TRANS-ATLANTIC DATA PRIVACY RELATIONS
AS A CHALLENGE FOR DEMOCRACY
European Integration and Democracy Series

Editor-in-Chief

ELŻBIETA KUŻELEWSKA, University of Białystok, Poland

Series Editors

DANIEL BARNHIZER, Michigan State University, East Lansing MI, United States of America
TOMAS BERKMANAS, Vytautos Magnus University, Kaunas, Lithuania
FILIP KŘEPELKA, Masaryk University, Brno, Czech Republic
ERICH SCHWEIGHOFER, University of Vienna, Austria
RYSZARD SKARZYŃSKI, University of Białystok, Poland
KONSTANTY A. WOJTASZCZYK, University of Warsaw, Poland
TRANS-ATLANTIC DATA PRIVACY RELATIONS AS A CHALLENGE FOR DEMOCRACY

Edited by
Dan Jerker B. Svantesson
Dariusz Kloza

intersentia
Cambridge – Antwerp – Portland
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>.
leading U.S. Internet companies: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. 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 Dishfire have since entered the public debate – and their aim was to procure national security with the help of surveillance. (These practices were not a novelty for the NSA has operated domestic surveillance programmes since the Agency’s establishment in 1952.

It is also true that surveillance practices are as old as humanity and over time have became an integral part of modernity, but these have intensified in the aftermath of the 11 September 2001 terrorist attacks.)

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). 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.

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

---

(GCHQ) and Australian Signals Directorate (ASD), 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,

---

13 Quoting from memory.
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

---


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.


21 Ibid., pp. 18–21.
The Snowden affair 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’: 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. 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’.

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.

---

III.

Subsequent events led the idea for this book to grow and mature. These took place predominantly on the European side of the Atlantic. On 8 April 2014 the Court of Justice of the European Union (CJEU; Luxembourg Court) delivered a landmark judgment in Digital Rights Ireland. In essence, the Court not only declared the 2006 Data Retention Directive 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), and of Police and Criminal Justice Data Protection Directive. The works on the ‘update’ of Regulation 2001/45 and e-Privacy Directive continue. 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’) 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.


Simultaneously, the EU has been negotiating comprehensive free trade agreements with numerous countries.\textsuperscript{34} Agreements with the US and Canada are particularly high on the political agenda. Even though free trade \textit{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.\textsuperscript{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. \textit{Scarlet v. Sabam} (24 November 2011)\textsuperscript{36} and \textit{Sabam v. Netlog} (16 February 2012)).\textsuperscript{37}

In the time since work on this book commenced, the Luxembourg Court rendered another milestone judgment in \textit{Schrems} (6 October 2015),\textsuperscript{38} invalidating the Safe Harbor arrangement.\textsuperscript{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 \textit{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'.\textsuperscript{40} Nine months later the Safe Harbor was replaced by a very similar Privacy Shield arrangement (12 July 2016).\textsuperscript{41} Its compatibility with fundamental rights in the EU remains questionable.

\textsuperscript{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) \textit{International Journal of Law and Information Technology} 93–100.
\textsuperscript{36} Case C-70/10, \textit{Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL} (SABAM).
\textsuperscript{37} Case C-360/10, \textit{Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA} (SABAM) v. Netlog NV.
\textsuperscript{38} Case C-362/14, \textit{Maximillian Schrems v. Data Protection Commissioner}.
\textsuperscript{40} Case C-362/14, \textit{Maximillian Schrems v. Data Protection Commissioner}, §94.
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, 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. 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 are mandatory, and in Tele2 Sverige, whether the post-Digital Rights Ireland retention of personal data is compatible with EU fundamental rights.

On the other side of the Atlantic – among ‘two dozen significant reforms to surveillance law and practice since 2013’ – 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) as well as the Judicial Redress Act of 2015, extending ‘Privacy Act [of 1974] remedies to citizens of certified states’.

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

---

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 telesystemen and Watson et al.
46 Swire, Ch. 4 in this volume.
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 in 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’.

