, Security and Justice - the so-called Stockholm Programme[26] - is about to end and a new programme for the next five years is under discussion. European institutions will develop in the so-called post-Stockholm process[27] a new framework for the Europeans' Area of Freedom, Security and Justice by the end of the year 2014.

The recent achievements in PJCC include the following four measures, which all have significant implications for the gathering of personal data: the new Schengen Information System II (SIS II); the European Investigation Order, the Europol Regulation and the establishment of the EU Intelligence Analysis Centre (EU INTCEN).

The Convention implementing the Schengen Agreement[28] created back in the year 1993 a legal basis for an information system to give police 'access to alerts on persons and property for the purposes of border checks and other

25 The Hague Programme: Strengthening Freedom, Security and Justice in the European Union [2005] OJ C53/1.

26 The Stockholm Programme 'An open and secure Europe serving and protecting citizens' [2010] OJ C115/1.

27 Communication (n 16).

28 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L239/19.

police and customs checks'.[29] The improvement of the old system led to the legal enactment of the new Schengen Information System II (SIS II) in 2006/2007;[30] however, it took until the year 2013 for the system to operate properly.[31] Based on the Schengen Information System of the 1990s the second generation provides 'enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system'.[32] The establishment costs of the new system are more than € 165m and the system includes about 45m alerts.[33] This powerful data processing tool serves a purpose not only in the context of migration but also regarding police and judicial cooperation in criminal matters.[34]

The European Arrest Warrant (EAW) is already more than 10 years old and is a well-established instrument of police and judicial cooperation in Europe.[35] With regard to criminal procedure, the EAW is a very limited tool, as it only allows judicial cooperation to arrest persons. Although the EAW is a very intrusive measure with regard to the right to liberty, the intrusion regarding the right to privacy is very low. However, the EAW serves as a legislative model to foster cooperation regarding criminal investigations. The European Investigation Order (EIO) fills this gap and opens up police cooperation in criminal investigations. On 1 May 2014, the EU enacted the Directive regarding the EIO in criminal matters.[36] The EIO functions in a similar way to the

29 Ibid, Art. 92.

30 See more details on SIS II at: <http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14544_en.htm> accessed 22 August 2014.

31 <http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130409_01_en.htm> accessed 2 September 2014.

32 <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm> accessed 22 August 2014.

33 <http://europa.eu/rapid/press-release_MEMO-13-309_en.htm> accessed 22 August 2014.

34 See Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) [2007] OJ L205/63; Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) [2006] OJ L381/4.

35 See Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision [2002] OJ L190/1.

36 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1.

European Arrest Warrant,[37] but refers to all kinds of investigation, including information on bank and other financial accounts,[38] covert investigation[39] or interception of telecommunications.[40] The EIO becomes a very powerful tool for gathering personal data in the EU.

Since the establishment of the European Police Office[41] (Europol) in the year 1995, the legislative foundation[42] of Europol has been amended several times[43] and changed towards a Council Decision in 2009.[44] These developments did not come to an end and the European Commission proposed a Europol Regulation in 2013[45] (Proposal for Regulation), which is still under discussion in the European Parliament.[46] Europol's access to personal data is increased,[47] and the cooperation between Europol and third countries as well as private parties will be intensified.[48] Further constraints relating to certain

37 Any competent investigative authority is able to issue an EIO (ibid, Art. 1). The EIO has to contain the object and reasons for the EOI (ibid, Art. 5). Further requirements are that the EIO is necessary and proportionate and that the investigative measure could have been ordered under the same conditions in a similar domestic case (ibid, Art. 6). Most importantly, the executive authority shall recognise the EIO without any further formality (ibid, Art. 9). According to Art. 10 Directive 2014/41/EU, the executing authority "shall have, wherever possible, recourse to an investigative measure other than that provided for in the EIO where: (a) the investigative measure indicated in the EIO does not exist under the law of the executing State; or (b) the investigative measure indicated in the EIO would not be available in a similar domestic case." Moreover, Art. 11 provides grounds for non-recognition, e.g. related to the freedom of press or essential harm to national security interests.

