BRILL
NIJHOFF

TILBURG LAW REVIEW 20 (2015) 5-13

Tilburg
Law Review
brill.com/tilr

# Introduction

# Privacy and National Security in the Digital Age

## *European and Comparative Constitutional Perspectives*

*Federico Fabbrini*
Assistant Professor of European & Comparative Constitutional Law, Tilburg Law School and Coordinator of the Research Group on "Constitutional Responses to Terrorism", International Association of Constitutional Law
*federico.fabbrini@gmail.com*

**Abstract**

The article introduces the theme of the protection of the right to privacy in a world characterized by rapid developments in digital technology and the need to fight terrorism. It identifies the challenges that surveillance policies raise on privacy and data protection and explains how the contributions to the Special Issue connect to the ongoing legal and policy debate in the field of European and comparative constitutional law.

**Keywords**

privacy – surveillance – constitutional law – European – comparative

Technological developments and the revolution in communication that generally go under the name of globalization have profoundly changed the world we live in. IT technology and the digital frontier, in particular, have fundamentally transformed the nature of inter-personal interactions. The internet connected with each other communities from all corners of the planet. Social networks allow every individual to share information across the globe in matters of seconds. And the cloud provides a virtual repository in which everyone can store at cheap or no price an invaluable set of personal or professional data. Yet, besides affecting trade and international relations, these transformations have also produced an unprecedented impact on human rights. On the one hand,

 | DOI 10.1163/22112596-02001004

innovation in communication technology has created new opportunities for the protection of fundamental rights and liberties, amplifying the voices of human rights activists and providing them with new tools to document abuses and to promote their cause. As the experience of the outburst of the Arab Spring has shown, smartphones and social networks have improved global access to information, boosted freedom of expression, and promoted civic engagement. However, on the other hand, the digital revolution has also created new challenges for the protection of human rights. The web has served as a fertile terrain in which terrorist networks such as Al Qaida have bred, made proselytism and plotted destruction of life and property. At the same time, communication technologies have also enhanced the capacity of governments, and private companies, to monitor individuals and collect data about their behavior.

In the context of terrorism and counter-terrorism, in particular, developments in telecommunications and the rise of digital technology have triggered an unprecedented challenge to the protection of privacy and personal data.[1] Since 9/11 public authorities have significantly expanded their surveillance powers with the aim to protect national security, and disrupt potential terrorist threats.[2] Either by directly taking on the surveillance task (e.g. by empowering intelligence or law enforcement agencies to monitor and intercept electronic communications)[3] or by delegating the surveillance function to the private sector (e.g. by requiring internet service providers and telephone companies to retain meta-data about electronic communications for a number of years and make them available to the police or the secret services if needed)[4] national governments and supranational organizations have dramatically increased their capacity to locate individuals, intercept their communications and target

1 Report of the United Nations High Commissioner for Human Rights on The Right to Privacy in the Digital Age, 30 June 2014, A/HRC/27/37, para 1 (emphasizing potentials, as well as risks, for human rights in the developments of digital technology).

2 See further F Fabbrini, 'Human Rights in the Digital Age. The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) 28 Harvard Human Rights Journal.

3 See eg Sec 215 USA Patriot Act, P.L. 113–99 (2001), currently codified as 50 U.S.C. § 1861 (regulating access to business record for foreign intelligence and international terrorism investigations).