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. In parallel, a number of

---


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. 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 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. (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. 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. Two

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.
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 affair 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-Cegiel 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 Swantesson 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 (Mišek; 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’ 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

*Foreword by Dr Wojciech R. Wiewiórowski* ........................................... v  
*Preface* ........................................... ix  
*List of Abbreviations* ........................................... xxxvii  

**PART I**  
**PRIVACY AND ...**  

**SECTION I**  
**PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA**  

1. **Transnational Data Privacy in the EU Digital Single Market Strategy**  
   Rolf H. Weber .................................................. 5  
   
1. Introduction .................................................. 5  
2. Tensions between free data flow and data privacy ..................... 6  
   2.1. Free data flow and data privacy as parallel EU objectives ........ 6  
   2.2. Data privacy as policy and regulatory topic ..................... 8  
      2.2.1. Tensions between fundamental rights and regulatory frameworks .......... 8  
      2.2.2. Current developments in the EU ................................ 8  
      2.2.3. Current developments in the US ................................ 10  
3. Inclusion of more actors in data protection rule-making ............ 13  
   3.1. Concept of multi-stakeholderism ................................ 13  
   3.2. Implementation in the data privacy field ........................ 15  
4. Transboundary impacts of the data privacy framework .............. 16  
   4.1. Sovereignty and legal interoperability ........................ 16  
      4.1.1. Traditional notion ....................................... 16  
      4.1.2. Challenges of a global cyberspace ......................... 17  
      4.1.3. Interoperability of legal frameworks ..................... 18  
      4.1.4. Achieving legal interoperability .......................... 19  
      4.1.5. Increased legal interoperability in the data privacy field ........ 21  
   4.2. New participation models for data privacy rule-making .......... 22  
      4.2.1. Increased quality of rule-making ......................... 24  
5. Outlook .................................................. 25
Erich SCHWEIGHOFER ......................................................... 27

1. Introduction .............................................................. 27
2. State sovereignty and the legal framework for international data transfer ........................................... 29
3. Requirement of essentially equivalent level of data protection ........... 33
4. US–EU data transfer regimes ........................................ 35
   4.1. Intelligence data .................................................. 36
   4.2. Law enforcement data ........................................... 37
   4.3. US–EU adequacy arrangements: from Safe Harbour to Privacy Shield ......................................................... 40
   4.4. Protection of the negotiation process by the estoppel principle ..... 43
5. An international treaty as a better solution for this dilemma? .... 44
6. Use of derogations as additional safeguards for data exchange due to the insufficiently solved data exchange question ........... 46
7. Conclusions .............................................................. 47

3. The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data
David LINDSAY .............................................................. 49

1. Introduction .............................................................. 49
2. Proportionality under EU law ........................................ 51
3. Proportionality and EU data privacy law ............................. 54
4. The Snowden revelations and the PRISM programme ............ 59
5. The Schrems decision ................................................... 61
   5.1. Background ......................................................... 61
   5.2. The CJEU ruling ................................................ 63
6. Legal evaluation of the Schrems decision ............................. 68
7. Proportionality, privacy rights and democracy ....................... 69
8. Proportionality, trans-Atlantic and transborder data flows ......... 72
9. The 'Privacy Shield' and proportionality ............................... 74
10. Conclusion .............................................................. 82

4. US Surveillance Law, Safe Harbour and Reforms Since 2013
Peter SWIRE .............................................................. 85

