TRANS-ATLANTIC DATA PRIVACY RELATIONS AS A CHALLENGE FOR DEMOCRACY

TRANS-ATLANTIC DATA PRIVACY RELATIONS AS A CHALLENGE FOR DEMOCRACY

Edited by
Dan Jerker B. Svantesson
Dariusz Kloza

intersentia
Cambridge – Antwerp – Portland

Intersentia Ltd
Sheraton House | Castle Park
Cambridge | CB3 0AX | United Kingdom
Tel.: +44 1223 370 170 | Fax: +44 1223 370 169
Email: mail@intersentia.co.uk
www.intersentia.com | www.intersentia.co.uk

Distribution for the UK and Ireland:
NBN International
Airport Business Centre, 10 Thornbury Road
Plymouth, PL6 7 PP
United Kingdom
Tel.: +44 1752 202 301 | Fax: +44 1752 202 331
Email: orders@nbninternational.com

Distribution for Europe and all other countries:
Intersentia Publishing nv
Groenstraat 31
2640 Mortsel
Belgium
Tel.: +32 3 680 15 50 | Fax: +32 3 658 71 21
Email: mail@intersentia.be

Distribution for the USA and Canada:
International Specialized Book Services
920 NE 58th Ave. Suite 300
Portland, OR 97213
USA
Tel.: +1 800 944 6190 (toll free) | Fax: +1 503 280 8832
Email: info@isbs.com

Trans-Atlantic Data Privacy Relations as a Challenge for Democracy

ISBN 978-1-78068-434-5
D/2017/7849/17
NUR 828

British Library Cataloguing in Publication Data. A catalogue record for this book is available from the British Library.

FOREWORD

On the Path to Globally Interoperable Schemes of Data Protection Law

Wojciech Rafał Wiewiórowski*

The dawn of the second decade of the twenty-first century has forced lawyers to rethink some widely used yet basic concepts in order to extract the fundamental rights principles from the flood of European legislation generated since the European Union really begun its operation in 1993. At the same time, legislators have been bombarded with the question of legitimacy of some European legal concepts in the new century. For instance, while the whole concept of personal data seems to be solid enough to survive even strongest attacks, some particular elements of the legal heritage of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, are still being strongly questioned.

Among many trans-Atlantic data privacy aspects, this book examines the many questions concerning the classic concept of restrictions of personal data transfers beyond the area considered, from a European viewpoint, as safe. This concept is illustrative to the whole spectrum of trans-Atlantic relations and I would like to offer a few remarks on this matter. It is furthermore essential, on the road to global interoperable schemes of personal data protection, to answer questions of international transfers and their influence on international trade, big data processing and new roads to cybercrime.

Under the Lisbon Treaties, which have been in force since 2009, the European Union regards itself as a distinct political entity, not a federation of Member States, held together – as Luuk van Middelaar says – with a 'unique, invisible glue'. This connection is grounded with shared goals. One of them – expressed both in the Treaty on the Functioning of the European Union (Art. 16) and in the Charter of Fundamental Rights of the European Union (Arts. 7 and 8) – is a unique obligation to protect personal data. Stating that everyone has the right

* Assistant European Data Protection Supervisor; University of Gdansk. E-mail: wojciech.wiewiorowski@edps.europa.eu.

to the protection of personal data concerning them, the European Union feels obliged to observe how safe is the data both held in its territory and transferred outside thereof.

Having implemented this rule in Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), the European legislator admits that rapid technological development and globalisation have brought new challenges for the protection of personal data. The legislator further recognises that the technology allows for both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities and that this phenomenon has transformed both the economy and social life. But, bearing all this in mind, the Regulation – also by its very title – confirms that the European Union should further facilitate the free flow of personal data within its territory and the transfer thereof to third countries and international organisations, while ensuring a high level of the protection of personal data.

Recital 101 of the Regulation clearly states that flows of personal data to and from countries outside the European Union and international organisations are necessary for the expansion of free trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. Although the level of protection of natural persons ensured in the European Union should not be undermined when personal data are transferred to controllers, processors or other recipients in third countries, the possibility of transfer is obvious. Such transfers could take place only if the controller or processor complies with the conditions laid down in European law.

Nevertheless, many sceptics ask whether the notion of the whole concept of international transfer of personal data is still legitimate? Whether a national border is still significant in the time of big data?

Data is often regarded as a commodity, such as crude oil, which can be traded between two equally aware parties to the transaction. It is of course not a commodity and it is not an anonymous resource belonging to the entity that pays more. Moreover, in the age of big data, large-scale resources of data are significant not because they are 'large' but because it is easy to transfer them and merge with other accessible datasets. The transfer starts to be the driver itself. It causes additional problems with the purpose of processing since the purpose the personal data was collected for is not necessarily the one for which it is processed after the transfer. The sustainability of such processing vanishes and the transfer starts to be the goal in itself, as it multiplies the possibility to achieve new purposes.

The term 'transfer of personal data' has not been defined, neither in the Directive in 1995 nor in the Regulation in 2016. It can be assumed, as a starting point, that the term is used in its natural meaning, i.e. that data 'move' or are

allowed to 'move' between different users. However, in reality, this issue is not always so straightforward. The European Data Protection Supervisor has called for a definition of this notion in the data protection reform, as it has proved to be a problematic issue in certain cases, which so far have been left for the Court of Justice of the European Union or for the legislator to resolve.

