JCMS Journal of Common Market Studies
JCMS 2018 Volume 56. Number 4. pp. 751–767 DOI: 10.1111/jcms.12634

Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair*

ANNA DIMITROVA[1] and MAJA BRKAN[2]
[1]ESSCA School of Management, France [2]Maastricht University

Abstract

Based on the unparalleled number of recent data protection reforms triggered by Snowden's revelations on both sides of the Atlantic, this article aims to examine the interplay between the two main transatlantic actors striking the balance between national security and privacy, namely EU and US policy-makers and courts. We argue, on the one hand, that the NSA affair has opened a window to policy-makers to pursue reforms in order to attain a level of adequacy of their respective data protection legal regimes. On the other hand, although some data protection reforms have been adopted by legislators in response to courts acting as reformers in the post-Snowden context, the EU and US courts' approaches to balancing national security and data protection remain diametrically opposite. Drawing upon recent case law, we demonstrate that US courts continue to tilt the balance in favour of national security while EU courts retain their pro-privacy stance.

Keywords: EU and US policy-makers and courts; privacy and data protection law; national security; NSA mass surveillance; Snowden's disclosures

Introduction

Despite the elapse of years, the impact of Snowden's disclosures – revealing the existence of several top-secret mass surveillance programmes run by the United States (US) National Security Agency (NSA) and some of its 'Five Eyes'[1] partners that aimed at accessing, collecting and processing in bulk the electronic personal data of both US persons and non-US persons, including European Union (EU) citizens and officials – has had 'a roiling, still unfolding effect' (Miller, 2017, p. 1) on both sides of the Atlantic in several contexts.

First, these revelations have reinvigorated the longstanding debate on balancing national security and civil liberties (Davis, 2003; Miller, 2017) by drawing fresh attention to the differences between the European and US approaches to privacy and data protection. These differences mostly stem from different cultural traditions in the two regions (Whitman, 2004) and the US reaction to the terrorist attacks of 2001, which resulted in the expansion of US extraterritorial surveillance (Newman, 2011; Suda, 2013). A prevailing view in this debate is that the US traditionally strikes the balance in favour of national security while the EU has a more measured approach that privileges law enforcement and

*The authors would like to thank the editors and the anonymous referees for their very helpful comments to improve this article. We are also very grateful to Professor Roger Snijders for his insightful suggestions on an earlier version of this paper.

[1] A communication intelligence sharing agreement between the United States, the United Kingdom, Australia, Canada and New Zealand.

civil liberties (Bignami, 2007, 2015; Boehm *et al*., 2015; Bowden and Bigo, 2013; Schwartz, 2013; Schwartz and Solove, 2014).

Second, it is generally argued that despite 'battles over privacy' (Farrell and Newman, 2013), close EU–US co-operation on intelligence sharing and counter-terrorism was established in the aftermath of 9/11 (Jančić, 2016; Pleschinger, 2006; Suda, 2013; Tzanou, 2015), which had the effect of sidelining EU privacy advocates. However, Snowden's revelations about the US spying on matters not necessarily related to terrorism have reversed, according to this view, the balance between national security and privacy in Europe and 'Europe's political pendulum swung back in favour of privacy advocates' (Farrell and Newman, 2013).

Third, and finally, the existence of mass surveillance programmes is not in itself new. What is unprecedented and striking today, however, is the sheer scope and magnitude that US electronic foreign intelligence activities have achieved as a result of technological advancements. Hence, there is 'an urgent need for a systematic assessment of the scale, reach, and character of contemporary surveillance practices, as well as the justifications they attract and the controversies they provoke' (Bauman *et al*., 2014, p. 122).

While it is the case that examining the change in the balance between national security and privacy in the context of post-Snowden developments is undoubtedly a very challenging topic, this contribution adopts a different approach. Based on the unparalleled number of recent privacy and data protection reforms implemented on both sides of the Atlantic, we aim to examine the impact of the NSA affair on two interconnected actors: the policy-makers and the courts. By policy-makers, we understand the US legislator (US Congress) and the US administration (including agencies such as NSA) and, on the EU level, the EU legislator (Council of the EU and European Parliament) and EU administration (European Commission). In line with the view that courts can produce significant social reform and act as 'public entrepreneurs' (Mattli and Woods, 2009, p. 30) under specific conditions, we argue that these conditions occurred in the aftermath of the mass surveillance revelations since the NSA scandal gave new impetus to both EU and US legislators and courts to adopt data protection reforms. In this context, the judicial constraint in the US was partially overcome because there was a support for change from both the Executive and Congress under the Obama Administration, while on the EU side there was strong pressure to reform existing EU–US data transfer agreements in order to meet the EU requirement of adequacy of the level of EU citizens' data protection ensured by the US. Yet, as stemming from the recent media reports, it can be argued that the Trump administration will pursue an aggressive surveillance policy; it is yet to be seen what impact such a policy will have on the courts' take on surveillance.

Building on this theoretical framework, we put forward a twofold argument. On the one hand, we argue that the NSA affair has opened a window both to policy-makers and courts to institute reforms in the EU and US data protection legal regimes, thus trying to bring the level of protection to an 'adequate level', all while recognising the continuous divergences between their approaches to privacy.

On the other hand, despite the fact that some data protection reforms have been adopted by legislators in response to courts acting as reformers, US courts have issued only a few pro-privacy opinions and continue to endorse, in the majority of cases, a security-based approach. Even in the recent *Riley v California* case (2014) that was praised as a 'victory for individual privacy rights and a signal to law enforcement that its

investigative powers are not without limits' (Lamparello and MacLean, 2014, p. 28), the Supreme Court's pro-privacy decision was in fact adopted in a case in which government interests were low, while privacy interests were high and universally shared (*Harvard Law Review*, 2014, p. 258). In contrast, the European courts retain their pro-privacy stance, as shown in some recent cases such as *Digital Rights Ireland* (2014), *Schrems* (2015) and *Tele2 Sverige* (2016), thereby confirming privacy as a core value of the European society.