38 Ibid, Art. 26.

39 Ibid, Art. 29.

40 Ibid, Art. 30.

41 <https://www.europol.europa.eu/content/page/about-us> accessed 22 august 2014.

42 See Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office (Europol Convention) [1995] OJ C316/01.

43 Regarding joint investigation teams, see the Europol Convention and the Protocol on the privileges and immunities of Europol, the members of its organs, the deputy directors and the employees of Europol [2002] OJ C312/1.

44 See Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL) [2009] OJ L 121/37.

45 Proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA COM (2013) 173 final. (Proposal for Regulation).

46 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-20140096+0+DOC+XML+V0//EN> accessed 22 August 2014.

47 Proposal for Regulation (n 45) Art. 23.

48 Ibid, Arts. 29–33.

databases of Europol (like the Europol Information System[49] or analysis work files[50]), which previously existed, can no longer be found in the European Regulation. The Europol Regulation leads to an intensified use of personal data and an easier access to personal data by Europol. A new complaint procedure at the European Data Protection Supervisor might help to improve data protection with regard to Europol.[51]

Finally, the EU Intelligence Analysis Centre (EU INTCEN) should be mentioned. Without an act of EU legislation and a particular competence mentioned in the TFEU,[52] the former Situation Center of the EU becomes more and more a kind of intelligence 'agency' of the EU Council. Since its establishment in 2011, it has been part of the European External Action Service.[53] INTCEN writes over 500 classified reports every year and cooperates with national intelligence services.[54]

In conclusion, the EU has recently been stepping up police and judicial cooperation in criminal matters, including the fight against terrorism. Mechanisms of cooperation are extended and broadened, this including significant exchange of personal data within the European Union. Although each initiative of the EU contains its own approach on data protection, an overall concept is still missing. The possibilities for gaining personal data from other Member States will become much easier for police and law enforcement. The extent to which intelligence agencies can make use of data is not clarified and remains unclear.[55] The new gathering of data, however, creates a huge

49 Council Decision establishing the European Police Office (Europol) [2009] OJ L121/37, arts 11–13.

50 Ibid, Arts. 14–16.

51 Proposal for Regulation (n 45) Arts. 49–50.

52 The legal basis of INTCEN remains unclear. A European intelligence agency might be based on Art. 222 TFEU. A European intelligence agency can provide two tasks: the coordination of intelligence agencies of the Member States and the information defence of the interests of the Union itself (in comparison to the European anti-fraud office regarding the EU´s combat on fraud).

53 <http://eeas.europa.eu/background/organisation/index_en.htm> accessed 22 august 2014.

54 See an interesting interview with the head of INTCEN Ilkka Salmi, available at <http://www.mo.be/node/37891> accessed 22 August 2014: 'All our reports are at least partially based on contributions from the Member States' intelligence and security services. In order to declassify the information, we would have to go back to those services. And they stick to their own national legislation, saying that the piece of intel or information they have provided us with, can't be declassified before a certain period of time. And of course we have to respect that'.

55 See the contribution of C Cocq, 'Developments of Regional Legal Framework for Intelligence and Information Sharing in the EU and ASEAN' in this Special Issue.

potential for access by any kind of state authorities. Clear control of the use of the data is missing on a European level and still remains the responsibility of the national data protection authorities.[56]

2.4 *The New European Data Protection Directive*

Data protection in the field of police cooperation within the EU is still based on the Framework Decision on Data Protection,[57] adopted before the Lisbon Treaty under the so-called third pillar of the EU.[58] This piece of legislation has significant loopholes. Three examples will suffice: first, its scope of application excludes important parts of the on-going cooperation (including Schengen, Europol or the Prüm Decision);[59] second, there exist significant exemptions to process or transfer of data without data protection guarantees;[60] third, there are extensive possibilities for refusing legal protection.[61]

The Union recently decided to revise the general legal framework of data protection, including the enactment of a new Data Protection Directive, which is exclusively dedicated to police and judicial cooperation in criminal matters.[62] However, in the proposal of the EU Commission there exist similar problems regarding the information of the data subject[63] and the right to access.[64] The Proposal opens the obligation to information of the data subject for broad exemptions:

Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject to the extent that, and

56 See the situation in Austria, for instance. In Austria, the Data Protection Act offers broad exemptions for police authorities and intelligence agencies.