A group of leading scholars and practitioners examines in this book how transborder data flows regime – either having its roots in General Data Protection Regulation or driven by separate instruments such as EU–US Privacy Shield – influences the everyday basis of data processing on both sides of the Atlantic and how it limits the scope of operations on data. The impact of the judgment of the Court of Justice of the European Union in the so-called *Schrems* case on other transborder data flows regime instruments is taken into consideration to examine what are the internal and global implications of trans-Atlantic information exchange.

Additional importance is given to the studies on the scope of processing which may be excluded from general rules on the basis of public security, defence, national security or criminal law exceptions. Bearing in mind that the Article 29 Working Party has expressed its wish to keep the exchange regime compliant with four essential guarantees to be used whenever personal data are transferred from the European Union to a third country – not only the United States. According to these principles, any processing of such data should be subject to clear, precise and accessible rules known for data subjects. The necessity and proportionality with regard to legitimate objectives have to be pursued and the independent oversight mechanisms has to be put in place. A legal system has to contain effective remedies to be possible to use by data subject.

This creates a mechanism of transborder data flows which may be based on the decision on adequacy issued by the European Commission towards a third country system. It may equally be based on model contact clauses with no prior authorisation, which are drafted by data protection authorities, proposed to the European Commission and adopted by the Commission or, alternatively, drafted by the Commission itself. Binding corporate rules (BCR) – in the new European legal framework – will no longer need national validation after being passed by the European Data Protection Board. Finally, transfers can by authorised by data protection authorities on an *ad hoc* decision.

In its position paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies from 2014, the European Data Protection Supervisor stated that the principle of adequate protection requires that the fundamental right to data protection is guaranteed even when personal data are transferred to a party outside the scope of the Directive. Although there is a growing consistency and convergence of data protection principles and practices around the world, we are far from full adequacy and full respect for EU fundamental rights cannot be assumed in

all cases. It will often happen that the level of data protection offered by third countries or international organisations is much lower than that of the European Union, or – worse – does not exist at all. The checklist to be used by controllers before carrying out a transfer and set in Annex 2 to Supervisor's position paper is still valid. But because it needs some revision according not only to the text of the new General Data Protection Regulation but also according to the practice of international cooperation – where the EU–US Privacy Shield is the best example – I recognise this book to be a step towards explanation of new rules, but also a list of questions to be considered both by legislators, supervisors, regulators and controllers as well as by entities representing them.

Brussels, September 2016

PREFACE

Yet Another Book about Snowden and Safe Harbor?

Dan Jerker B. Svantesson* and Dariusz Kloza**

I.

A series of events have led to the idea for this book and the first one is more than obvious: the Edward Snowden *affaire*.[1] On 6 June 2013 Glenn Greenwald published in *The Guardian* the first in a series of articles – and later co-authored a few other – on global mass surveillance practices led by the United States' National Security Agency (NSA).[2] On the first day, the worldwide public learned that the NSA has obtained a clandestine court order from a secretly operating court of law, called the Foreign Intelligence Surveillance Court (FISC), and on its basis the Agency has been collecting metadata on telephone calls of millions customers of a major private telecommunications provider, Verizon. This provider was forbidden from disclosing both the order itself and its compliance with it. On the second day (7 June), the worldwide public learned further that these practices had not been limited to a single provider and that the NSA was allegedly 'tapping directly into the central servers of nine

* Centre for Commercial Law, Faculty of Law, Bond University. E-mail: dan_svantesson@bond.edu.au.

** Research Group on Law, Science, Technology & Society, Vrije Universiteit Brussel; Peace Research Institute Oslo. E-mail: dariusz.kloza@vub.ac.be.

1 We understand 'Snowden *affaire*' broadly: it is both the disclosures Edward Snowden made to the journalists about global mass surveillance practices, as well as their ramifications. We have spent some time discussing how to name it in this book. It could have been e.g. 'NSA scandal' or 'PRISM-gate', but ultimately we have named it after the person who stands behind the disclosures. We chose the French word '*affaire*' since it can signify both a case in a court of law as well as a political scandal, as contributions in this book are concerned with legal and political analysis of trans-Atlantic data privacy relations. Cf. *Le trésor de la langue française*, <http://atilf.atilf.fr>.

2 Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily', *The Guardian*, 6 June 2013, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

leading U.S. Internet companies': Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.[3] The worldwide public also learned that the NSA has been 'listening' to anything about anybody whose data merely flew through servers located on US soil, even when sent from one overseas location to another. Finally, the NSA has shared these data with its fellow agencies in the US, such as with the Federal Bureau of Investigation (FBI). These practices were variously codenamed – labels of surveillance programmes such as PRISM, Xkeyscore, Upstream, Quantuminsert, Bullrun or Dishfir have since entered the public debate[4] – and their aim was to procure national security with the help of surveillance. (These practises were not a novelty for the NSA has operated domestic surveillance programmes since the Agency's establishment in 1952.[5] It is also true that surveillance practices are as old as humanity and over time have became an integral part of modernity,[6] but these have intensified in the aftermath of the 11 September 2001 terrorist attacks.)[7]

These revelations were built on a series of leaks from a former NSA contractor to a number of major media outlets worldwide such as *The Guardian*, *The Washington Post* and *Der Spiegel*. He revealed his identity on the fourth day (9 June).[8] The disclosures Edward Snowden brought to the public eye have sparked a continuous, and sometimes rather heated, debate about the pursuit of national security through the use of mass surveillance practices and individual rights and freedoms – not least in the trans-Atlantic setting.[9]

Initially, the whole *affaire* had a predominantly vertical dimension, focusing on the relations between an individual and the state. However, this changed when it was revealed that the NSA, in its global mass surveillance practices, had been cooperating with its counterparts in the Anglo-Saxon world. This included, *inter alia*, the United Kingdom's Government Communications Headquarters

---

3 Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post*, 7 June 2013, <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

4 Zygmunt Bauman et al., 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8(2) *International Political Sociology* 122.