In order to examine this hypothesis, the article is structured as follows. First, it examines the differences between the EU and US policy-makers' approaches to balancing national security and privacy before and after mass surveillance revelations. A special focus is put on reforms undertaken by the EU and US policy-makers in response to the NSA affair by arguing that legislators on both sides of the Atlantic have been seeking to achieve an adequate level of protection in relation to the processing of personal data. Second, it analyzes courts' approaches to balancing national security and privacy issues before and after the scandal by stressing that although in some cases courts have been of help to reformers, their ruling in the matter keeps on acting as a source of transatlantic divergence.

I. Policy-Makers and Mass Surveillance: In Search of an 'Adequate' Level of Data Protection?

Policy-makers' Approach before Mass Surveillance Revelations

It is traditionally argued that the EU and the US approaches to defining 'privacy' and 'personal data' are fundamentally different (Bignami, 2007, 2015; Boehm *et al*., 2015; Davis, 2003; Schwartz, 2013; Schwartz and Solove, 2014).

Often described as a 'patchwork of federal and state statutes' (Weiss and Archick, 2016, p. 3), the complexity of US data protection law stems from constitutional protections, statutes and private law rules (Solove and Schwartz, 2009). The cornerstone of the right to privacy under US law is the Fourth Amendment which lays down the two main guarantees of the right to privacy: 1) the 'search and seizure clause and the requirement of reasonableness' (Fowler, 2014, p. 212), meaning that any search and seizure requires the finding of a 'reasonable articulable suspicion' (RAS) that the search term is associated with a certain person believed to be involved in a crime-related or national security investigation; and 2) the 'warrant clause and the requirement of probable cause' (Fowler, 2014, p. 213) postulating that a search conducted without a prior court order is considered unconstitutional. However, the balancing between competing state and individual interests is difficult because the presumption that 'warrantless searches are per se unreasonable' is subject to a number of exceptions, in particular the 'national security exception' (Atkinson, 2013; Fowler, 2014) which will be discussed later.

US modern foreign intelligence activities and programmes find their legal basis mainly in the Foreign Intelligence Surveillance Act (FISA) adopted by Congress in 1978, in the wake of the surveillance scandals of the 1970s, especially the Watergate affair. The legislation was enacted 'to provide greater protection of civil liberties by erecting a wall between intelligence collection and law enforcement' (Davis, 2003, p. 175). A special court was established by the provisions of the FISA under the name of Foreign

Intelligence Surveillance Court (FISC) to grant or deny orders authorizing electronic surveillance of particular targets (Donohue, 2014, p. 784). However, non-US persons are explicitly excluded from the scope of this provision.

The 'double-track' system of US privacy law also operates in the case of the Privacy Act of 1974 which is considered as 'the closest analogue to a European data protection law in that it seeks to regulate comprehensively personal data processing, albeit only with respect to federal government departments and agencies' (Bignami, 2015, p. 10). It contains some of the main principles of EU data protection law, such as the principle of transparency in personal data processing and the principle of proportionality.[2] However, data mining for national security purposes is exempted from the enforcement of the Privacy Act. Additionally, the application of the Act is limited only to US residents.

The terrorist attacks of 9/11 pushed national security to the top of the list of the US government's priorities and prompted the overwhelming majority vote for the USA Patriot Act.[3] The latter made significant amendments to FISA by giving 'federal law enforcement and intelligence officers greater authority to gather and share evidence from wire and electronic surveillance' (Doyle, 2001, p. 4). Furthermore, under Section 215, the Patriot Act actually allowed intelligence agencies to expand their surveillance activities at the expense of the right to privacy and data protection by giving them access to records and other items for foreign intelligence and international terrorism investigation purposes. Additionally, Section 505 expanded the use of the National Security Letters (NSLs), administrative subpoenas authorizing government agencies, without prior judicial approval, to gather information for national security purposes.

One more legal document worth mentioning is the FISA Amendments Act, voted upon in 2008. Section 702 of this Act has been at the centre of critiques because it provides the legal basis for NSA surveillance practices by giving the agency a blank cheque to target, without a warrant, the communications of foreign targets, namely non-US citizens and persons outside the US, for national security purposes. It thus reaffirms that US surveillance law does not treat US and non-US citizens equally.

Despite the fact, that throughout the years, US policy-makers have attempted to strengthen the safeguards on privacy and data protection, there are still numerous legal loopholes that allow US intelligence agencies to possess double standards on regulations related to domestic and foreign surveillance.

By way of contrast, under EU law, both privacy and data protection are viewed as fundamental rights (Amtenbrink, 2013; Horsley, 2015) protected by the Charter of Fundamental Rights of the European Union (Charter) in Articles 7 and 8, respectively. The origins of the EU right to privacy are found in Article 12 of the United Nations (UN) Universal Declaration of Human Rights (UDHR) of 1948 and in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) of the UN of 1966 which are the first international legal instruments to lay down the foundations for protecting the right to privacy from intrusion from others, especially from the state. These legal instruments epitomise the rights-based approach towards privacy and data protection in Europe. Besides the EU law sources for the right to privacy, it is also necessary to take into account the relevant provisions of the European Convention on Human Rights (ECHR)

[2] Title 5, §552a, Privacy Act, p. 47.
[3] USA Patriot Act, Public Law 107–56 of 26.10.2001, 107th Congress (2001–2003).

and their interpretation by the European Court of Human Rights (ECtHR). According to Article 6(3) of the Treaty on European Union (TEU), fundamental rights as guaranteed by the ECHR 'shall constitute general principles of the Union's law'. This leads to the result that the rights embedded in the Charter should be interpreted as having the same meaning and scope as those in ECHR, whereby a more extensive protection is not precluded.[4]

There has been some discussion in the literature as to the distinction between the right to privacy and the right to protection of personal data, but to date this distinction is not entirely clear (Lynskey, 2014). Moreover, ever since its recognition as a fundamental right, the right to data protection has been continuously expanding in its scope of application, both within and outside of the EU (Brkan, 2016). This expansion is highly relevant because the EU data protection rules will, to a certain extent, apply also to US-based companies which will need to conform to the EU legislation. The principal EU legal document on data protection currently in force is the General Data Protection Regulation (GDPR)[5] which will be applicable as of 25 May 2018.[6]

Unlike the EU privacy and data protection law, US law contains neither a comprehensive definition of 'privacy' (Solove, 2002) nor a comprehensive approach to 'privacy' (Farrell and Newman, 2016, p. 129). Instead, the US Constitution defines different aspects of 'privacy', such as the 'right to freedom of expression' and the 'right of people to be secure in their persons and houses against unreasonable searches and seizures'. There is also no coherent definition of 'personal data'. The latter most often refers to 'any information which identifies a person' and is, in this sense, equivalent to 'personally identifiable information (PII)', but there are other meanings that can be encountered in various laws and regulations (Schwartz and Solove, 2011, pp. 1828–1836).