57 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.

58 Before the Lisbon Treaty, the PJCC constituted the so-called third pillar of the EU, which was characterized by an intergovernmental approach instead of the supranational European approach of the first pillar. The effect was that decisions had to be agreed upon unanimously, the EP was not included in the decision-making process and the jurisdiction of the CJEU was limited.

59 See Recommendation No. 39 of the Council Framework Decision 2008/977/JHA (n 57).

60 Regarding third countries, see ibid, Art. 13 para 3.

61 Ibid, Art. 17 para 2.

62 Commission, 'Proposal for a Directive 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' COM(2012) 10 final.

63 Ibid, Art. 11.

64 Ibid, Art.12.

as long as, such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned: (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 rights and freedoms of others.[65]

These exemptions include all reasons for police activities and judicial cooperation in general. The state authority merely has to give any reason for the omission or restriction of the information of the data subject. In a similar way, the right to access can be limited by Article 13.1 of the Proposal, which provides the possibility for a partial or complete restriction to the right of access in a proportionate way to avoid obstructing official or legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties as well as to protect national or public security or to protect the rights and freedoms of others. Although the police authorities have the possibility to deny access, it is important that they communicate that access has been denied.[66]

The designation of a data protection officer regarding Article 30 of the Proposal cannot replace the effective legal protection of the individual. As an internal method of control, it has only limited possibilities for contributing to effective data protection, but at least it might create a certain awareness for data protection in the relevant authorities.

The transfer of personal data to third countries is subject to certain restrictions, which can be derogated from in many cases, including when '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; or the transfer is necessary in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[67] In these cases, adequate legal protection in the third country is not necessary. The

65 Ibid, Art. 11 para 4.

66 Ibid, Art. 13 para 3 final remains ambivalent with regard to the information passed to the person concerned: 'Member States shall provide that the controller informs the data subject in writing on any refusal or restriction of access, on the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. The information on factual or legal reasons on which the decision is based may be omitted where the provision of such information would undermine a purpose under paragraph 1'.

67 Ibid, Art. 36.

transfer of data only depends on the consent of the Member State and not on other restrictions.

If one compares the existing Framework Decision on Data Protection with the planned Directive on Data Protection regarding PJCC, the major advantage is that the new Directive will be under the full jurisdiction of the CJEU. Thus, the Court will be able to concretize the constitutional framework regarding data protection in PJCC. The draft legislation, however, contains the same problems of the Framework Decision on Data Protection. The restrictions (eg regarding information and right to access) or the exceptions (eg regarding an adequate standard of third countries) remain too wide. Police authorities can still easily circumvent the rights of the individuals to be made aware about data gathering and data exchange. Without knowing, any further legal protection will fail.

2.5 *Conclusion*

As this Section explained, the Stockholm Programme led to the establishment of a lot of new and more powerful databases to be used in the context of counter-terrorism. Together with the proposal for a Data Protection Directive regarding PJCC, which is lacking fully-fledged protection of data privacy, the perspective of the future of data protection in counter-terrorism and surveillance cannot be seen in an entirely positive light. The role of the CJEU, however, becomes more and more important. First, the CJEU itself achieved an important milestone by declaring the Data Retention Directive as unconstitutional. Second, the transitional provision regarding the Lisbon Treaty will end in December 2014.[68] After this transitional period the CJEU will have full jurisdiction regarding all legislative acts in police and judicial cooperation in criminal matters.[69]