1. Introduction .............................................................. 85
2. The fundamental equivalence of the United States and EU Member States as constitutional democracies under the rule of law ........... 86
   2.1. The United States is a constitutional democracy under the rule of law ......................................................... 88
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.</td>
<td>Fundamental protections related to law enforcement surveillance</td>
<td>89</td>
</tr>
<tr>
<td>2.3.</td>
<td>Fundamental protections related to national security surveillance</td>
<td>91</td>
</tr>
<tr>
<td>2.4.</td>
<td>Conclusion</td>
<td>93</td>
</tr>
<tr>
<td>3.</td>
<td>The section 702 PRISM and Upstream programmes are reasonable and lawful responses to changing technology</td>
<td>94</td>
</tr>
<tr>
<td>3.1.</td>
<td>The legal structure of section 702</td>
<td>96</td>
</tr>
<tr>
<td>3.2.</td>
<td>The PRISM programme is not a bulk collection programme</td>
<td>98</td>
</tr>
<tr>
<td>3.3.</td>
<td>The Upstream programme accesses fewer electronic communications than PRISM</td>
<td>101</td>
</tr>
<tr>
<td>3.3.1.</td>
<td>How the Upstream technology works</td>
<td>102</td>
</tr>
<tr>
<td>3.3.2.</td>
<td>Judge Bates’ declassified opinion about section 702 illustrates judicial oversight of NSA surveillance</td>
<td>105</td>
</tr>
<tr>
<td>3.4.</td>
<td>Conclusion</td>
<td>106</td>
</tr>
<tr>
<td>4.</td>
<td>The US has taken multiple and significant actions to reform surveillance laws and programmes since 2013</td>
<td>106</td>
</tr>
<tr>
<td>4.1.</td>
<td>Independent reviews of surveillance activities</td>
<td>106</td>
</tr>
<tr>
<td>4.1.1.</td>
<td>Review Group on Intelligence and Communications Technology</td>
<td>107</td>
</tr>
<tr>
<td>4.1.2.</td>
<td>Privacy and Civil Liberties Oversight Board</td>
<td>108</td>
</tr>
<tr>
<td>4.2.</td>
<td>Legislative actions</td>
<td>109</td>
</tr>
<tr>
<td>4.2.1.</td>
<td>Increased funding for the PCLOB</td>
<td>109</td>
</tr>
<tr>
<td>4.2.2.</td>
<td>Greater judicial role in section 215 orders</td>
<td>109</td>
</tr>
<tr>
<td>4.2.3.</td>
<td>Prohibition on bulk collection under section 215 and other laws</td>
<td>110</td>
</tr>
<tr>
<td>4.2.4.</td>
<td>Addressing the problem of secret law – declassification of FISC decisions, orders and opinions</td>
<td>110</td>
</tr>
<tr>
<td>4.2.5.</td>
<td>Appointment of experts to brief the FISC on privacy and civil liberties</td>
<td>111</td>
</tr>
<tr>
<td>4.2.6.</td>
<td>Transparency reports by companies subject to court orders</td>
<td>112</td>
</tr>
<tr>
<td>4.2.7.</td>
<td>Transparency reports by the US government</td>
<td>114</td>
</tr>
<tr>
<td>4.2.8.</td>
<td>Passage of the Judicial Redress Act</td>
<td>115</td>
</tr>
<tr>
<td>4.3.</td>
<td>Executive branch actions</td>
<td>115</td>
</tr>
<tr>
<td>4.3.1.</td>
<td>New surveillance principle to protect privacy rights outside of the US</td>
<td>117</td>
</tr>
<tr>
<td>4.3.2.</td>
<td>Protection of civil liberties in addition to privacy</td>
<td>117</td>
</tr>
<tr>
<td>4.3.3.</td>
<td>Safeguards for the personal information of all individuals, regardless of nationality</td>
<td>117</td>
</tr>
<tr>
<td>4.3.4.</td>
<td>Retention and dissemination limits for non-US persons similar to US persons</td>
<td>118</td>
</tr>
</tbody>
</table>
4.3.5. Limits on bulk collection of signals intelligence. ............ 119
4.3.6. Limits on surveillance to gain trade secrets
for commercial advantage .................................. 120
4.3.7. New White House oversight of sensitive intelligence
collection, including of foreign leaders ..................... 120
4.3.8. New White House process to help fix software flaws
rather than use them for surveillance ....................... 121
4.3.9. Greater transparency by the executive branch
about surveillance activities .......................... 122
4.3.10. Creation of the first NSA civil liberties and privacy
office ............................................................ 123
4.3.11. Multiple changes under section 215 ......................... 123
4.3.12. Stricter documentation of the foreign intelligence
basis for targeting under section 702 ......................... 124
4.3.13. Other changes under section 702 ......................... 124
4.3.14. Reduced secrecy about national security letters ............ 125
4.4. Conclusion ................................................. 126

INVITED COMMENTS

5. The Paper Shield: On the Degree of Protection of the EU–US Privacy
Shield against Unnecessary or Disproportionate Data Collection
by the US Intelligence and Law Enforcement Services
Gert VERMEULEN .............................................. 127

1. Background: inadequacy of the US data protection regime:
clear to everyone after Snowden .................................. 127
2. Safe Harbour unsafe ........................................ 130
3. Safe Harbour is dead ........................................ 132
4. Long live the Privacy Shield! .................................. 135
5. Limitations and safeguards regarding data collection in the interest
of national security ........................................ 137
   5.1. Collection and access versus access and use: one big
        amalgamation ........................................ 137
   5.2. Bulk collection remains possible ........................ 140
   5.3. Access and use do not comply with strict necessity
        and proportionality requirements ..................... 142
   5.4. Ombudsperson ........................................ 145
6. Limitations and safeguards regarding data collection in the interest
of law enforcement or public interest ........................ 146
7. Conclusion .................................................. 147
6. International Data Transfers in Brazil
   Danilo Doneda ................................................................. 149

1. Introduction ................................................................. 149
2. The situation in Brazil and Latin America ......................... 149
3. Elements of regulation of international data transfers in Brazil . 152
4. Conclusion ................................................................... 155

SECTION II
PRIVACY AND INTERNATIONAL TRADE

7. From ACTA to TTIP: Lessons Learned on Democratic Process
   and Balancing of Rights
   Trisha Meyer and Agnieszka Vetulani-Cęgiel ....................... 159