Additionally, the differences between the two legal systems in terms of law enforcement are also noteworthy, especially when national security interests are involved. In this context, the US surveillance law is far more permissive than the EU law because it is largely governed by the principle that 'surveillance is legal unless forbidden' (Richards, 2013, p. 1942), and that personal data processing is allowed unless it causes a legal harm or is limited by law (Schwartz and Solove, 2014, p. 882; Tourkochoriti, 2014, p. 164). In other words, conducting an anti-terrorism investigation and data mining could very well be legal under US law; by way of contrast, under EU law any personal data processing and surveillance activities are forbidden in the absence of a legal basis (Bignami, 2007, p. 609). The approach of the EU is therefore diametrically opposite to the one in the US.

Policy-makers' Response to Mass Surveillance Revelations

The reforms of policy-makers regarding the balancing of national security and privacy are currently visible at three levels.

At the US level, since Snowden's disclosures, two dozen significant actions to reform surveillance laws and programmes have been undertaken including independent reviews of the NSA activities, the legislative and executive branch actions (Swire, 2015a, p. 22).

[4] Art. 52(3), Charter of the Fundamental Rights of the European Union, 2000/C 364/01.
[5] Regulation (EU) 2016/679 of the European Parliament and the Council of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.
[6] See Art. 99(2) of the GDPR (General Data Protection Regulation).

One of the most prominent legislative actions was the passing of the USA Freedom Act[7] by Congress on 2 June 2015. Qualified by some civil liberties advocates as 'the biggest pro-privacy change to US intelligence law since the original enactment of the Foreign Intelligence Surveillance Act in 1978' (Swire, 2015b, p. 1) because it restricts the bulk collection of electronic data of US citizens, this legislation can only partly satisfy EU privacy observers for it does not really apply to US surveillance overseas (Swire, 2015b, p. 7). Nevertheless, it paved the way for the passage of the Judicial Redress Act[8] a few months later. Adopted on 24 February 2016, this Act authorizes the Department of Justice to extend the protection of the Privacy Act of 1974 to non-US citizens of designated foreign countries by granting them the right to bring a civil action against US agencies that intentionally violate conditions on disclosing records without the consent of the individual to whom the records belong.[9] The enactment of the Judicial Redress Act was surrounded by high stakes regarding not only the NSA affair but also earlier EU calls on US policy-makers to amend the Privacy Act in order to provide judicial redress to Europeans. Although the Judicial Redress Act was welcomed by the European Commission as 'a historic achievement' in the EU–US efforts to restore trust in transatlantic data flows,[10] it is to be noted that it contains numerous exceptions and limitations. In fact, the law enforcement system of records for national security purposes remains exempt from access and amendment. Consequently, it gives Europeans the right 'to sue to enforce only some, but not all, of the rights that US citizens can sue to enforce under the Privacy Act' (Hasbrouck, 2016, p. 22).

At the European level, following Snowden's leaks, Members of the European Parliament (EP) called on the European Commission to apply more intensive scrutiny and even suspend some EU–US data sharing accords in the commercial, security and law enforcement sectors (Jančić, 2016; Weiss and Archick, 2016). Moreover, courts' rulings, especially the CJEU's decision in the *Schrems* case (2015), were consequential in effecting significant social reform and thus put more pressure on EU and US policy-makers to finalize the replacement of the invalidated Safe Harbor agreement with the Privacy Shield.[11] During the negotiations of the latter, the EP continually urged the Commission to remedy deficiencies in this agreement.[12] Even after its adoption on 12 July 2016, the EP issued a resolution on Privacy Shield in which it voiced 'great concerns' about the level of protection of personal data in the US, especially after contentious executive orders were issued by the Trump administration.[13] It is therefore submitted that the EP often acts as a watchdog over the Commission's actions which makes it the most pro-privacy oriented institution of the EU. In contrast with the EP, regarding the Privacy Shield adoption, the Commission proved itself as a negotiator searching for midway

[7] USA Freedom Act, Public Law, 114–23 of 2.6.2015, 114th Congress (2015–2016).
[8] Judicial Redress Act, Public Law 114–126 of 24.2.2016, 114th Congress (2015–2016).
[9] Sec. 2, Judicial Redress Act.
[10] EC press release of 24.2.2016, 'Statement by Commissioner Věra Jourová on the Signature of the Judicial Redress Act by President Obama'.
[11] European Commission, 'Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield', Art. 2.
[12] Press release of the 26.5.2016 Plenary session of the European Parliament, 'EU-US "Privacy Shield" for data transfers: Further improvements needed, MEPs say'.
[13] European Parliament resolution of 6.4.2017 on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP)), at para 23.

solutions whose positions were criticized also by the Article 29 Working Party (Cadiot *et al*., 2016). However, the Privacy Shield is a highly political instrument in which 'legal disagreements' are 'essentially political arguments in disguise' (Kuner, 2017, p. 35) and which might put the EU institutions' role under a different spotlight. Indeed, the Commission was equally seeking to attain a high level of data protection in the GDPR adoption by introducing, for example, the new duty for data controllers requiring them to assess the risks of processing data in advance.[14] Among the three EU institutions, the Council remains, perhaps, the most 'neutral' institution without strong opinions on data privacy matters.