Further ambivalence will remain due to the language of the EU treaties. National security is formally exempted from the competences of the Union. Yet, the borders between the competences of the EU and the Member States are far from being clear. The blurred situation of national security between exclusionary competences of the member states and the EU's counter terrorism activities based on different competences (e.g. PJCC or the solidarity clause in Art. 222 TFEU) show an unpredictable future of the role of the Union in questions of data protection in counter-terrorism. On the one hand, the Member States can claim that the role of intelligence agencies is exempted from the scope of EU competences. On the other hand, the Member States are contributing to the establishment of European intelligence

68 Lisbon Treaty (transitional provisions), Art, 10 of Protocol 36.

69 See, however, the limitations established by Arts. 275–276 of the Lisbon Treaty.

structures (like INTCEN or Europol) and so should be subject to EU data protection laws.

The ongoing post-Stockholm process will show how willing the EU is to impose substantive and procedural limitations on the increasing and expanding use of personal data in counter-terrorism. Only if this goal is achieved can data protection become effective in this field of EU law. The strengthening of the rights of individual will be a crucial part of effective protection in data privacy and much will depend on the CJEU, which signalled its willingness to protect personal data by striking down the Data Retention Directive.

3 Comparative Insights on Data Privacy and National Security

3.1 *Introduction*

Approaches towards national security have changed significantly since 9/11. Three main reasons driving these changes have to be taken into consideration: first the new attitude towards terrorism; second, the technical developments, especially with regard to communication technologies, and third, globalization as an economic, technical and political phenomenon. The result of these three developments has been a huge expansion of surveillance in the name of national security and counter-terrorism. Political readiness to extend counter-terrorism measures has led to a 'migration of anti-constitutional ideas'.[70] Counter-terrorism measures adopted since 9/11 have increasingly impacted upon human rights.[71] The privacy problems still seemed minor in comparison to questions of torture or the right to life. The intrusion into the private sphere of innocent people around the world, however, has increased enormously.

The privacy concerns emerged as a crucial issue during the last three years and were magnified by the Snowden revelations.[72] These showed a new

70 See K Lane Scheppele, 'The Migration of Anti-Constitutional Ideas: the Post-9/11 Globalization of Public Law and the International State of Emergency' in S Choudhry (ed), *The Migration of Constitutional Ideas* (Cambridge University Press 2007) 347–73.

71 See F Fabbrini, 'The Role of the Judiciaries in Times of Emergency: Judicial Review of Counter-terrorism Measures in the US Supreme Court and the European Court of Justice' (2010) 28 Oxford Yearbook of European Law 664; C Eckes, *EU Counter-Terrorist Policies and Fundamental Rights. The Case of Individual Sanctions* (Oxford University Press 2010).

72 See G Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books 2014). Edward Snowden revealed various covert activities by the US intelligence agency NSA, for which he was working. What was so particular about

dimension and a new quality of surveillance by the states and international co-operation between states and between states and private corporations. The aim is to gain as much information as possible about as many persons as possible. The demand for national and international protection of data privacy is becoming increasingly important in public discussions in liberal democracies.

As analysed above, the EU takes a strong rights-based approach, which has its foundation in the constitutional framework of the Union and the approach of the CJEU, especially after the Lisbon Treaty. Data privacy in the context of counter-terrorism cannot be understood as a regional phenomenon. The analysis therefore has to expand to a further transnational level beyond European perspectives. In a short comparative overview, the US and the Australian perspective shall be considered. From a rights-based perspective, both constitutional orders are of great interest. In contrast to the EU, both jurisdictions do not provide an explicit constitutional right to data privacy. The developments in the US and Australia are, however, very different. The US Supreme Court developed a rights-based perspective towards privacy based on the US Bill of Rights, whereas the Australian High Court, which cannot build upon a bill of rights, did not even provide a tort on privacy issues.

The three legal orders (EU, US, Australia) show that the challenge to address data privacy with regard to counter-terrorism is significant. The approaches embraced by the EU, the US and Australia towards data privacy are different. However, in any of the three legal orders, major deficits of data privacy can be identified when it comes to national security and counter-terrorism.