1. Introduction ................................................................. 159
   1.1. Anti-Counterfeiting Trade Agreement .......................... 160
   1.2. Transatlantic Trade and Investment Partnership .......... 162
2. Participatory turn ........................................................... 164
   2.1. Problem definition .................................................... 164
   2.2. European Commission principles of good governance .... 165
       2.2.1. Anti-Counterfeiting Trade Agreement .................. 166
       2.2.2. Transatlantic Trade and Investment Partnership .... 168
3. Balancing of rights ......................................................... 170
   3.1. Problem definition .................................................... 170
       in Bilateral and Regional Agreements .......................... 171
       3.2.1. Anti-Counterfeiting Trade Agreement .................. 172
       3.2.2. Transatlantic Trade and Investment Partnership .... 175
4. Conclusion ................................................................... 177

8. Free Trade Agreements and Data Privacy: Future Perils
   of Faustian Bargains
   Graham Greenleaf ............................................................ 181

1. Introduction – bargaining with privacy rights .................... 181
   1.1. The USA’s forum-shifting on personal data exports ........ 182
   1.2. Data privacy agreements: not bananas ........................ 183
2. FTAs and data privacy prior to 2016 – a quiescent past ......... 185
   2.1. GATS exception and unpredictable WTO jurisprudence .. 185
   2.2. Regional trade agreements – examples ....................... 187
       2.2.1. SAARC trade agreements ................................. 188
       2.2.2. ASEAN trade agreements (ASEANFAS and AANZFTA) . 188
       2.2.3. Latin America – the Pacific Alliance agreement .... 189
2.3. The impact of multilateral FTAs on privacy prior to 2016 .......... 190
present danger ................................................................. 190
  3.1. The parties, now and future: nearly all of APEC, perhaps
       beyond ................................................................. 191
  3.2. Scope includes any measures affecting trade ...................... 193
  3.3. Vague and unenforceable requirements for personal information
       protection ................................................................. 193
  3.4. Direct marketing limitations ........................................ 196
  3.5. Restrictions on data export limitations ............................ 196
  3.6. Prohibitions on data localisation ................................... 197
  3.7. Dispute settlement .................................................. 198
  3.8. The spectre of ISDS ................................................... 199
  3.9. The TPP as an anti-privacy precedent .............................. 200
4. FTAs in progress: the veil of secrecy, lifted in part .............. 202
  4.1. Trade in Services Agreement (TISA) – potentially
       the broadest FTA ....................................................... 203
  4.2. FTAs involving the EU – unusual openness and privacy
       constraints ............................................................... 205
      4.2.1. Transatlantic Trade and Investment Partnership (TTIP) –
            the EU/USA FTA ................................................ 206
      4.2.2. EU–Canada Comprehensive Economic and Trade
            Agreement (CETA) ............................................. 208
  4.3. Regional Comprehensive Economic Partnership (RCEP) –
       a TPP alternative or complement ................................ 209
  4.4. Pacific Agreement on Closer Economic Relations (PACER)
       Plus – a privacy opportunity? ..................................... 209
5. Conclusions: future FTAs, the fog of trade and national privacy
   laws – Faustian bargains? ............................................. 210

INVITED COMMENT

9. Nine Takeaways on Trade and Technology
   Marietje SchAAKE .................................................... 213

   1. No old-school trade – views to address the digital economy
      of the future ........................................................... 213
   2. Trade negotiations can learn from Internet governance .............. 214
   3. Don’t panic! Proposals in negotiations are not final texts .......... 215
   4. Data flows have a legitimate place in 21st-century trade agreements,
      but this does not mean our privacy will be destroyed ............ 215
   5. Trade agreements can improve digital rights ........................ 216
   6. Strengthening digital trade is not just a question of data flows .... 216
7. The possibility of setting information and communications technologies standards in trade agreements should be explored. .... 217
8. Discussions at bilateral and multilateral levels are moving, more should be done at the WTO. ................................. 217
9. Lessons from ACTA are still relevant .............................. 218

SECTION III
PRIVACY AND TERRITORIAL APPLICATION OF THE LAW

10. Extraterritoriality in the Age of the Equipment-Based Society: Do We Need the ‘Use of Equipment’ as a Factor for the Territorial Applicability of the EU Data Protection Regime? Michał Czerniawski .................................................. 221
1. Introduction .............................................................. 221
2. Territorial scope of the Data Protection Directive .................. 224
3. Role of ‘equipment’ criterion in practice ............................ 231
4. Article 3(2) of the General Data Protection Regulation ............ 234
   4.1. General description .................................................. 234
   4.2. Possible impact on the EU–US data privacy relationships .... 236
5. Conclusion .................................................................. 239

11. Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds
Heidi Beate Bentzen and Dan Jerker B. Svanstesson .................. 241
1. Introduction .............................................................. 241
2. DNA in the clouds – the basics ....................................... 242
   2.1. How and why DNA data is used ................................. 242
   2.2. Why cloud? .......................................................... 244
3. Why it is so important to find legal solutions in this field ......... 246
4. Entering the international arena – public, and private, international law ......................................................... 250
   4.1. Public international law: the not so golden triangle: sovereignty, territoriality and jurisdiction .............. 251
   4.2. Private international law ............................................. 253
       4.2.1. Where disputes should be settled ....................... 253
       4.2.2. Applicable law .................................................. 254
5. Contours of a solution .................................................. 256
   5.1. The limits of territoriality ........................................... 256
   5.2. Harmonisation ....................................................... 257
   5.3. Better relation between regulation and technology .......... 258
   5.4. Risk mitigation ....................................................... 258
Contents

5.5. Education ................................................................. 259
5.6. Balance of responsibilities ........................................... 259
6. Concluding remarks ....................................................... 260

SECTION IV
PRIVACY AND CRIME

12. Regulating Economic Cyber-Espionage among States
under International Law
Maša Kovič Dine .............................................................. 263

1. Introduction ................................................................. 263
2. Legality of espionage under international law .................... 264
   2.1. Traditional espionage and international law ............... 264
   2.2. Definition of economic cyber-espionage/exploitation .... 268
3. Special characteristics of economic cyber-exploitation .......... 270
4. Economic cyber-exploitation and privacy considerations
   at the international level ............................................... 272
5. Economic cyber-espionage and the TRIPS Agreement .......... 276
6. Act of pillage ............................................................... 279
7. Economic cyber-exploitation among states ....................... 282
8. Conclusion ................................................................. 285

INVITED COMMENTS

13. Terrorism and Paedophilia on the Internet: A Global and Balanced
    Cyber-Rights Response Is Required to Combat Cybercrime,
    Not Knee-Jerk Regulation
Felicity Gerry QC ............................................................ 287

1. Introduction ............................................................... 287
2. Cyber-communication ................................................... 288
3. Cyber rights ............................................................... 290
4. Cyber freedom ........................................................... 292
5. Cyber regulation .......................................................... 294
6. Cyber surveillance ......................................................... 295
7. Cyber change .............................................................. 296
8. Cyber law ................................................................. 297
9. Cyber protection .......................................................... 301
10. Conclusion ................................................................. 302

14. Understanding the Perpetuation of ‘Failure’: The 15th Anniversary
    of the US Terrorist Finance Tracking Programme
Anthony Amicelle ............................................................. 305

xxx
Interentia
## SECTION V
PRIVACY AND TIME

### INVITED COMMENTS

   Iván Székely ................................................................. 313

   1. The legal landscape .................................................. 314
   2. Converging technologies, diverging policies .................... 316
   3. Prospects for the future deceased .................................. 319

16. **The Right to be Forgotten, from the Trans-Atlantic to Japan**
   Hiroshi Miyashita .......................................................... 321

   1. The trans-Atlantic debate ............................................. 321
   2. Judicial decisions in Japan ......................................... 322
      2.1. For the right to be forgotten .................................. 322
      2.2. Against the right to be forgotten ............................ 323
   3. Delisting standard .................................................... 323
      3.1. Torts and right to be forgotten ............................... 323
      3.2. Balancing ........................................................ 324
      3.3. Standard-making ................................................ 325
   4. Technical issues ..................................................... 326
   5. Legislative debate .................................................. 327
   6. Time and privacy ................................................... 328

### PART II
THEORY OF PRIVACY

17. **Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing)**
   Jakub Míšek ................................................................. 331

   1. Introduction .......................................................... 331
      1.1. Definition of personal data ..................................... 332
      1.2. Hyperlink and personal data ................................... 336
         1.2.1. Hyperlink as personal data ............................... 337
         1.2.2. Hyperlink as personal data processing .................. 338
         1.2.3. Comparison of the two approaches and their consequences .............................................. 340
         1.2.4. Practical example .......................................... 342
      1.3. Discussion and conclusion .................................... 343
18. Big Data and ‘Personal Information’ in Australia, the European Union and the United States
Alana MAURUSHAT and David VAILE ............................................ 347