5 George F. Howe, 'The Early History of NSA' (1974) 4(2) *Cryptologic Spectrum* 11, <http://www.senderling.net/6988th.org/Docs/The_Early_History_of_the_NSA.pdf>.

6 David Lyon, *Surveillance Studies: An Overview*, Wiley, 2007, p. 12.

7 On this matter, cf. esp. David Lyon, *Surveillance After September 11*, Wiley, 2003.

8 Glenn Greenwald, Ewen MacAskill and Laura Poitras, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations', *The Guardian*, 9 June 2013, <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

9 Francesca Musiani, 'Edward Snowden, L'«homme-Controverse» de La Vie Privée Sur Les Réseaux' (2015) 3(73) *Hermès, La Revue* 209, <www.cairn.info/revue-hermes-la-revue-2015-3-page-209.htm>.

(GCHQ) and Australian Signals Directorate (ASD),[10] both members of the 'Five Eyes' alliance. The worldwide public's attention was drawn to the GCHQ who had used the PRISM programme to directly obtain data without 'the formal legal process required to seek personal material … from an internet company based outside the UK' (7 June).[11]

Next, on 29 June 2013 *Der Spiegel* published a finding in the Snowden leaks that European leaders had also been spied on.[12] The bugged mobile phone of the German Chancellor Angela Merkel became iconic. (There was even a cartoon that went viral on social media in which the US President Barack Obama on a phone says to Merkel: 'I will tell you how I am because I already know how you are doing'.)[13] This created political turmoil in Europe and many of the political leaders, bugged or not, criticised the excessive surveillance practices and began to question the *status quo* of the Euro–American relations. In November 2013 the then European Union Commissioner for Justice Viviane Reding even threatened taking steps to suspend the (now defunct) Safe Harbor arrangement.[14] Thus, the Snowden *affaire* took on another, international dimension (horizontal) in which relations between states have been put at stake.

II.

The second source of our inspiration is perhaps a little more surprising. John Oliver, a British comedian and a host of popular US TV programme *The Daily Show*, devoted an episode (10 June 2013) to the then-breaking Snowden *affaire*.[15] He quoted President Obama's San José, California speech (7 June), in which the latter had stated 'there are a whole range of safeguards involved' against the surveillance practices of the NSA, thus implying they are OK. Oliver concluded with a comment: 'I think you are misunderstanding the perceived problem here,

---

10 Philip Dorling, 'Australia gets "deluge" of US secret data, prompting a new data facility', *The Sydney Morning Herald*, 13 June 2013, <http://www.smh.com.au/it-pro/security-it/australia-gets-deluge-of-us-secret-data-prompting-a-new-data-facility-20130612-2o4kf>.

11 Nick Hopkins, 'UK gathering secret intelligence via covert NSA operation', *The Guardian*, 7 June 2013, <https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>.

12 Laura Poitras, Marcel Rosenbach, Fidelius Schmid and Holger Stark, 'NSA horcht EU-Vertretungen mit Wanzen aus', *Der Spiegel*, 29 June 2013, <http://www.spiegel.de/netzwelt/netzpolitik/nsa-hat-wanzen-in-eu-gebaeuden-installiert-a-908515.html>.

13 Quoting from memory.

14 Ian Traynor, 'NSA surveillance: Europe threatens to freeze US data-sharing arrangements', *The Guardian*, 26 November 2013, <https://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing>.

15 Victor Luckerson, 'How the 'John Oliver Effect' Is Having a Real-Life Impact', *Time*, 10 July 2015, <http://time.com/3674807/john-oliver-net-neutrality-civil-forfeiture-miss-america>.

Mr President. No one is saying that you broke any laws. We are just saying it is a little bit weird that you did not have to'.[16]

John Oliver formulated in this context the very question about the *limits*, about the *use* and *abuse*, of the law and of the state's power when it comes to global mass surveillance practices. Where does lie the 'thin red line' between the two legitimate yet seemingly competing interests: national security and privacy? This question touches upon all the 'stars' in a classical 'constellation of ideals that dominate our political morality',[17] i.e. democracy, the rule of law and/or the legal state (*Rechtsstaat*), and fundamental rights. Two aspects triggered our particular attention: the conformity of these practices with the rule of law and/or the *Rechtsstaat* doctrines, and the extent of the permissible interference with the fundamental rights affected, such as the right to (data) privacy and the freedom of expression.

First, both the rule of law and the *Rechtsstaat* concepts serve multiple purposes in society and one of them is to channel the exercise of 'public power through law'.[18] They achieve their goals in two different manners, yet these manners share a few characteristics.[19] For the sake of our argument, it shall suffice to acknowledge that they occur in two understandings. In the narrow, rather formal one ('thin'), both concepts comprise the requirement of some form of 'legality', such as the enactment of a legal statute in accordance with a given procedure, and certain safeguards, such as access to a court of law.[20] The comprehensive, substantive understanding ('thick') of the rule of law (*Rechtsstaat*) 'encompass[es] procedural elements, and, additionally, focus[es] on the realization of values and concern[s] the content of law'.[21]

---

16 John Oliver, 'Good News! You're not paranoid – NSA Oversight', *Comedy Central*, 10 June 2013, <http://www.cc.com/video-clips/cthyr1/the-daily-show-with-jon-stewart-good-news--you-re-not-paranoid---nsa-oversight>.