3.2 *The Constitutional Dimension*

The US in comparison to the European approach faces other challenges towards privacy.[73] The US Constitution does not contain an explicit right to privacy.[74] The case law of the US Supreme Court developed certain elements of a right to privacy based on the US Bill of Rights, especially the Fourth and the First Amendment.[75] In decisions such as *Katz v United States*,[76] and, recently,

---

the information provided by Snowden was the intensity and variety of the US surveillance. See more details about Snowden <http://www.theguardian.com/world/edward-snowden> accessed 22 August 2014.

73 See K Lachmayer and N Witzleb, 'Challenge to International Privacy from ever Increasing State Surveillance' (2014) UNSW Law Journal 748.

74 SJ Schulhofer, *More Essential Than Ever: The Fourth Amendment in the Twenty-First Century* (Oxford University Press 2012).

75 Th N McInnis, *Evolution of the Fourth Amendment* (Lexington Books 2009) 222–29.

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

Jones,[77] the US Supreme Court developed certain guarantees against surveillance by the state. At the same time, in cases in which the Court limited the right to privacy - like in the *Miller* case,[78] where the Court held that because a person voluntarily gave personal data to a third party (a bank) he waived his privacy right against the state accessing the personal data - the US legislator reacted and limited the possibilities for gathering information from banks. The rights-based approach in the case law of the US Supreme Court still remains limited and faces further restrictions, like the exclusive protection of US citizens. The US constitutional framework shifts the responsibility for protecting data privacy towards the legislature.[79] The US Congress has focused on counter-terrorism instead of promoting privacy over the last decade.[80] Privacy was not protected more effectively and personal data become more easily accessible for intelligence agencies. The legislative empowering of the administration regarding counter-terrorism created a big space for state surveillance.[81] Developments like the US Freedom Act, show a certain shift of the US Parliament towards stronger limitations of the activities of intelligence agencies. It remains unclear if the rights of individuals with regard to data privacy will be strengthened by the legislator at the same time.

The situation in Australia, finally, differs from that in the EU and the US. The constitutional framework in Australia is characterized by the absence of a Bill of Rights.[82] Data privacy is only guaranteed by parliamentary legislation. The Australian Privacy Act was recently reformed.

The Privacy Act has recently been amended to reflect changes in modern information practices. Under the revised Act, 'APP entities', which includes the

77 *United States v. Jones*, 132 S. Ct. 949, 565 U.S. (2012). The Court declared the car tracking tools as an unconstitutional search of a car. See also F Fabbrini and M Vermeulen, 'GPS Surveillance and Human Rights Review: The European Court of Human Rights and the US Supreme Court in Comparative Perspective' in F Davis, N McGarrity and G Williams (eds), *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge 2014) 134.

78 *United States v. Miller*, 425 U.S. 435 (1976).

79 See e.g. the initiatives towards the USA Freedom Act (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act) introduced by Representative Jim Sensenbrenner as HR 3361 in both houses of the U.S. Congress on October 29, 2013.

80 K Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University Press 2011) 184–6.

81 WC Banks, 'The United States a decade after 9/11' in VV Ramraj, M Hor, K Roach and G Williams (eds), *Global Anti-Terrorism Law and Policy* (Cambridge University Press 2012) 449 (470–78); K Roach, ibid (n 81) 175–186.

82 C Saunders, *The Constitution of Australia. A Contextual Analysis* (Hart Publishing 2011) 257–91.

(public sector) agencies and (private sector) organisations to which the Privacy Act applies, must handle personal information in conformity with the 'Australian Privacy Principles' (APP). The APP 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. 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 UK-USA 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)). In conclusion, the activities of the intelligence agencies are not subject to the Act and exceptions to the APP give law enforcement agencies relatively free reign in designing their information handling practices as well as easier access to information held by other agencies. The powers provided under ASIO Act 1979 and the Telecommunications (Interception and Access) Act 1979 have been significantly extended since 2001 and are due for further expansion under legislative proposals recently announced by the federal Government. The recent reforms of the Privacy Act, including the introduction of revised privacy principles, has not substantially changed Australia's surveillance situation.[83]

The lack of a fully-fledged privacy concept in the Australian legal order has led to an absence of limits in counter-terrorism regarding the gathering and exchange of personal data.[84]

83 This paragraph is based on Lachmayer and Witzleb (n 74); see also 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.