4 See eg Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ 2006 L105/54, Art. 3 (requiring telecommunication service providers to retain meta data about electronic communications for up to 2 years).

them.[5] However, despite the legitimate concerns about national security, and the duty of states and supranational institutions to provide to their citizens security against terrorist threats, the creation of this pervasive regime of surveillance has raised widespread concerns about the protection of the rights to privacy and personal data.[6]

The right to privacy and to the protection of personal data are well entrenched both in national constitutions and in international human rights treaties.[7] In fact, as it has been recently suggested, in a departure from conventional patterns, the right to privacy was first recognized by international human rights instruments before being explicitly enshrined in national basic laws[8] – witness Article 12 of the Universal Declaration of Human Rights of 1948,[9] Article 8 of the European Convention on Human Rights of 1950,[10] and Article 17 of the International Covenant on Civil and Political Rights of 1966.[11] Whereas in jurisdictions with older constitutions the recognition of a right to privacy has been the result of the case law of national supreme or constitutional courts – as evidenced by the rulings of the Supreme Court of the United States (US),[12] discovering a right to privacy in the US Constitution IV Amendment's prohibition of unreasonable searches and seizures[13] – privacy and the protection of personal data feature prominently in the charter of rights adopted between the end of the 20th century and the beginning of the 21st.[14] Notably, in the context of the European Union (EU), Articles 7 and 8 of the Charter of Fundamental

5 See also *Uzun v. Germany* App no 35623/05 ECtHR, 2 September 2010 (rejecting a challenge against the GPS tracking of a suspected terrorist in light of privacy rules); *Big Brother Watch and others v. United Kingdom* App no 58170/13 ECtHR, pending (considering a challenge against dragnet surveillance in light of privacy rules).

6 See D Cole, 'Can Privacy Be Saved?' *The New York Review of Books*, 6 March 2014 <http://www.nybooks.com/articles/archives/2014/mar/06/can-privacy-be-saved/> accessed 11 September 2014.

7 See LA Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014).

8 See O Diggelman and MN Cleis, 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review 441 (stressing that the right to privacy found recognition in international treaties before being enshrined in national constitutions and case law).

9 UNGA Res 217A (III) (1948) U.N. Doc A/810, 71.

10 1950 ETS 5.

11 999 UNTS 171.

12 See *Katz v United States* 389 US 347 (1967) (holding that the US Constitution Fourth Amendment protects a person's reasonable expectation of privacy).

13 But see S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193 (discussing already the possibility to recognize a right to privacy in the US).

14 See S Gutwirth and others (eds) *Reinventing Data Protection* (Springer 2009).

Rights adopted in 2000 and binding since 2009,[15] enshrine both a right to respect for private and family life, and a right to the protection of personal data concerning him or her.[16] Although legal scholars debate whether privacy finds its roots in conceptions of either liberty, or dignity,[17] transnational consensus exist on the idea that privacy, at a minimum, must protect a sphere of intimate relationship against interference by public authorities.[18]

Yet, as the recent revelations of systematic practices of dragnet surveillance of phone call, e-mails and text messages by governments in the US and some EU member states have made clear, the protection of the right to privacy has been put under significant pressure in the name of fighting terrorism. National security restrictions on the right to privacy, at the same time, have been aggravated by a number of factors. To begin with, many surveillance programs have been designed and carried out in secret, behind closed doors, and without the possibility of adequate scrutiny:[19] in fact, it is often only through the action by whistleblowers or the like that the public has come to know about the breath of the surveillance programs designed since 9/11. Moreover, because of the border-less nature of contemporary digital communications, with data instantly travelling across IT servers located throughout the world, surveillance programs have empowered national security agencies to spy on individuals' action on a global scale.[20] Issues of extraterritoriality to the side, states have developed pervasive surveillance abilities abroad. Finally, as a result of growing cooperation between intelligence and law enforcement agencies at the regional and international level, information collected through surveillance programs has increasingly been the object of data sharing.[21] Combined

15 OJ 2007 C303/17.

16 On the protection of fundamental rights in the EU see generally F Fabbrini, *Fundamental Rights in Europe* (OUP 2014).

17 See J Whitman, 'The Two Western Culture of Privacy: Dignity Versus Liberty' (2004) 113 Yale Law Journal 1151 (emphasizing that historically the foundation of privacy in the US is liberty while in the EU it is dignity).

18 See also Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedom while Countering Terrorism on The Protection of the Right to Privacy in the Fight Against Terrorism, 28 December 2009, A/HRC/13/37.