1. Introduction ................................................................. 347
2. Big data, de-identification and re-identification ......................... 349
3. Definitions of information capable of identifying a person .......... 351
   3.1. ‘Personal Information’ (PI) in Australia ....................... 352
       3.1.1. OAIC Australian Privacy Principles Guidelines .......... 353
       3.1.2. Factors affecting ‘identifiability’ and reasonableness ...... 354
       3.1.3. ‘Not reasonably identifiable’ – guidance? ............... 357
       3.1.4. Consideration of the scope of ‘personal information’ ...... 358
   3.2. ‘Personal Information’ (PI) in the APEC Privacy Framework ... 360
   3.3. ‘Personally Identifying Information’ (PII) in the US .......... 361
       3.3.1. HIPAA ............................................................ 363
       3.3.2. Office of Management and Budget ....................... 364
       3.3.3. Data breach .................................................... 365
       3.3.4. Children’s Online Privacy Protection Act ................. 365
   3.4. De-identification .................................................... 366
   3.5. ‘Personal Data’ (PD) in Europe and the OECD ......... 367
       3.5.1. CoE Convention 108 .......................................... 367
       3.5.2. OECD Privacy Framework ................................. 368
       3.5.3. EU Data Protection Directive ............................. 368
       3.5.4. EU e-Privacy Directive .................................... 370
       3.5.5. Article 29 Data Protection Working Party Guidance ...... 370
       3.5.6. National implementation example: UK Data Protection Act 1998 ......................................................... 373
       3.5.7. New EU General Data Protection Regulation ............ 374
4. Comparing the frameworks ................................................. 376
   4.1. Australia and US ...................................................... 376
   4.2. Australia and EU ...................................................... 376
   4.3. US and EU ............................................................. 377
5. Concluding remarks ........................................................ 378

Stephen WILSON ................................................................. 379

1. Introduction ................................................................. 379
2. What engineers understand about privacy ................................ 380
3. Reorientating how engineers think about privacy ...................... 382
   3.1. Privacy is not secrecy ............................................... 383
   3.2. Defining personal information ................................. 384
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3. Indirect collection</td>
<td>385</td>
</tr>
<tr>
<td>4. Big Data and privacy</td>
<td>386</td>
</tr>
<tr>
<td>4.1. ‘DNA hacking’</td>
<td>387</td>
</tr>
<tr>
<td>4.2. The right to be forgotten</td>
<td>388</td>
</tr>
<tr>
<td>4.3. Security meets privacy</td>
<td>389</td>
</tr>
<tr>
<td>5. Conclusion: rules to engineer by</td>
<td>390</td>
</tr>
</tbody>
</table>

20. It’s All about Design: An Ethical Analysis of Personal Data Markets
Sarah Spiekermann                                                       | 391  |

1. A short utilitarian reflection on personal data markets              | 393  |
  1.1. Financial benefits                                              | 393  |
  1.2. Knowledge and power                                              | 393  |
  1.3. Belongingness and quality of human relations                     | 394  |
2. A short deontological reflection on personal data markets            | 396  |
3. A short virtue-ethical reflection on personal data markets            | 400  |
4. Conclusion                                                           | 403  |

PART III
ALTERNATIVE APPROACHES TO THE PROTECTION OF PRIVACY

Mary Julia Emanuel                                                       | 407  |

1. Introduction                                                         | 407  |
  1.1. A brief history of US privacy policy                             | 409  |
  1.2. A brief history European privacy policy                          | 411  |
  1.3. The dangers of surveillance                                     | 412  |
  1.4. Recognising privacy as a societal concern                        | 413  |
2. Three proposals based on concepts of American environmental policy   | 415  |
  2.1. Right-to-know                                                    | 416  |
    2.1.1. The Emergency Planning and Community Right-to-Know Act of 1986 | 416  |
    2.1.2. Establishing the right-to-know in the data protection arena  | 417  |
    2.1.3. Evaluation of relevant US policy                             | 418  |
    2.1.4. Evaluation of relevant EU policy                             | 418  |
  2.2. Impact assessments                                               | 419  |
    2.2.1. The National Environmental Policy Act of 1970               | 419  |
    2.2.2. NEPA as a model for privacy impact assessment                | 420  |
    2.2.3. Evaluation of relevant US policy                             | 421  |
2.2.4. Evaluation of relevant EU policy ........................................... 421
2.3. Opt-in privacy policy ............................................................... 422
  2.3.1. Mineral rights and the value of ‘opting in’ ............................. 422
  2.3.2. Consumer benefits from data collection ............................... 423
  2.3.3. Evaluation of relevant US policy ...................................... 425
  2.3.4. Evaluation of relevant EU policy ...................................... 425
3. Conclusion ................................................................. 426