84 See G Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35 Melbourne University Law Review 1136–1176, 1150–1; see also D Hume and G Williams, 'Who's Listening? Intercepting the Telephone Calls, Emails and SMS's of Innocent People' (2006) 31

3.3 *Conclusion*

From a constitutional point of view, the starting points of data protection are quite different in the EU, the US and Australia, while it can be acknowledged that in the three legal orders there is a lack of data privacy when it comes to state surveillance and intelligence agencies. The EU depends to a significant extent on the constitutional approaches of the Member States, whereas the US and Australia refer to legislation. While the US Supreme Court as well as the CJEU has developed a stronger rights-based approach, the Australian approach has to rely on Parliament. Without privacy rights of individuals the effective limitation of counter-terrorism seems questionable. In each legal system the vertical separation of powers (in each form of federalism) comes into play and states also have – at least to a certain extent – the possibility to choose a more privacy-friendly approach or not. The federal surveillance initiatives still have to be addressed on a federal level.

The fostering of data privacy is facing the huge developments in the field of counter-terrorism in the last decade. The protection of data privacy depends on how far constitutional approaches towards data privacy are balanced with security issues.[85] The Snowden revelations increased the chance for a stronger impact of privacy in the surveillance debate. To analyse the constitutional struggle between data privacy and counter-terrorism beyond borders, the next section will focus on developments of privacy rights on an international level.

4 International Rights on Data Privacy

4.1 *Introduction*

Beyond the European and comparative perspective, the international level offers a broad variety of approaches towards privacy rights. To address global surveillance properly, it is necessary to develop international tools, which supplement domestic and regional approaches regarding privacy. When addressing the data privacy challenge on an international level, different perspectives have to be taken into account: the international dimension of surveillance, the

Alternative Law Journal 211 and G 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 177–239.

85 See K Lachmayer, 'Constitutional Limits to Security – An Introduction' in Eberhard et al (eds), *Constitutional Limits to Security. Proceedings of the 4th Vienna Workshop on International Constitutional Law* (Facultas Publishing & Nomos Publishing 2009) 9–19.

limits of institutional control by the states themselves and the effectiveness of data privacy. Only if these different elements are jointly considered might there be a chance for an appropriate approach towards data privacy regarding state surveillance and counter-terrorism.

The international dimension of state surveillance can only be properly addressed by the development of international standards of data privacy. There already exist different approaches and initiatives to data privacy in international law, including the general human rights catalogues like the UN International Convention on Civil & Political Rights (ICCPR) or the ECHR and certain international standards regarding data protection like the OECD Guidelines, the Council of Europe Convention 108 and further initiatives like the Madrid Resolution.[86] As will be explained in this section, these different international standards provide to a certain extent transnational principles and rights regarding data protection.

This paper illustrated that it is necessary to go beyond a general right to privacy and to provide certain more particular rights to individuals. The creation of new and the deepening of existing data privacy rights empowers the individuals to start judicial review and control state surveillance. A principle-oriented approach is able to define certain standards for state authorities; it is however not enough to bind authorities only by principles. It is also necessary to give individuals certain rights.

The empowerment of individuals is a crucial part of data privacy, including different elements like the right to be informed by public authority once data have been collected, the right to receive a (detailed) answer once the public authority is asked about the personal data detained, or the possibility to challenge in a court the rejection of information. However, different mechanisms have been developed to exempt state surveillance from effective legal protection. Substantive rights of data privacy have to be combined with certain procedural rights and an access to an independent court, which create the basis for effective legal protection.