19 See generally D Cole, F Fabbrini and A Vedaschi (eds) *Secrecy, National Security and the Vindication of Constitutional Law* (Elgar Publishing 2014) (discussing increasing use of secrecy claims in the fight against terrorism).

20 See generally F David, N McGarrity and G Williams (eds) *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge 2014) (emphasizing global nature of surveillance).

21 See generally KL Scheppele, 'Global Security Law and the Challenge to Constitutionalism After 9/11' (2011) Public Law 353 (discussing trans-national intelligence cooperation).

with the different degree of privacy protections that most legal systems accord to citizens and foreigners,[22] the reality of transnational cooperation has de facto allowed governments to circumvent constitutional safeguards on the privacy of citizens, by resorting to the support of foreign authorities to undertake unlawful surveillance on their own nationals.

The latest disclosure of massive programs of government surveillance and the growing awareness of the deleterious impact of these measures on the right to privacy have sparked a global conversation about the balance between liberty and security in the digital era.[23] Under the sponsorship of Brazil and Germany, the United Nations General Assembly has adopted an anti-spy resolution in December 2013.[24] In the US, during the last months all branches of government have been involved in re-considering the legality, effectiveness and morality of data mining and data collection by national security agencies: a lower federal court declared the US spying program likely in violation of the US Constitution,[25] Congress took steps to reform the relevant legislation,[26] and even the executive branch advanced proposals to curb overreaching by the intelligence agencies.[27] In the EU, otherwise, action in the political process and the courts has responded to growing popular concerns and signaled a potential turn in the EU approach to counter-terrorism and human rights: after the EU Parliament voted in March 2014 a resolution harshly criticizing the US surveillance program and the EU member states' support to it,[28] in April 2014 the

22 See generally D Cole, *Enemy Aliens* (The New Press 2003) (emphasizing different treatment of citizens and foreigners in the struggle against terrorism).

23 See also US President B Obama's speech on 17 January 2014 <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> accessed 12 September 2014 (welcoming a debate on surveillance policies and their impact on privacy).

24 See UNGA Res 167, 18 December 2013, A/Res/68/167.

25 See *Klayman v Obama*, 2013 US Dist LEXIS 176925 (D.D.C. 16 December 2013) (ruling the telephone metadata program likely unconstitutional). But see *ACLU v Clapper*, 2013 US Dist LEXIS 180863 (S.D.N.Y. 27 December 2013) (reaching opposite conclusion).

26 See USA Freedom Act, HR 3361/ S 1599 (purporting to end national security agencies dragnet collection of meta-data about electronic communications).

27 See President's Review Group on Intelligence and Communication Technologies, 'Liberty and Security in a Changing World: Report and Recommendations' (12 December 2013) <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 12 September 2014.

28 European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, P7_TA(2014) 0230 (calling US authorities to prohibit blanket mass surveillance activities and bulk

EU Court of Justice (ECJ) in *Digital Rights Ireland*[29] struck down the EU Data Retention Directive,[30] strengthening the arguments in favor of an overhaul of the EU data protection regime, as planned also by the EU Commission in its proposal for a new General Data Protection Regulation.[31] Yet the transnational public conversation is still ongoing and many pressing challenges remain on how to reconcile privacy and security in the digital age.[32]

This Special Issue – which collects papers originally presented at a panel on "National Security, Data Sharing and Data Protection", organized by the Research Group on Constitutional Responses to Terrorism within the International Association of Constitutional Law and hosted at Harvard Law School in March 2014 – brings together a number of contributions on the pressing constitutional questions raised by the protection on privacy in the struggle against terrorism. The articles – which are written by scholars of EU law, public law and comparative law – are characterized by several common traits, which make this Special Issue a relevant contribution to the field of European and comparative constitutional law. To begin with, all articles embrace a *comparative*, *trans-national* perspective, exploring how surveillance has posed challenges to privacy *across borders*: in some articles, the comparison unfolds within the EU, by contrasting legislation and courts' cases in the jurisdiction of several EU member states; in other articles, however, the comparison is brought beyond the EU, by looking at how the EU regime of data protection and data sharing fares in light of comparable laws in the US, Australia, as well as in the Association of South East Asian Nations (ASEAN). Moreover, all articles reflect a *global*, *multi-layered* mindset, which is attentive to the interaction between human rights rules and national security imperatives *across levels* of government: hence, all articles emphasize the complex interplay between domestic,