17 Jeremy Waldron, 'The Rule of Law and the Importance of Procedure,' in James Fleming (ed.), *Getting to the Rule of Law*, New York University Press, 2011, p. 3, <http://lsr.nellco.org/cgi/viewcontent.cgi?article=1235&context=nyu_plltwp>.

18 Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights*, Oxford University Press, 2013, p. 18.

19 We are aware that there exist essential differences between the rule of law and the *Rechtsstaat* doctrines. We are further aware of a never-ending debate both as to the delineation between these two and as to their building blocks. Both doctrines overlap in many aspects, yet their origins are different, each of them having slightly different contents and *modus operandi*. Each of them can be found applied differently in different jurisdictions; the former concept dominates in the Anglo-Saxon world, the latter on continental Europe. The analysis of all these aspects lies beyond the scope of this contribution. Cf. e.g. James R. Silkenat, Jr., James E. Hickey and Peter D. Barenboim (eds.), *The Legal Doctrines of the Rule of Law and the Legal State (Rechtsstaat)*, Springer, 2014; Tom Bingham, *The Rule of Law*, Allen Lane, 2010; Brian Z. Tamanaha, *On the Rule of Law: History, Politics, Theory*, Cambridge University Press, 2004.

20 Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights*, Oxford University Press, 2013, p. 18.

21 Ibid., pp. 18–21.

The Snowden *affaire* demonstrated that the contents of legal provisions matter too. If we look at the rule of law and the *Rechtsstaat* doctrines in their narrow understanding, then – simplifying – when a legal provision fulfils only formal criteria, it is all ok. There are indeed commentators who prefer this 'thin' understanding as it is simply 'easier to identify' its meaning; it is a fair, theoretical argument. There are too sometimes businesses and authoritarian governments who prefer the 'thin' understanding as formal criteria are 'easier to satisfy'. They create an illusion in diplomatic and international trade circles that their actions are (to be) judged ok. 'Legality' or the mere access to a court of law are important but they are not enough. Consequently, many commentators 'find thin conceptions quite inadequate':[22] it is of lesser importance that a legal statute validly exists; it is of much greater importance what this statute actually does.

Second, fundamental rights – short of a few – are not absolute. Their enjoyment can be limited in some circumstances. For example, in the European context, an interference with a fundamental right is permissible when it is made 'in accordance with the law and is necessary in a democratic society' and serves some public interest, e.g. national security or public safety.[23] In this sense – and again, simplifying – a legal norm is judged to be in conformity with fundamental rights when it does not exceed what is necessary and proportionate to a legitimate aim pursued and such a norm was enacted legally. Some parallels can be drawn here with the rule of law and the *Rechtsstaat* doctrines: there exist both formal (i.e. legality) and substantive limitation criteria of fundamental rights (i.e. proportionality, necessity and legitimacy). Again, the latter are of much greater importance. Some commentators even heralded that 'to speak of human rights is to speak about proportionality'.[24] The Snowden *affaire* demonstrated disproportionality of global mass surveillance practices to the main legitimate aim these practices pursued: security. As Lyon asks, '[i]s mass surveillance the right way to achieve it?'[25]

The sequence of events sketched above has inspired the main idea for this book with John Oliver formulating its central research question: to explore trans-Atlantic relations challenging the doctrines of democracy, rule of law (*Rechtsstaat*) and fundamental rights. The perspective is that of data privacy.

---

22 Martin Krygier, 'Rule of Law (*and Rechtsstaat*)', in James R. Silkenat, Jr., James E. Hickey and Peter D. Barenboim (eds.), *The Legal Doctrines of the Rule of Law and the Legal State (Rechtsstaat)* Springer, 2014, p. 46, pp. 51–52.

23 European Convention on Human Rights, Rome, 4 November 1950, ETS 5. Cf. Arts. 8–11.

24 Grant Huscroft, Bradley W. Miller and Grégoire C.N. Webber (eds.), *Proportionality and the Rule of Law: Rights, Justification, Reasoning*, Cambridge University Press, 2014, p. 1.

25 David Lyon, *Surveillance After Snowden*, Polity Press, 2015, p. 13.

III.

Subsequent events led the idea for this book to grow and mature. These took place predominantly on the European side of the Atlantic.[26] On 8 April 2014 the Court of Justice of the European Union (CJEU; Luxembourg Court) delivered a landmark judgment in *Digital Rights Ireland*.[27] In essence, the Court not only declared the 2006 Data Retention Directive[28] invalid but also held under what conditions personal data retention practices can be considered proportionate to the national security goals pursued.

In parallel, the European Union (EU) has been reforming its data privacy legal framework, which on 27 April 2016 eventually took the form of General Data Protection Regulation (GDPR),[29] and of Police and Criminal Justice Data Protection Directive.[30] The works on the 'update' of Regulation 2001/45[31] and e-Privacy Directive continue.[32] The Council of Europe is nearing the conclusion of the five-year process of modernisation of its data privacy convention (the so-called 'Convention 108'),[33] at the same time aiming to make it a global instrument. It was the need to keep up with technological developments, on the one hand, as well as political, economic and societal changes, on the other, that created a need to update both legal frameworks.