4.2 *International Standards on Data Protection*

Different international standards offer an international legal framework for data privacy. Besides the efforts of the EU, the Council of Europe provides the

86 The Madrid Resolution arose from the 31st International Conference of Privacy and Data Protection Commissioners in Madrid and has been signed by more than 100 civil society organizations and privacy experts. More information about the Declaration, including translations, is available at <http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf> accessed 21 September 2014.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108[87]) as well as the Cybercrime Convention (Convention 185[88]). While the first offers certain general standards of data privacy (including rights in Art. 8 Convention 108), the second legitimizes the gathering of data by the states to fight cybercrime and opens up the exchange of personal data. Although both are not applicable regarding intelligence agencies, they are part of the international data protection framework and play an important role in international references to data protection. The relevance of these treaties for state surveillance, however, can only be achieved if the scope is extended explicitly.

Other more economic-focused approaches like the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[89] exclude questions of national security.[90] Based on the OECD Guidelines the APEC Privacy Framework[91] follows this concept of excluding national security.[92] The Madrid Privacy Declaration[93] by data protection and privacy commissioners from the

87 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981, entered into force 1 October 1985) CETS No.: 108.

88 The Cybercrime Convention has been ratified by most of the European countries (exceptions include Greece, Ireland, Poland, Russia, Sweden and Turkey), but also a number of non-CoE countries including Australia, Japan, Panama and the United States. OSCOLA-consistent reference is needed here too.

89 For the OECD Guidelines see <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 21 September. See also Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy' (2011) 1 International Data Privacy Law 6–13.

90 Ibid, part 2.4: 'Exceptions to the Principles … , including those relating to national sovereignty, national security and public policy ("ordre public"), should be: a) as few as possible, and b) made known to the public'.

91 Available at <http://publications.apec.org/publication-detail.php?pub_id=390> accessed 22 August 2014. See also G Greenleaf, 'Five years of the APEC Privacy Framework: Failure or Promise?' (2009) 25 Computer Law & Security Review 28–43.

92 Ibid, Art. 13: 'Exceptions to these Principles … , including those relating to national sovereignty, national security, public safety and public policy should be: a) limited and proportional to meeting the objectives to which the exceptions relate; and, b) (i) made known to the public; or, (ii) in accordance with law'.

93 At the time of the 31st International Conference of Privacy and Data Protection Commissioners in Madrid, more than 100 civil society organizations and privacy experts had signed the Madrid Privacy Declaration. For more information, see < http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_en.pdf> accessed 21 September 2014.

year 2009 also provides restrictions to data protection in a way, which resembles Article 8 para 2 ECHR.

On a UN level the protection of respect for privacy in Article 17 of the ICCPR,[94] includes but does not distinguish specific data protection rights.[95] Moreover, the UN General Assembly calls upon all states in a recent resolution on the 'Right to privacy in the digital age' (68/167):[96] 'to respect and protect the right to privacy, including in the context of digital communication' and to 'take measures to put an end to violations of those rights and to create the conditions to prevent such violations' especially to 'review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law'. This resolution could be a starting point for further initiatives towards an international treaty of data protection.

In conclusion, a fragmented structure of an international data privacy framework can be identified.[97] Besides the general international human rights regimes, different forms of principles and rights, especially by soft law, are provided on an international level. State surveillance is to a certain extent excluded from the scope of the international data privacy framework. The development and amendment of existing international treaties as well as the jurisdiction of international human rights courts and bodies will be necessary to improve data privacy in the fields of police authorities and intelligence agencies. Moreover, transnational data flows in the context of surveillance have to be addressed explicitly by international conventions.

4.3 *Developing International Digital Rights*

All international standards of data privacy include certain rights.[98] State surveillance is often excluded as far as privacy rights are concerned. One international approach can be found in international human rights catalogues,

94 See LA Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247, 252–54.

95 See S Joseph and M Castan, *The International Covenant on Civil and Political Rights. Cases, Materials and Commentary* (Oxford University Press 2013) 559–61.