The NSA affair had a broader impact than just on the Privacy Shield and the GDPR; it undoubtedly also had an influence on the adoption of the Directive on Data Protection for Prevention of Criminal Offences[15] on 27 April 2016. This Directive aims to regulate the free movement of personal data within the Union,[16] as well as the transfer of personal data to a third country on the basis of an adequacy decision allowing the Commission to assess the adequacy of the level of protection.[17] At the same time, the Passenger Name Record (PNR) Directive was also adopted which contains rules on the transfer of personal data of aircraft passenger from the EU to the US authorities for the purpose of combating terrorism.[18]

At the transatlantic level, efforts to provide stronger safeguards related to the US government when accessing EU citizens' personal data resulted in the signature of the EU–US 'Umbrella Agreement'[19] on 2 June 2016. It is important to note that the latter could only be adopted after the passing of the Judicial Redress Act which was a substantive prerequisite for the conclusion of the 'Umbrella Agreement'. The latter allows the sharing of data sent by EU law enforcement agencies to US law enforcement agencies and puts limits on the 'onward transfer' of such data to third parties. Moreover, it also strengthens legal safeguards by granting EU citizens the right to seek judicial redress with regard to records containing their personal information, including the case of 'unlawful disclosure of such information that has been wilfully or intentionally made'.[20] However, the 'Umbrella agreement', although it allows for the conclusion of further agreements between the US and the EU or the Member States,[21] is not an all-encompassing 'umbrella', as it covers only law enforcement purposes and not any further possibilities for determining material standards of data protection.

[14] Art. 35 and Art. 36 of the GDPR.
[15] Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, (EU) 2016(680), OJ L 119/89 (Directive on Data Protection for Prevention of Criminal Offences).
[16] Art. 1(1), Directive on Data Protection for Prevention of Criminal Offences.
[17] Art. 36 (2), (3).
[18] Art. 1 and 2 of the Directive (EU) 2016(681) of 27.4.2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
[19] European Commission draft for initialling of 2.6.2016, 'Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offences' (Umbrella Agreement).
[20] Art. 19, Umbrella Agreement.
[21] Art. 3.

II. Courts and Mass Surveillance: The Source of Transatlantic Divergence?

Balancing National Security and Data Protection: The Early Case law of US Courts

When balancing between national security and privacy, the US Supreme Court announced strict rules, under the Fourth Amendment, for government surveillance practices or wiretaps, although these rules are different for law enforcement uses (crimes) and national security (foreign intelligence) (Swire, 2015a, p. 6).

The case of *Olmstead v United States* (1928) led to the first debate over how electronic surveillance is related to the rights established under the Fourth Amendment. In this case, the Court held that the interception of telephone communications, not requiring a physical trespass onto a person's property, did not amount to a search or seizure within the meaning of the Fourth Amendment'.[22] The Court's ruling was much debated because it actually permitted 'non-trespassory forms of electronic surveillance' (Atkinson, 2013, p. 1360).

The contradictory 'trespass doctrine' was confirmed in other cases, namely *Goldman v United States*[23] (1942) and *Lee v United States*[24] (1952), thus setting up the legal standard for surveillance at the expense of individual privacy for several decades. Breaking new ground, the Supreme Court finally overruled the 'trespass doctrine' in *Katz v United States* (1967) by holding that 'because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure'.[25] It was also held that any intrusion, be it physical or electronic, of a place where a person has a 'reasonable expectation of privacy', may constitute a violation of the Fourth Amendment.[26] Moreover, FBI wiretapping was qualified as 'unreasonable' because it was undertaken without any warrant authorizing it.[27] Hence, for the first time, the Court in *Katz* endorsed a privacy-based approach to the Fourth Amendment (Larkin, 2013, p. 4). Yet it is noteworthy to underline that in footnote 23 the Court introduced the 'national security exception doctrine' by pointing out that '[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case'.[28] Footnote 23 in the *Katz* case was interpreted by the US government as a 'judicial blessing of the national security exception' (Atkinson, 2013, p. 1380) and has had a crucial influence on surveillance activities.

The question of regulating surveillance related to national security was later addressed in *United States v United States District Court* (1972), commonly called the '*Keith*' case. While the government asserted that 'the surveillance was lawful, though conducted without prior judicial approval, as a reasonable exercise of the President's power to protect the national security',[29] the District Court ruled that government's surveillance for domestic national security purposes had to respect the warrant requirement. However, this case did not give an explicit answer as to whether the warrant clause applied to situations of

[22] *Olmstead v United States*, 277 U.S. 438 (1928), p. 277 U.S. 466.
[23] *Goldman v United States*, 316 U.S. 129, 135–36 (1942).
[24] *Lee v United States* 343, U.S. 747 (1952).
[25] *Katz v United States*, 389 U.S. 347 (1967), p. 389 U.S. 351.
[26] *Katz v United States*, p. 389 U.S. 361.
[27] *Katz v United States*, p. 389 U.S. 363.
[28] *Katz v United States*, p. 389 U.S. 358, n. 23.
[29] *United States v United States District Court for the Eastern District of Michigan*, 407 U.S. 297 (1972), p. 301.

foreign intelligence surveillance. Hence, in *Keith*, the District Court not only confirmed the existence of the 'national security exception' doctrine, but also introduced the distinction between domestic security surveillance subject to the Fourth Amendment's guarantees for protecting the right of privacy, and foreign security surveillance that remained in the hands of the Executive and, consequently, exempted from any oversight (Goitein and Patel, 2015, p. 19).

For the first time the 'national security exception doctrine' was officially recognized by the US Court of Appeals for the Fourth Circuit in *United States v Truong Dinh Hung* (1980). In this case, the Court of Appeals accepted the government's argument that there exists a foreign intelligence exception to the warrant requirement and stressed that 'the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, "unduly frustrate" the President in carrying out his foreign affairs responsibilities'.[30]

The key findings of the above-analyzed cases reveal, first, that the US courts have frequently endorsed a national-security approach to the Fourth Amendment whose provisions appear to be 'nebulous and adaptive' (Fowler, 2014, p. 211). Second, the Fourth Amendment rests upon a 'double-track' system based on the distinction between domestic security and foreign security surveillance. Accordingly, it treats US persons and non-US persons differently. Last but not least, guarantees and safeguards related to US persons' privacy are minimal, even more so when applied to EU citizens (Bignami, 2015).