---

26 We have been closely observing the European response to the Snowden *affaire*, account of which is given e.g. in David Wright and Reinhard Kreissl, 'European Responses to the Snowden Revelations' in id., *Surveillance in Europe*, Routledge, 2014, pp. 6–49. Cf. also Lindsay, Ch. 3, Sec. 4, in this volume. Here we only give account of some of our further inspirations.

27 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

28 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] OJ L 105/54–63.

29 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 119/1–88.

30 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119/89–131.

31 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, [2001] OJ L 8/1–22.

32 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37–47.

33 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28 January 1981, Strasbourg <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>. Cf. also Council of Europe, *Modernisation of Convention 108*, Strasbourg, 29 November 2012, T-PD(2012)4Rev3_en.

Simultaneously, the EU has been negotiating comprehensive free trade agreements with numerous countries.[34] Agreements with the US and Canada are particularly high on the political agenda. Even though free trade *prima facie* does not concern data privacy, all parties keep in mind the failure on such grounds of the multilateral Anti-Counterfeit Trade Agreement (ACTA) in February 2012. Among other provisions, its Art. 27 provided for a possibility of requesting an order from a competent authority aiming at the disclosure of information to identify the subscriber whose account allegedly been used for intellectual property rights (IPR) infringement, upon which right holders might take action. Many commentators considered this and many similar solutions in the text of ACTA as disproportionate, thus not living up to the democratic standards.[35] At the same time, the Luxembourg Court held that the monitoring of Internet traffic in order to prevent infringements of IPR, seek violators and/or police them constitutes a disproportionate interference with fundamental rights (cf. *Scarlet v. Sabam* (24 November 2011)[36] and *Sabam v. Netlog* (16 February 2012)).[37]

In the time since work on this book commenced, the Luxembourg Court rendered another milestone judgment in *Schrems* (6 October 2015),[38] invalidating the Safe Harbor arrangement.[39] For 15 years it allowed American data controllers, who had self-certified to the US Department of Commerce their adherence to the principles of this arrangement, to freely transfer personal data from Europe. Building to a large extent on its *Digital Rights Ireland* judgment, the Court declared invalid the so-called adequacy decision that laid behind the arrangement. The judges in Luxembourg held that bulk collection of personal data compromises 'the essence of the fundamental right to respect for private life'.[40] Nine months later the Safe Harbor was replaced by a very similar Privacy Shield arrangement (12 July 2016).[41] Its compatibility with fundamental rights in the EU remains questionable.

---

34 Cf. <http://ec.europa.eu/trade/policy/countries-and-regions/agreements>.

35 Irina Baraliuc, Sari Depreeuw and Serge Gutwirth, 'Copyright Enforcement in the Digital Age: A Post-ACTA View on the Balancing of Fundamental Rights' (2013) 21(1) *International Journal of Law and Information Technology* 93–100.

36 Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*.

37 Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*.

38 Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

39 Commission Decision of 26 July 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, 2000/520/EC, [2000] OJ L 215/7–47.

40 Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, §94.

41 Commission Implementing Decision (EU) 2016/1250 of 12 July 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, C/2016/4176, [2016] OJ L 207/1–112.

As the gestation of this book was coming to an end (September 2016), the Luxembourg Court was seized, *inter alia*, with the questions who controls the handling of personal data on a 'fan page' on a major social network site, therefore determining responsibilities for violations of data privacy laws,[42] and whether the use of such a social network site for purposes both private and professional still qualifies its user as a consumer, therefore allowing her to benefit from protective rules on jurisdiction.[43] The Court has also to decide two joined cases on data retention: in *Watson et al.*, whether the requirements laid down in *Digital Rights Ireland*[44] are mandatory, and in *Tele2 Sverige*, whether the post-*Digital Rights Ireland* retention of personal data is compatible with EU fundamental rights.[45]

On the other side of the Atlantic – among 'two dozen significant reforms to surveillance law and practice since 2013'[46] – President Obama signed into law the USA Freedom Act of 2015, which, *inter alia*, increases transparency of the work of the Foreign Intelligence Surveillance Court (FISC)[47] as well as the Judicial Redress Act of 2015, extending 'Privacy Act [of 1974][48] remedies to citizens of certified states'.[49]

These legislative developments and judicial decisions (as well as those in the future) have significant implications for trans-Atlantic data privacy relations. Not only because they either involve a private organisation or an authority originating from one or another side of the Atlantic or because they concern conditions for handling personal data within global mass surveillance practices, but rather because they set step-by-step standards for data privacy protection.

IV.

There has been one more inspiration for this book. Outside the *Consilium* building on rue de la Loi/Wetstraat in Brussels, hosting both the European Council and the Council of Ministers of the European Union, stands the bronze statue depicted on the back cover of this book. 'Stepping Forward' was created by Dutch-born sculptor Hanneke Beaumont, and erected where it stands today in 2007. We think this statue – and the multiple ways that it can be viewed – is

42 Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein GmbH v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*.

43 Case C-498/16, *Maximilian Schrems v. Facebook Ireland Limited*.

44 Above n. 27.

45 Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and *Watson et al*.

46 Swire, Ch. 4 in this volume.

47 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 [USA Freedom Act of 2015], Public Law 114-23, 50 USC 1801, §601 ff.