96 <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167> accessed 22 August 2014.

97 See LA Bygrave, *Data Privacy Law. An International Perspective* (Oxford University Press 2014).

98 See the analysis of national and international developments in data protection laws in G Greenleaf, 'Data protection in a Globalised Network' in I Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar 2013) 221–54.

which refer to privacy as a human right. National security, however, is always a legitimate justification for restricting privacy. The limits of the principle of proportionality seems weaker in comparison to other rights.

A general right to privacy is a starting point for dealing with the challenges of data privacy by counter-terrorism measures by states. If one wants to address these challenges to data privacy on an international level, different rights are necessary to address the various elements of privacy in the information society. From a normative perspective, several liberal rights could be developed in the direction of digital rights in the information age. As surveillance and data exchange are getting more complex, it is necessary to distinguish more clearly between different elements of data privacy. Based on a fundamental right to self-determination of the use of personal data, different digital rights can be developed, including the prohibition of internet censorship and the guarantee of the freedom of speech in the context of cyberspace participation; a right to non-discrimination by profiling software; the right to be informed, the right of access, the right to rectify and to delete (including the right to be forgotten, also by the state) as well as the right to object. Certain rights have to be clarified in the context of surveillance. Absolute limits could be established like the prohibition of erasure or manipulation of the identity of a person in digital systems of a state. Another important possibility would be a certain time limit, after which everybody has to be informed about covert surveillance. Furthermore, a right to access has to include all the countries and other organisations where the personal data has been transferred. The German Constitutional Court showed that it is possible to develop further rights to limit state surveillance in the digital age (Right in Confidentiality and Integrity of Information Technology Systems[99]). In conclusion, the existing privacy rights can be taken much further and we can learn from certain domestic or regional approaches to enable appropriate protection of the individual in the digital age.

5 Conclusion

In the last decade counter-terrorism activities have led to a migration of anti-constitutional ideas.[100] The intrusion into the privacy of people all over the

99 See BVerfG, 27.2.2008, 1 BvR 370/07. The German Constitutional Court had to decide to what extent the intelligence agencies are allowed to intrude into personal computers of individuals by using the internet. Deciding that this form of intrusion is unconstitutional, the German Constitutional Court argued that this kind of surveillance violates the newly established constitutional right.

100 Scheppele (n 71).

world has become apparent in recent years. The need for an adoption of a more sophisticated concept concerning the protection of data privacy in the information seems obvious. This article has shown that it is necessary to follow a rights-based approach to challenge and limit transnational surveillance measures and data exchange of states effectively.

Starting from a strong rights-based approach in the European Union, the article has followed in a comparative perspective the development of privacy rights in the US and illustrated the problems evolving in a country like Australia, where privacy rights are lacking on a constitutional level. The efforts on a domestic level to establish certain limits on state surveillance have already created a significant challenge. All three legal orders have to struggle to address intelligence agencies in the context of data privacy rights. Parliaments and (constitutional/supreme) courts will have to work together to develop certain privacy standards. Moreover, trans-national cooperation and international agreements will be necessary to address these challenges. The international human rights regimes offer certain rights to privacy; however, a more differentiated approach would be necessary to address all the different issues of data privacy in the context of trans-border surveillance.

In conclusion, it might be interesting to come back to the example at the beginning of the paper. The Austrian student did not only receive the information from the Austrian Ministry of Interior, but a public discussion was started if this data storage was legal and legitimate. The effectiveness of data privacy rights contributes to a functioning democracy. The introduction of a general framework for data protection in the European Union gives the EU the possibility to develop an effective rights system and to guarantee data privacy rights. In a comparative perspective liberal democracies all over the world have to face the same challenge to rethink privacy domestically and beyond borders. The establishment of an international framework of data privacy, which is focussing on questions of state surveillance, would be an adequate answer to the global cooperation of intelligence and law enforcement agencies.