22. Flagrant Denial of Data Protection: Redefining the Adequacy Requirement
Els De Busser ................................................................. 429
  1. Point of departure ............................................................... 429
  2. Reasons for using extradition in redefining adequacy ............... 431
     2.1. Interstate cooperation ..................................................... 432
     2.2. Protected interests and human rights ................................ 433
     2.3. Trust ........................................................................... 436
     2.4. Jurisprudence ............................................................... 436
  3. Using the perimeters of extradition for data protection ........... 437
     3.1. Avoidance strategies ....................................................... 438
        3.1.1. Negated and assumed adequacy ................................ 438
        3.1.2. Assurances ............................................................... 439
        3.1.3. Legal remedies ......................................................... 442
        3.1.4. Evidence ................................................................ 442
     3.2. Real risk ....................................................................... 443
     3.3. New limit for the adequacy requirement ............................ 446
  4. Conclusion: a flagrant denial of data protection ...................... 447

23. A Behavioural Alternative to the Protection of Privacy
Dariusz Kloza ................................................................. 451
  1. Introduction ................................................................. 451
  2. Tools for privacy protection .................................................. 459
     2.1. Regulatory tools ............................................................ 459
        2.1.1. Legal tools ............................................................. 459
        2.1.2. Not only law regulates ............................................. 466
     2.2. Beyond regulation .......................................................... 467
        2.2.1. Organisational protections .................................... 467
        2.2.2. Technological protections ..................................... 471
  3. Inadequacies of contemporarily available tools for privacy protection .. 473
     3.1. Introduction: irreversibility of harm ................................ 473
     3.2. Inadequacies ................................................................. 476
        3.2.1. Regulatory tools ..................................................... 476
3.2.2. Organisational tools ................................................. 487
3.2.3. Technological tools ................................................. 489

4. The behavioural alternative ............................................. 491
4.1. History ........................................................................ 491
4.2. Typology ...................................................................... 493
4.3. Implications .................................................................. 498
   4.3.1. Characteristics ......................................................... 498
   4.3.2. Conditions .............................................................. 499
   4.3.3. Problems .............................................................. 502

5. Conclusion ...................................................................... 504

24. The Future of Automated Privacy Enforcement
   Jake Goldenfein ................................................................. 507

   1. Characterising contemporary law enforcement surveillance .... 508
   2. The utility of existing legal mechanisms ............................ 509
   3. Articulation into infrastructure .......................................... 510
   4. Automated privacy enforcement ........................................ 511
   5. Questions for further research ........................................... 517
   6. Conclusion ...................................................................... 519

   Paul De Hert and Vagelis Papakonstantinou ............................. 521

   1. Introduction .................................................................... 521
   2. The deficit in global cooperation for the protection of data privacy .......................... 523
   3. Past and recent UN initiatives in the data privacy field ............ 526
   4. Suggesting the establishment of a new, specialised UN agency on data privacy .......... 527
   5. The WIPO model as useful guidance towards the establishment of a UN system for the global protection of data privacy .................. 529
   6. Conclusion ...................................................................... 531

INVITED COMMENT

26. Convention 108, a Trans-Atlantic DNA?
   Sophie Kwasny ................................................................. 533

   1. Convention 108, trans-Atlantic at birth ............................. 534
   2. Definitely more trans-Atlantic 30 years later ...................... 535
      2.1. Canada ................................................................. 535
## Contents

2.2. Mexico ............................................. 535  
2.3. Uruguay ......................................... 536  
2.4. United States .................................... 536  
2.5. The Ibero-American network of data protection authorities  
\((Red\ Iberoamericana\ de\ proteccion\ de\ datos)\) ................. 537  
3. A new landscape: the Committee of Convention 108 .................. 538  
4. To ultimately transcend all borders ......................... 538  
5. Conclusion ...................................... 540  

### CONCLUSION

27. Landscape with the Rise of Data Privacy Protection  
Dan Jerker B. Svantesson and Dariusz Kloza ................. 545  