48 Privacy Act of 1974, Public Law 93-579, 5 USC 552a.

49 Judicial Redress Act of 2015, Public Law 114-126, 5 USC §552a.

an interesting symbol for data privacy regulation. One way to look at the statue is to focus on how this proud androgynous person, representing humanity (or at least the people of Europe), clad in only a thin gown, bravely takes a necessary leap of faith into the unknown. This is no doubt a suitable representation of how some people view (European) efforts aimed at data privacy regulation.

However, the statue also lends itself to quite a different – less flattering – interpretation. One can perhaps see the statue as a malnourished, clearly confused, possibly deranged, frail man in a lady's night gown, engaging in a foolish endeavour bound to end in a nasty, indeed catastrophic, fall. Those sceptical of data privacy regulation, at least it its current forms, may see some parallels between this interpretation and the current European approach to data privacy.

This is indeed how different are the perspectives people may have on data privacy regulation. And while the difference in perspectives is too complex to be mapped geographically, it may be fair to say that more people in Europe would prefer the first interpretation of the parallels between Beaumont's statue and data privacy regulation, while more people in the US are likely to see the parallel as we described second; in any case, the trans-Atlantic divide remains palpable.

V.

For our ideas to bear fruit, we chose the *European Integration and Democracy* series, edited at the Centre for Direct Democracy Studies (CDDS) at the University of Białystok, Poland and published by Belgian-based Intersentia, a suitable outlet for our book. Both institutions welcomed our proposal. Since the Series was launched in 2011, each volume therein is meant to look at a particular aspect of European integration as matter of – broadly understood – democracy, rule of law (*Rechtsstaat*) and fundamental rights. Therefore the title of each volume finishes with '… as a challenge for democracy'.[50]

The present book is a response to a call for papers. It was issued in June 2015 and we have been overwhelmed with the answer thereto: we have accepted 18 submissions from around the world. All of them underwent a double blind peer-review process in accordance with the Guaranteed Peer-Review Contents (GPRC) scheme, a standard used by Intersentia.[51] In parallel, a number of

[50] The previous volumes are: Elżbieta Kużelewska and Dariusz Kloza (eds.), *The Challenges of Modern Democracy and European Integration*, Aspra-JR, 2012; Elżbieta Kużelewska and Dariusz Kloza (eds.), *Elections to the European Parliament as a Challenge for Democracy*, Aspra-JR, 2013; Elżbieta Kużelewska, Dariusz Kloza, Izabela Kraśnicka and Franciszek Strzyczkowski (eds.), *European Judicial Systems as a Challenge for Democracy*, Intersentia, 2015.

[51] Cf. <http://www.gprc.be/en/content/what-gprc>.

informal conversations during the gestation of the book led to eight invited contributions by distinguished experts in the field.

On 29 January 2016, we hosted a dedicated authors' panel at the 9th Computers, Privacy and Data Protection (CPDP) in Brussels, Belgium, a world-leading annual event in the field.[52] Four authors accepted our invitation – in the order of appearance – Peter Swire, Els De Busser, Michał Czerniawski and Trisha Meyer; Gemma Galdon Clavell moderated the debate. We thank them for their participation. With the then-upcoming European football championships in France (10 June–10 July 2016), the panellists at the very end were asked – in an imaginary 'data privacy game' – in which team they would play – European or American, in what role and why. The vast majority chose the European team.

The result we present to the reader might seem merely another book about the Snowden *affaire* and the fall of Safe Harbor, but these two have been (only) an inspiration. Our object of interest is the protection of data privacy[53] in relations between Europe and Americas as a challenge for democracy, the rule of law (*Rechtsstaat*) and fundamental rights. Both geographical notions are understood *sensu largo*.[54] (A careful reader would notice we have not necessarily been consistent and we have included also contributions treating Austral-Asian data privacy matters, as we found that they add value to the book.) As the regulation of data privacy is in the competences of the EU, our object of interest has gained relevance for European integration.[55] Therefore, this book looks into the *status quo* of such relations. In parallel, Hanneke Beaumont's sculpture – a step into the unknown – inspired us to conclude this book with some postulates as to their future shape.

We have split this book into three main parts. The first part deals with five pertaining problems the concept of data privacy protection faces in trans-Atlantic relations. The opening problem is that of transborder flows of personal data. The scene is set in the first chapter in which *Weber* analyses the place of the protection of data privacy in the EU Digital Single Market Strategy.[56] Two

---

52 Cf. <http://www.cpdpconferences.org>.

53 We deliberately chose 'data privacy' as a term to encompass both the European understanding of 'data protection' and the Anglo-Saxon one of 'informational privacy'. Cf. Christopher Kuner et al., 'Taking Stock after Four Years' (2014) 4(2) *International Data Privacy Law* 87–88.

54 By 'Europe *sensu largo*' we mean the patchwork of supranational and regional arrangements of political and economic nature occurring at the European continent. In particular, our understanding comprises, but is not limited to, the European Union and the Council of Europe. By 'Americas *sensu largo*' we deploy its geographical meaning, but the reader will notice that the focus is predominantly on the United States of America.