processing of personal data and threatening to veto EU-US transatlantic trade deals unless the program was discontinued).

29 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*, judgment of 8 April 2014, nyr.

30 See (n 4).

31 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data' COM (2012) 11 final.

32 On how technological developments unrelated to national security challenge the right to privacy see instead BJ Koops and R Leenes, 'Code and the slow erosion of privacy' (2005) 12 Michigan Telecommunication & Technology Law Review 115, as well as now Case C-131/12 *Google Spain SL v. Agencia Española de Protección de Datos*, judgment of 13 May 2014, nyr (holding that search engines are processor of personal data subject to EU law and may be required to remove on-line content).

supranational, and international law, and some of them also consider the principles and best practices which are slowly emerging on a global scale.

The Special Issue is opened by the article of Arianna Vedaschi and Valerio Lubello on "Data Retention and its Implications for the Fundamental Right to Privacy." The piece by Vedaschi and Lubello sets the context, by examining the EU regime for the protection of privacy and personal data and its evolution in light of EU anti-terrorism laws adopted since 9/11. In particular, Vedaschi and Lubello focus on the Data Retention Directive – a piece of legislation enacted by the EU in 2006, which required IT companies to retain all the meta-data about telephone and internet communications for future law enforcement purposes – and discuss the recent milestone decision by the ECJ in *Digital Rights Ireland*, striking down the Data Retention Directive as in violation of the right to privacy and data protection enshrined in the EU Charter of Fundamental Rights. As Vedaschi and Lubello explain, the Data Retention Directive constituted a major interference with the right to privacy, and in fact had raised widespread legal challenges before member states' constitutional and supreme courts during its implementation phase. According to the two authors, therefore, the judgment of the ECJ should be seen as a welcome step by the EU supreme judicial authority to limit the surveillance policies devised by the EU political branches; and the precedent of the ECJ should serve as a benchmark to rein into anti-terrorism laws also at the domestic level, to restore a proper balance between human rights and national security.

The second article, by Valsamis Mitsilegas, broadens the examination conducted in Vedaschi and Lubello's piece by considering "The Transformation of Privacy in an Era of Pre-Emptive Surveillance". Mitsilegas, in particular, focuses on the transatlantic cooperation in the field of national security and seeks to emphasize the influence of the US anti-terrorism policy on the laws and practices of the EU. To make his point, Mitsilegas examines the Passenger Name Record (PNR) agreement and the Terrorist Financing Tracking Program (TFTP) concluded between the EU and the US. Under the PNR, EU institutions required EU air carriers to comply with demands by US law enforcement agencies to provide the name records of passengers flying on EU planes directed to the US. Pursuant to the TFTP, instead, US law enforcement agencies were authorized to access data on bank transactions occurred in the EU internal market with the aim to prevent the possible financing of terrorism. As Mitsilegas argues, the conclusion of both the PNR agreement and the TFTP was strongly influenced by the willingness of the EU institutions to cooperate with the US anti-terrorism efforts – yet they contributed to the development of a culture of pre-emptive surveillance also in the EU. Mitsilegas evaluates the implications of this development on the right to privacy and attempts to trace a way forward

to enhance the protection of personal data. Whereas the initial conclusion and subsequent renegotiation of these transatlantic deals has faced rising opposition from the EU Parliament (which has seen its role expanded since the entry into force of the Lisbon Treaty), Mitsilegas places particular faith in the capacity of the ECJ (notably after its decision in *Digital Rights Ireland*) to revert the securitization trend unleashed by terrorist attacks in the US and the EU and to protect adequately the right to privacy.