The Recent Case of US Courts

Clapper v Amnesty International[31] (2013) represents one of the Supreme Court's most recent cases that evaluates the government's inference in people's privacy in the post-Snowden era. In this case, various US human rights organizations challenged the constitutionality of Section 702 of FISA which authorized electronic surveillance by the federal government for foreign intelligence purposes. The plaintiffs' argument that they were suffering present injuries because their telephone and e-mail communications were wiretapped by the government was rejected by the Court, thus tipping the balance in favour of national security interests.

The tendency of rulings in favour of national security continued in later case law. The government's surveillance of internet communications under Section 702 of FISA was also challenged in *Klayman v Obama* (2013), whereby the District Court for the District of Colombia ruled that the NSA data collection programme was most likely unconstitutional,[32] but stayed the order pending an appeal review by the US Court of Appeals for the District of Columbia Circuit. The latter disagreed with the District Court by stressing, as in *Clapper v Amnesty International*, there was no substantial evidence that the plaintiffs' metadata were collected by the government.

The pro-surveillance tendency of US courts was, however, interrupted in some cases which enabled further legislative reforms in the US. A case conflicting with *Klayman v Obama* is *ACLU v Clapper* (2013). The American Civil Liberties Union (ACLU) brought a lawsuit against James Clapper, the Director of national intelligence, by claiming that the

[30] *United States v Truong Dinh Hung,* US Court of Appeals for the Fourth Circuit, 629F.2nd 908 (4th Cir. 1980).
[31] *Clapper v Amnesty International*, US Supreme Court, 638F, 3d 118 (2013).
[32] *Klayman v Obama,* 957 F. Supp. 2d 1, 43–44 (D.D.C. 2013).

NSA data mining programme was illegal on both constitutional and statutory grounds. In May 2015, the Court of Appeals for the Second Circuit ruled that the NSA activities exceeded the scope of what Congress had authorized in Section 215 of the USA Patriot Act. Although Section 215 was amended by the Freedom Act which prohibits the bulk collection of personal data, it is worth noting that this amendment concerns only US-citizens and the 'national security exception' to the Fourth Amendment rights continues to be applied by US courts.

Another recent case loudly applauded by privacy advocates 'for endorsing a rule that protects digital privacy' (*Harvard Law Review*, 2014, p. 251), is *Riley v California* (2014). In *Riley*, the Court held that law enforcement officers could seize but not search an arrestee's cell phone 'incident to arrest' without a warrant or an absent exigent situation. To assess the reasonableness of the search, the Court conducted a balancing analysis by weighing the government's interests against the plaintiff's privacy interests. The Court's decision was thus taken in a very specific situation where government interests were not substantial, while cell-phone searches implicated very high privacy interests. Hence, it was an 'easy case under reasonableness balancing' (*Harvard Law Review*, 2014, p. 260). For this reason, the decision in *Riley* will hardly set up a legal standard for endorsing a privacy-based approach in future cases.

Notwithstanding some reforms and a few pro-privacy cases in the US, it is most likely that the US and EU courts' approaches to balancing data protection and national security will continue to diverge.

Balancing National/Public Security and Data Protection: The Case of Europe's Courts

Before examining the case law of European courts, it needs to be pointed out that the notions of 'national security' and 'public security' should be distinguished under EU law. According to Article 4(2) TEU, 'national security remains the sole responsibility of each Member State'. This means that the term 'national security' is limited to the security of each particular Member State and not of the Union as a whole and that the Union's competence does not extend to encompass issues of national security. It has already been stressed that there is an absence of a clear definition of the term 'national security' in EU law.[33] The term that is used rather more frequently in data privacy legislation is 'public security'. Although this notion is not defined in EU law, it is deemed to be a broader notion extending to the security within the whole EU. The notion of public security can be found in other fields of EU law, namely in Article 36 of the Treaty on the Functioning of the European Union (TFEU) concerning the justifiable grounds for restrictions of free movement of goods, in Article 45 TFEU relating to free movement of workers and in Article 202 TFEU concerning the freedom of workers from overseas countries and territories. 'Public security' therefore relates more to the security of the European public, its citizens and the EU territory.

It is important to clarify that the GDPR is not applicable to national security, or to public security. According to its Article 2, the GDPR does not apply to processing of data relating to 'the prevention of threats to public security'.[34] The legal instrument on the basis

[33] Working Party 29, Working Document on surveillance of electronic communications for intelligence and national security purposes of 5.12.2014, WP 228, pp. 21–24.
[34] Art. 2(2)(e) of the GDPR.

of which it is possible to process data relating to public security is the Directive 2016/680, also known as the Directive on Data Protection for Prevention of Criminal Offences. It expressly states that it regulates the protection of personal data with regard to the 'prevention, investigation, detection or prosecution of criminal offences', including 'the prevention of threats to *public security*'.[35] Moreover, the Directive also allows the Member States to restrict the provision of information on data subjects in order to protect public security or national security[36] and can, on the same grounds, limit the data subject's right of access.[37]

The Early Case law of the European Courts

The early case law on balancing of national security with privacy can be found mostly in the jurisprudence of the ECtHR. The ECHR expressly puts forward the possibility of balancing between privacy and national security or public safety. According to Article 8 ECHR, 'everyone has the right to respect for his private life', but the public authorities can interfere with that right 'in the interests of national security or public safety'. It is important to stress that the notion of 'public safety', in the context of the interpretation of the ECtHR, can be understood either as national security or the prevention of disorder or crime (Greer, 1997, p. 18); it will therefore not be examined as a separate category of prevailing national security interests. When analyzing the case law of the ECtHR, several interesting and important judgments can be identified.