55 Cf. Art. 16(2) of the Treaty on the Functioning of the European Union, [2012] OJ C 326/47–390.

56 European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, Brussels, 6 May 2015.

subsequent chapters analyse the principles for the trans-Atlantic data flows: *Schweighofer* gives a broad picture, while *Lindsay* focuses on the principle of proportionality. Next, *Swire* analyses the reforms 'US surveillance law' underwent since the Snowden *affaire* broke out and *Vermeulen* argues the Privacy Shield arrangement does not meet the necessity and proportionality criteria set forth in the EU fundamental rights law. Finally, *Doneda* offers an insight on international data transfers from Brazil, a jurisdiction without a comprehensive data privacy legal framework.

The second problem discussed in this part deals with the regulation of international trade. *Meyer & Vetulani-Cęgiel* write about public participation in a decision making process concerning a free trade agreement (FTA); their observations are equally applicable to the data privacy universe. *Greenleaf* surveys the variety of ways in which FTAs have affected the protection of data privacy. *Schaake* concludes with her suggestions for regulating trade and technology. The third problem deals with territorial application of the data privacy laws. *Czerniawski* asks whether 'the use of equipment' is – in a contemporary digitalised and globalised world – an adequate determinant for such laws to apply. *Bentzen* and *Svantesson* give a comprehensive overview of applicable laws when personal data containing DNA information are being processed. The fourth problem confronted is that of data privacy and crime. *Kovič Dine* attempts to understand the peacetime economic cyber-espionage among states under international law with a special reference to the theft of personal and otherwise privileged data. *Gerry* takes a critical look at existing legal arrangements to better understand how cyber law deals with combating terrorism and paedophilia on the Internet. *Amicelle* gives three hypotheses to understand the failure of the US Terrorist Finance Tracking Program after 15 years of its operation. The fifth and final problem deals with data privacy and the passage of time. *Szekely* comparatively analyses the regulation of the post-mortem privacy in the EU and the US. *Miyashita* compares the legal *status quo* of the 'right to be forgotten' in the EU and Japan.

The second part discusses the constitutive elements of the notion of data privacy. The four contributions published here discuss the understanding of a piece of 'information linked to an individual' in jurisdictions ranging from Europe to US to Australia (*Míšek; Maurushat & Vaile*), the distinction between 'privacy' and 'security' (*Wilson*) and the ethicality of personal data markets (*Spiekermann*).

The final, third part suggests a few alternative approaches to the protection of data privacy. It subconsciously builds on a premise that contemporary, existing approaches do not necessarily live up to the expectations vested therein and thus more is needed. This part looks at possible lessons to be learned from US environmental law – about community right-to-know, impact assessments and 'mineral rights' in property (*Emanuel*) as well as from criminal law – to replace the European criterion of 'adequacy' in transborder data flows by the criterion

of a flagrant denial of data protection (*De Busser*). A subsequent contribution recognises a new category of data privacy protections – i.e. behavioural – that is to supplement existing regulatory, technological and organisational protections (*Kloza*). *Goldenfein* explores ideas around automated privacy enforcement and the articulation of individual protections from profiling into the telecommunications infrastructure. Subsequently, *De Hert & Papakonstantinou* plea for more data privacy at the political agenda of the United Nations (UN). This is to be achieved by establishing a dedicated data privacy agency, similar to the World Intellectual Property Organisation (WIPO). Finally, *Kwasny* discusses the prospects of the (modernised) 'Convention 108' of the Council of Europe as an international standard for data privacy protection. A few of our observations as to the *status quo* and the future of trans-Atlantic data privacy relations conclude this book.

The present book is very clearly an anthology – it is a compilation of diverse contributions, from different perspectives, within a broad topic. Our aim with this volume is to highlight a selection of particularly 'hot' questions within the topic of trans-Atlantic data privacy relations as they look at the end of 2016. In a sense, what we have aimed to create could be seen as a snapshot, giving a picture of what is on the agenda for scholars concerned with data privacy at this particular point in time, which just happens to be a particularly important, indeed formative, moment within this area.

We have been exceptionally careful to allow the authors to express their ideas as they wish to do so, with only minimal editorial intervention. The advantage of this approach is obvious given our stated aim of reflecting the great diversity of thinking that exists on the matters addressed. However, we hasten to acknowledge that this approach comes at the cost of a lower level of consistency and coherence within the volume. Put simply, we have not aimed at any, and the reader is unlikely to find any, *fil rouge* apart from the above-mentioned broad terms. However, that is not to say that the contributions to this volume – as a collective – do not lend themselves to conclusions. In the final chapter, we too draw out and highlight those themes we see emerging within the body of this work. We eventually attempt to suggest a few lessons *de lege ferenda*.

This book is predominantly addressed to policy-makers and fellow academics on both sides of the Atlantic, and indeed, around the world. It is our hope that this volume will be an interesting read from front to back as well as serve as a reference work.

VI.

This book is a fruit of 'nomadic writing operations'[57] and these operations have at least two aspects. First, throughout the gestation of the book we have met with

[57] Mireille Hildebrandt coined this term.

the majority of authors at various occasions around the world. The exchange of ideas has been inestimable. Second, the book has been practically edited *en route*, naturally contributing to the said exchange of ideas, yet to a slight detriment to the regularity of the writing process. A good deal of work was done in Australia. Dan is based in Gold Coast, Queensland where he is a Professor of Law at the Faculty of Law, Bond University and a Co-Director of the Centre for Commercial Law. Dariusz, who on a daily basis is a researcher at the Vrije Universiteit Brussel (VUB), was a visiting scholar at Bond University from March to May 2016. (Dariusz Kloza gratefully acknowledges the financial support he received for that purpose from the Fonds Wetenschappelijk Onderzoek – Vlaanderen in Belgium.) The book was finalised in Scandinavia. Dan has spent the summer of 2016 at Stockholm University and Dariusz – at his other academic home, the Peace Research Institute Oslo (PRIO).