Whereas Mitsilegas' piece deals with the relationship between the EU and the US, the third article of the Special Issue – Celine Cocq's "Developments of Regional Legal Framework for Intelligence and Information Sharing in the EU and ASEAN" – expands the analysis in a direction which has so far received only limited exploration in scholarship: namely a comparison between the EU and ASEAN. As Cocq explains, during the last decade the framework for intelligence and information sharing among the 10 nations of South-East Asia which are part of ASEAN has significantly developed. Certainly – as her article underlines – ASEAN, as a regional organization, does not yet meet the degree of integration featured by the EU. In the EU, member states have started cooperation in the area of criminal law and counter-terrorism more than three decades ago, and, despite persisting jalousies between several member states, the degree of trust among them is far greater than that currently visible in the ASEAN. As a result, by now a rich set of laws and regulations on intelligence sharing is in place in the EU, whereas a transnational legal regime is still only in its infancy in ASEAN. Nevertheless, Cocq emphasizes a clear trend toward growing transnational cooperation also in ASEAN, along the EU model. Yet – as she notices – growing intelligence and information sharing also poses growing challenges to privacy and data protection. To address this state of affairs, therefore, Cocq concludes by making the case for strengthening the protection of personal data at the regional level: if regional integration creates a functional demand for more inter-states' cooperation in the intelligence domain, then also human rights protections must be pushed upwards to secure their enduring effectiveness.

The article by Konrad Lachmayer concludes the Special Issue by taking the debate about privacy and surveillance from the regional to the global scale. In his piece, "Rethinking Privacy Beyond Borders: Developing Transnational Rights on Data Privacy", Lachmayer examines the challenges of protecting privacy and personal data in an era in which technology and trans-national communications render data easily available instantly everywhere in the world and makes the case in favor of a new, far-reaching legal framework at the international level to protect privacy. Lachmayer begins his analysis by considering the tension between the EU data protection regime and the growing role that

EU laws and policies adopted in the area of criminal justice and police cooperation play in restricting privacy rights. He then compares the EU regime with that of the US and Australia and claims that the EU offers in comparative terms a more protective constitutional framework to safeguard data privacy, as opposed to the US (which has an older Constitution) and Australia (which lacks a legally binding Bill of Rights). Finally, he surveys recent developments occurring at the international level, but suggests that these are not enough, and that further steps must be taken to entrench at the global level a privacy Bill of Rights. Whereas Lachmayer's discussion on the EU data protection regime connects with the analysis by Vedaschi and Lubello and Mitsilegas, his proposal to level up the legal mechanisms to secure privacy calls to mind the arguments by Cocq and her idea that power and constraints should go hand in hand.

In the end, all contributions to this Special Issue plead in favor of updating privacy protections to face new technological developments. Yet, how to achieve this result remains an open question: should we strengthen constitutional rules and resistance norms in the EU, as Vedaschi and Lubello, and Mitsilegas suggest, or develop new global privacy standards, as advocated by Lachmayer, or – as an intermediate solution – purse an EU-US agreement creating a transatlantic compact for privacy protection, as David Cole and I argue elsewhere?[33] Needless to say, none of these alternative proposals appears easy to put in practice. However, the need for a serious debate about how to reconcile privacy and surveillance in the digital age seems to be ever more compelling. By collecting four timely analyses on the challenges of how to simultaneously protect human rights and national security this Special Issue seeks to contribute to this important debate from a European and comparative constitutional perspective.

33 D Cole and F Fabbrini, 'Bridging the Transatlantic Divide? The European Union, the United States and the Protection of Privacy Across Borders' in F Fabbrini and V Jackson (eds) *Constitutionalism Across Borders in the Struggle Against Terrorism* (Elgar Publishing 2016, forthcoming).