Balancing between surveillance and national security has already been relevant in earlier case law, notably *Klass and Others v Germany*[38] (1978) where the ECtHR did not find a violation of Article 8 ECHR because the German law restricting the secrecy of mail and telecommunications was, according to the ECtHR, necessary to protect national security and to prevent disorder or crime.[39]

The ECtHR also dealt with several cases relating to secret surveillance during the communist regimes in Eastern Europe and Russia. In *Rotaru v Romania*[40] (2000) and *Association '21 December 1989' and Others v Romania,*[41] (2011) the ECtHR found a violation of Article 8 ECHR due to the Romanian system of secret surveillance. In 1989, Romania faced anti-government demonstrations that were violently suppressed. During those events, the demonstrators were subject to secret surveillance and the information obtained on the basis of this surveillance was still kept many years afterwards. The ECtHR concluded that the Romanian system of keeping information did not contain sufficient safeguards in order to protect the privacy of people taking part in the events in 1989.[42]

A case where the ECtHR found that the fight against terrorism prevails over an individual's right to access the information about him/her in a police database, is the case of

[35] Art. 1(1) of the Directive on Data Protection for Prevention of Criminal Offences (emphasis added).
[36] Art. 13(3).
[37] Art. 15(c) and (d).
[38] ECtHR, *Klass and Others v Germany*, Appl. No. 5029/71, judgment of 6.9.1978.
[39] *Klass and Others v Germany* at para. 60.
[40] ECtHR, *Rotaru v Romania*, Appl. No. 28341/95, judgment of 4.5.2000.
[41] ECtHR, *Association '21 December 1989' and Others v Romania*, Appl. No. 33810/07, judgment of 24.5.2011.
[42] *Association '21 December 1989' and Others v Romania* at para. 175.

Segerstedt-Wiberg and Others v Sweden (2006).[43] In this case, the ECtHR considered that there had indeed been an interference in the applicant's rights under Article 8(1) ECHR,[44] but that the storage of information on the said database had a legitimate aim, that is, the protection of national security.[45] Therefore, with regard to the majority of the applicants, no violation of Article 8 ECHR was found.[46]

The CJEU has equally dealt with the issue of public security in connection with data protection in its early case law. One of the most obvious cases in this regard is the case *Parliament v. Council and Commission*, also known as the *Passenger Name Record* (PNR) case (2006), which led to the annulment of decisions relating to the PNR agreement.[47] Following the grounds for annulment action, brought by the EP, the CJEU annulled the decision on which the PNR agreement was concluded,[48] as well as the adequacy decision on the transfer of PNR to the US.[49] The grounds on which the adequacy decision were annulled was due to the fact that the processing of personal data, transferred on the basis of PNR agreement, did not fall within the scope of the DPD because it constituted 'processing operations concerning public security'.[50] Given that the adequacy decision did not fall within the scope of application of the DPD, the CJEU subsequently annulled it.[51]

Two interconnected trends can be observed from the earlier case law of both European courts. On the one hand, the courts did not lean towards a preference for protecting privacy – which is, as we shall see below, a tendency which can be observed in cases ruled after Snowden's revelations – but instead balanced the two values in a rather neutral manner. This neutral way of balancing allowed the courts to rely heavily on a factual background of the cases, leading to the result that, in the majority of cases, public security still prevailed over privacy. On the other hand, such a security-oriented stance could be explained by the fact that the European courts dealt mostly with the post-WWII type of surveillance which cannot be assimilated to the global extent of the US mass surveillance. In this earlier case law, the courts have therefore not played a role of initiators of social and policy change.

Recent Case law of the European Courts

It is in the context of the gradual awareness of the existence of mass surveillance measures, strengthened by Snowden's revelations, that the European courts, notably the CJEU, increasingly began to tilt the balance towards the protection of privacy rather than security. Legally speaking, this does not mean an absolute preference for privacy since the latter can be limited in accordance with the principle of proportionality. Nevertheless,

[43] ECtHR, *Segerstedt-Wiberg and Others v Sweden*, Appl. No. 62332/00, judgment of 6.6.2006.
[44] At para. 73.
[45] At para. 87.
[46] At para. 92.
[47] *European Parliament v Council and Commission* (C-317/04 and C-318/04) [2006] ECR I-04721, para. 56.
[48] Council Decision 2004/496/EC of 17.5.2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data, OJ L 183/83.
[49] Commission Decision 2004/535/EC of 14.5.2004 on the adequate protection of personal data contained in the PNR of air passengers transferred to the United States Bureau of Customs and Border Protection, OJ L 235/11.
[50] *European Parliament v Council and Commission*, para. 56.
[51] At para. 61.

through the lens of the policy-making of the CJEU, privacy is seen as an overriding value that systematically trumps other competing values.

An exemplary case is *Digital Rights Ireland*[52] (2014), whereby the CJEU annulled the Directive 2006/24/EC on the retention of data.[53] In this case, public security played an important role as a potential ground for justifying the restriction of fundamental rights to privacy and the protection of personal data. The CJEU first established that the Data Retention Directive constituted an interference with those two fundamental rights because the providers of electronic communications services had to retain the personal data of their users for a certain period of time[54] and because the authorities had access to this data.[55] This interference was particularly serious given the fact that the data were retained and used without the user being informed about retention of his/her data.[56] When moving to analyzing the justification of this interference, the CJEU pointed out that the 'objective of that directive is […] to contribute to the fight against serious crime and thus to public security'.[57] The CJEU's final decision was that the interference with the fundamental rights to privacy and data protection was disproportionate, consequently leading to the annulment of the Data Retention Directive.[58]

Digital Rights Ireland is a seminal case where the CJEU acted as a catalyst of policy change by striking a different balance between data protection and public security as the EU legislator. The CJEU reaffirmed its strict stance towards data retention measures in *Tele2 Sverige* (2016) where it found incompatibility of the national data retention measures with the EU privacy legislation.[59] The new data retention legislation is currently still under adoption while the legislator is searching for solutions to satisfy the high standards of data protection required by the CJEU's judgment.