In producing this volume, we have racked up numerous debts which it is a pleasure to record. We both thank and congratulate the authors for their excellent work. We thank Wojciech R. Wiewiórowski, Assistant European Data Protection Supervisor (EDPS), for providing this book with an insightful foreword. Furthermore, the series editors, the anonymous reviewers and the peer-reviewers helped us ensuring academic quality of this volume. We received further help and support from (in alpha order) Rocco Bellanova, Katja Biedenkopf, Michał Czerniawski, Barry Guihen, Władysław Jóźwicki, Catherine Karcher, Christopher Kuner, Elżbieta Kużelewska and Lucas Melgaço. We have been fortunate to work again with Intersentia and our editor Tom Scheirs. Magdalena Witkowska took the picture printed on the back cover of this book. We extend our gratitude to all of them. Finally, we gratefully acknowledge the financial support of the Research Group on Law, Science, Technology and Society (LSTS) at VUB.

Stockholm/Oslo, September 2016

CONTENTS

LIST OF ABBREVIATIONS

AANZFTA	ASEAN–Australia–New Zealand Free Trade Area
ACTA	Anti-Counterfeiting Trade Agreement
AEPD	Agencia Española de Protección de Datos
APEC	Asia-Pacific Economic Cooperation
API	Advance Passenger Information
APP	Australian Privacy Principle
ASD	Australian Signals Directorate
ASEAN	Association of South East Asian Nations
BCR	Binding Corporate Rules
BD	big data
CETA	Comprehensive Economic and Trade Agreement
CFR	Charter of Fundamental Rights of the European Union
CISA	Convention Implementing the Schengen Agreement
CJEU	Court of Justice of the European Union
CMPPA	Computer Matching and Privacy Protection Act [US]
CoE	Council of Europe
COPPA	Children's Online Privacy Protection Act [US]
CPDP	Computers, Privacy and Data Protection conference
CPO	chief privacy officer
Cth	Commonwealth [Australia]
DG	Directorate-General (of the European Commission)
DNA	deoxyribonucleic acid
DPD	Data Protection Directive
DPIA	data protection impact assessment
DPO	data protection officer
DRM	Digital Rights Management
DSM	Digital Single Market
DTC	direct-to-consumer
EC	European Commission
ECHR	European Convention on Human Rights
ECJ	European Court of Justice (former name of CJEU)
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area

EFTA	European Free Trade Agreement
EIS	environmental impact statement
EP	European Parliament
EPAL	Enterprise Privacy Authorisation Language
ETS	European Treaty Series
EU	European Union
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FoI	Freedom of Information
FONSI	finding of no significant impact
FTA	free trade agreement
FTC	Federal Trade Commission [US]
GAO	Government Accountability Office [US]
GATS	General Agreement on Trade in Services
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HIPPA	Health Insurance Portability and Accountability Act [US]
HTML	HyperText Markup Language
IaaS	Infrastructure as Service
IANA	Internet Assigned Numbers Authority
IATA	International Civil Aviation Organization
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICRC	International Committee of the Red Cross
ICT	information and communications technologies
IDPC	Irish Data Protection Commissioner
ILO	International Labor Organization
IMAP	Internet Mail Access Protocol
IP	intellectual property
IP	Internet Protocol
IPR	intellectual property rights
ISDS	investor-state dispute settlement
IT	information technology
JHA	Justice and Home Affairs
LEA	law enforcement agency
MEP	Member of European Parliament

NAFTA	North American Free Trade Agreement
NEPA	National Environmental Policy Act
NGO	non-governmental organisation
NIS	Network and Information Security
NIST	National Institute of Standards and Technology [US]
NSA	National Security Agency
NSL	National Security Letter
OAIC	Office of Australian Information Commissioner
ODNI	Office of the Director of National Intelligence
OECD	Organization of Economic Cooperation and Development
OJ	Official Journal
OMB	Office of Management and Budget [US]
PaaS	Platform as Service
PACER	Pacific Agreement on Closer Economic Relations
PbD	Privacy by Design
PCLOB	Privacy and Civil Liberties Oversight Board
PD	personal data
PET	Privacy Enhancing Technologies
PGP	Pretty Good Privacy
PI	personal information
PIA	privacy impact assessment
PII	personally identifiable information
PNR	passenger name record
POP3	Post Office Protocol 3
PPD	Presidential Policy Directive
RCEP	Regional Comprehensive Economic Partnership
RFID	radio-frequency identification
RTBF	right to be forgotten
SAARC	South Asia Area of Regional Cooperation
SaaS	Software as Service
SIGINT	signal intelligence
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAMI	Transparent Accountable Data Mining Initiative
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Programme
TISA, TiSA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
TRIMS	Trade Related Investment Measures
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TTIP	Transatlantic Trade and Investment Partnership
UDHR	Universal Declaration of Human Rights

UK	United Kingdom
UKSC	United Kingdom Supreme Court
UN	United Nations
URL	uniform resource locator
US	United States of America
VIS	Visa Information System
VPN	virtual private network
WIPO	World Intellectual Property Organization
WP29	Article 29 Working Party
WTO	World Trade Organisation
XACML	eXtensible Access Control Markup Language