Moreover, the *Schrems*[60] (2015) case also addresses, albeit indirectly, the issue of public security. *Schrems* is the European response to Snowden's revelations and the mass surveillance exercised by the US authorities. Mr. Schrems claimed that his data as a Facebook user were transferred from the European Facebook subsidiary to its headquarters from the US under the US Safe Harbour Privacy Principles, and from there onwards to US authorities under the PRISM programme.[61] He thus challenged the decision issued by the European Commission according to which the Safe Harbour guarantees an adequate level of protection of personal data for the purpose of data transfer from the EU to the US.[62] The CJEU disagreed with the Commission and decided that the Safe Harbour did not offer an adequate level of data protection for European data subjects.[63]

[52] *Digital Rights Ireland and Seitlinger and Others* (C-293/12 and C-594/12) EU:C:2014:238.
[53] Directive 2006/24/EC of the Parliament and Council of 15.3.2006 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] L 105/54.
[54] *Digital Rights Ireland* (C-293/12 and C-594/12), para. 34.
[55] At para. 35.
[56] At para. 37.
[57] At para. 41.
[58] At paras 46–71.
[59] *Tele2 Sverige AB* (C-203/15 and C-698/15) EU:C:2016:970.
[60] *Schrems* (C-362/14) EU:C:2015:650.
[61] At paras 24–27.
[62] Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215/7.
[63] *Schrems*, para. 98.

The reason for that was that the US authorities had access to data transferred to US businesses and processed data of European subjects in a way that was disproportionate to the objectives pursued by the protection of national security.[64] Even though the EU–US discussions on review of Safe Harbour were already underway prior to Snowden's revelations and prior to the *Schrems* case, the latter gave a clear and urgent message regarding the need for a policy reform of that instrument. In the aftermath of the *Schrems* case, the new Privacy Shield was adopted that is supposed to remedy the shortcomings of Safe Harbour, containing assurances that the data of European citizens will only be transferred to the US authorities if the fundamental rights of those citizens are adequately protected.[65]

Finally, the most important case from the perspective of current issues of post-Snowden surveillance is the pending ECtHR case *Big Brother Watch and Others v. the United Kingdom*.[66] In this case, several UK-based NGOs and a German academic are claiming that they are subject to secret surveillance by the UK authorities. The case has been communicated to the UK government and is currently pending. Once decided, this case could either establish a new balance between privacy and security or further deepen the importance of privacy in Europe.

From the case law analyzed above it can be seen that the CJEU puts privacy on a glorious pedestal where it seems to have, relatively speaking, more weight than other potentially overriding reasons, including public security. It is argued that the protection of privacy and personal data in Europe has been significantly strengthened through the intervention of European courts which played a role as the 'entrepreneurs' of policy reforms. Given the strong role of the courts in Europe and their policy impact, it can even be questioned whether the European courts are overstepping their powers as seen from the traditional Montesquieu's perspective of *trias politica*. Anyhow, the increasing privacy threats, the existence of which were revealed *inter alia* through Snowden's revelations, are taken very seriously by the European courts. From a policy perspective, these courts are beginning to play a global role in which they push the European policy-makers towards ever-higher standards of data privacy and thereby create an even bigger divide with the US courts' approach to this field of law.

Conclusion

The classical 'national security v. civil liberties' debate was brought back to life by Snowden's disclosures and the resulting broader awareness of the global mass surveillance measures.

The originality of this article resides in the circumstance that it studies this question from the standpoint of the two main actors striking the balance between national security and privacy, namely policy-makers and courts. By adopting a comparative approach that allows us to highlight the main discrepancies between the EU and US approaches to privacy and data protection, as well as to see the interaction between courts and policy-

[64] At para. 90.
[65] For the Commission adequacy decision, see Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
[66] ECtHR, *Big Brother Watch and Others v the United Kingdom*, Appl. No. 58170/13 (pending).

makers, we test here a twofold hypothesis. On the one hand, the analysis asks whether the unparalleled number of policy-makers' reforms implemented on both sides of the Atlantic have reached a sufficient level of adequacy of data protection despite the fundamental differences between the two legal systems. On the other hand, by examining the earlier and more recent EU and US case law relating to this balancing, the analysis asks to what extent the courts have been acting as agents of reform, all while continuing to diverge in their approaches to balancing national security and data protection.

On the threshold question, this article concludes in line with numerous legal studies that the EU and US approaches to privacy and data protection contain notable differences, especially when it comes to law enforcement. Despite recent reforms and agreements concluded between the EU and the US, US surveillance law still has numerous loopholes that allow US intelligence agencies to possess double standards on regulations regarding domestic and foreign surveillance.

By way of contrast, personal data processing in the EU is strictly forbidden and rests upon a high level of protection of fundamental rights to privacy and data protection. The absence of the fundamental rights status of privacy and data protection in the US legal system explains, to a large extent, the fact that balancing national security and data protection in the US continues to be done in favour of national security, while data protection and privacy are clearly given priority in the EU. The latter is demonstrated by the dynamics between the European policy-makers and the European courts' approach in which the courts have paved the way for a particularly high level of data privacy protection. Such a judicial approach is subsequently followed by the European policy-makers which, in turn, have an influence on the stance of the US policy-makers in the field of transatlantic data transfers. However, while the policy-makers on both sides of the Atlantic attempt to reach adequacy of data protection, from the courts' perspective there is still a deep Atlantic ocean between their perception and shaping of the societal importance of privacy and data protection.

Correspondence:
Anna Dimitrova
International Studies and Business Department
ESSCA School of Management
55 quai Alphonse Le Gallo
92513 Boulogne-Billancourt
France
email: anna.dimitrova@essca.fr

References

Amtenbrink, F. (2013) 'Legal Developments'. *JCMS*, Vol. 51, No. s1, pp. 139–54.
Atkinson, L.R. (2013) 'The Fourth Amendment's National Security Exception: Its History and Limits'. *Vanderbilt Law Review*, Vol. 66, No. 5, pp. 1343–405.
Bauman, Z. *et al*. (2014) 'After Snowden: Rethinking the Impact of Surveillance'. *International Political Sociology*, Vol. 8, No. 2, pp. 121–44.
Bignami, F. (2007) 'European versus American Liberty: A Comparative Analysis of Antiterrorism Data Mining'. *Boston College Law Review*, Vol. 48, No. 3, pp. 609–98.

Bignami, F. (2015) 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens'. Study for the LIBE Committee, European Parliament, PE 519.215, pp. 1–40.
Boehm *et al*. (2015) 'A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes'. Study for the LIBE Committee, European Parliament, PE 536.459, pp. 1–77.
Bowden, C. and Bigo, D. (2013) 'The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights', European Parliament, PE 474.405, pp. 1–37.
Brkan, M. (2016) 'The Unstoppable Expansion of EU Fundamental Right to Data Protection: Little Shop of Horrors?' *Maastricht Journal of European and Comparative Law*, Vol. 23, No. 5, pp. 812–41.
Cadiot, S., Hoffman, S.G. and De Boel, L. (2016) 'Article 29 Working Party Calls for Improvements to the EU-U.S. Privacy Shield', WSGR Alert, 13 April 2016. Available online at: https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-WP29.htm.
Davis, R. (2003) 'Striking the Balance: National Security vs. Civil Liberties'. *Brooklyn Journal of International Law*, Vol. 29, No. 1, pp. 175–238.
Donohue, L. (2014) 'Bulk Metadata Collection: Statutory and Constitutional Considerations'. *Harvard Journal of Law and Public Policy*, Vol. 37, No. 3, pp. 759–900.
Doyle, Ch. (2001) 'Terrorism: Section by Section Analysis of the USA Patriot Act'. CRS Report for Congress, 10 December.
Farrell, H. and Newman, A. (2013) 'Senseless Spying'. *Foreign Affairs*, 9 July. Available online at: https://www.foreignaffairs.com/articles/europe/2013-07-09/senseless-spying.
Farrell, H. and Newman, A. (2016) 'The Transatlantic Data War'. *Foreign Affairs*, January/February, Vol. 95, No. 1, pp. 124–33.
Fowler, S. (2014) 'Circumventing the Constitution for National Security: An Analysis of the Evolution of the Foreign Intelligence Exception to the Fourth Amendment's Warrant Requirement'. *University of Miami National Security & Armed Conflict Law Review*, Vol. 4, No. 1, pp. 207–40.
Goitein, E. and Patel, F. (2015) 'What Went Wrong with the FISA Court?' Brennan Center for Justice, 18 March, pp. 1–53.
Greer, S. (1997) *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights* (Strasbourg: Council of Europe Publishing).
Harvard Law Review (2014) 'Search and Seizure. Searching Cell Phones Incident to Arrest'. *Riley v California*, Vol. 128, No. 1, pp. 251–61.
Hasbrouck, E. (2016) 'The Limits of the US Judicial Redress Act'. *Privacy Laws and Business*, Vol. , No. 114, April, pp. 21–3.
Horsley, T. (2015) '"The Court Hereby Rules ..." – Legal Developments in EU Fundamental Rights Protection'. *JCMS*, Vol. 53, Annual Review, pp. 108–27.
Jančić, D. (2016) 'The Role of the European Parliament and the US Congress in Shaping Transatlantic relations: TTIP, NSA Surveillance, and CIA Renditions'. *JCMS*, Vol. 54, No. 4, pp. 896–912.
Kuner, C. (2017) 'Reality and Illusion in EU Data Transfer Regulation Post Schrems'. *German Law Journal*, Vol. 18, No. 4, pp. 881–918.
Lamparello, A. and MacLean, C. (2014) 'Riley v. California: Privacy Still Matters, but How Much and in What Contexts?' *Regent University Law Review*, Vol. 27, No. 1, pp. 25–41.
Larkin, P. (2013) 'The Fourth Amendment and New Technologies'. *The Heritage Foundation, Legal Memorandum*, Vol. , No. 102, pp. 1–9.

Lynskey, O. (2014) 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order'. *International and Comparative Law Quarterly*, Vol. 63, No. 3, pp. 569–97.
Mattli, W. and Woods, N. (2009) *The Politics of Global Regulation* (Princeton, NJ: Princeton University Press).
Miller, R. (2017) 'Introduction: Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair'. In Miller, R. (ed.) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge: Cambridge University Press), 1–37.
Newman, A. (2011) 'Transatlantic Flight Fights: Multi-level Governance, Actor Entrepreneurship and International Anti-terrorism Cooperation'. *Review of International Political Economy*, Vol. 18, No. 4, pp. 481–505.
Pleschinger, S. (2006) 'Allied against Terror: Transatlantic Intelligence Cooperation'. *Yale Journal of International Affairs*, Vol. 2, No. 1, pp. 55–67.
Richards, N. (2013) 'The Dangers of Surveillance'. *Harvard Law Review*, Vol. 126, No. 7, pp. 1934–65.
Schwartz, P. (2013) 'The EU-US Privacy Collision: A Turn to Institutions and Procedures'. *Harvard Law Review*, Vol. 126, No. 7, pp. 1966–2009.
Schwartz, P. and Solove, D. (2014) 'Reconciling Personal Information in the United States and European Union'. *California Law Review*, Vol. 102, No. 4, pp. 877–916.
Schwartz, P. and Solove, D. (2011) 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information'. *New York University Law Review*, Vol. 86, No. 6, pp. 1814–94.
Solove, D. (2002) 'Conceptualizing Privacy'. *California Law Review*, Vol. 90, No. 4, pp. 1088–155.
Solove, D. and Schwartz, P. (2009) *Information Privacy Law* (3rd edition) (Wolter Kluwer Law & Business: Aspen Publishers).
Suda, Y. (2013) 'Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism'. *JCMS*, Vol. 51, No. 4, pp. 772–88.
Swire, P. (2015a) 'US Surveillance Law, Safe Harbor, and Reforms since 2013'. White Paper submitted to the Belgium Privacy Authority, December 17, pp. 1–43.
Swire, P. (2015b) 'The USA Freedom Act: A Partial Response to European Concerns about the NSA Surveillance'. GTJMCE Working Paper, No. 1.
Tourkochoriti, I. (2014) 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between US-EU Data Privacy Protection'. *University of Arkansas at Little Rock Law Review*, Vol. 36, No. 2, pp. 161–76.
Tzanou, M. (2015) 'The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy and Spillovers of Security?' *Utrecht Journal of International and European Law*, Vol. 31, No. 80, pp. 87–103.
Weiss, M. and Archick, K. (2016) 'U.S.-EU Data privacy: From Safe Harbor to Privacy Shield'. CRS Report No. R44257.
Whitman, J.Q. (2004) 'The Two Western Cultures of Privacy: Dignity Versus Liberty'. *The Yale Law Journal*, Vol. 113, pp. 1151–221.