1. Introduction ..................................... 545  
2. General observations ................................ 546  
   2.1. Novelty of the concept of data privacy and a growing nature  
        thereof. ........................................... 546  
   2.2. The rapid and continuous change of data privacy, its diagnoses  
        and solutions ...................................... 548  
   2.3. Entanglement of data privacy in the entirety of trans-Atlantic  
        relations ......................................... 553  
   2.4. Intermezzo: audiatur et altera pars ......................... 553  
3. Specific observations .................................. 554  
   3.1. Regulation of cross-border data flows ................. 554  
   3.2. Territorial reach of data privacy law ................. 557  
   3.3. Free trade agreements and data privacy ................. 559  
   3.4. Regulation of encryption .......................... 561  
   3.5. Regulation of whistle-blowing ......................... 562  
4. A few modest suggestions as to the future shape of trans-Atlantic  
   data privacy relations .............................. 564
## LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AANZFTA</td>
<td>ASEAN–Australia–New Zealand Free Trade Area</td>
</tr>
<tr>
<td>ACTA</td>
<td>Anti-Counterfeiting Trade Agreement</td>
</tr>
<tr>
<td>AEPD</td>
<td>Agencia Española de Protección de Datos</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>API</td>
<td>Advance Passenger Information</td>
</tr>
<tr>
<td>APP</td>
<td>Australian Privacy Principle</td>
</tr>
<tr>
<td>ASD</td>
<td>Australian Signals Directorate</td>
</tr>
<tr>
<td>ASEAN</td>
<td>Association of South East Asian Nations</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules</td>
</tr>
<tr>
<td>BD</td>
<td>big data</td>
</tr>
<tr>
<td>CETA</td>
<td>Comprehensive Economic and Trade Agreement</td>
</tr>
<tr>
<td>CFR</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>CISA</td>
<td>Convention Implementing the Schengen Agreement</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>CMPPA</td>
<td>Computer Matching and Privacy Protection Act [US]</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>COPPA</td>
<td>Children's Online Privacy Protection Act [US]</td>
</tr>
<tr>
<td>CPDP</td>
<td>Computers, Privacy and Data Protection conference</td>
</tr>
<tr>
<td>CPO</td>
<td>chief privacy officer</td>
</tr>
<tr>
<td>Cth</td>
<td>Commonwealth [Australia]</td>
</tr>
<tr>
<td>DG</td>
<td>Directorate-General (of the European Commission)</td>
</tr>
<tr>
<td>DNA</td>
<td>deoxyribonucleic acid</td>
</tr>
<tr>
<td>DPD</td>
<td>Data Protection Directive</td>
</tr>
<tr>
<td>DPIA</td>
<td>data protection impact assessment</td>
</tr>
<tr>
<td>DPO</td>
<td>data protection officer</td>
</tr>
<tr>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>DSM</td>
<td>Digital Single Market</td>
</tr>
<tr>
<td>DTC</td>
<td>direct-to-consumer</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECJ</td>
<td>European Court of Justice (former name of CJEU)</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>EFTA</td>
<td>European Free Trade Agreement</td>
</tr>
<tr>
<td>EIS</td>
<td>environmental impact statement</td>
</tr>
<tr>
<td>EP</td>
<td>European Parliament</td>
</tr>
<tr>
<td>EPAL</td>
<td>Enterprise Privacy Authorisation Language</td>
</tr>
<tr>
<td>ETS</td>
<td>European Treaty Series</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FISA</td>
<td>Foreign Intelligence Surveillance Act</td>
</tr>
<tr>
<td>FISC</td>
<td>Foreign Intelligence Surveillance Court</td>
</tr>
<tr>
<td>FoI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>FONSI</td>
<td>finding of no significant impact</td>
</tr>
<tr>
<td>FTA</td>
<td>free trade agreement</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission [US]</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office [US]</td>
</tr>
<tr>
<td>GATS</td>
<td>General Agreement on Trade in Services</td>
</tr>
<tr>
<td>GCHQ</td>
<td>Government Communications Headquarters</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HIPPA</td>
<td>Health Insurance Portability and Accountability Act [US]</td>
</tr>
<tr>
<td>HTML</td>
<td>HyperText Markup Language</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as Service</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>IATA</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>ICC</td>
<td>International Criminal Court</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICDPPC</td>
<td>International Conference of Data Protection and Privacy Commissioners</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communications technologies</td>
</tr>
<tr>
<td>IDPC</td>
<td>Irish Data Protection Commissioner</td>
</tr>
<tr>
<td>ILO</td>
<td>International Labor Organization</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Mail Access Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>intellectual property</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPR</td>
<td>intellectual property rights</td>
</tr>
<tr>
<td>ISDS</td>
<td>investor-state dispute settlement</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>JHA</td>
<td>Justice and Home Affairs</td>
</tr>
<tr>
<td>LEA</td>
<td>law enforcement agency</td>
</tr>
<tr>
<td>MEP</td>
<td>Member of European Parliament</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>NAFTA</td>
<td>North American Free Trade Agreement</td>
</tr>
<tr>
<td>NEPA</td>
<td>National Environmental Policy Act</td>
</tr>
<tr>
<td>NGO</td>
<td>non-governmental organisation</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology [US]</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSL</td>
<td>National Security Letter</td>
</tr>
<tr>
<td>OAIC</td>
<td>Office of Australian Information Commissioner</td>
</tr>
<tr>
<td>ODNI</td>
<td>Office of the Director of National Intelligence</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization of Economic Cooperation and Development</td>
</tr>
<tr>
<td>OJ</td>
<td>Official Journal</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget [US]</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as Service</td>
</tr>
<tr>
<td>PACER</td>
<td>Pacific Agreement on Closer Economic Relations</td>
</tr>
<tr>
<td>PbD</td>
<td>Privacy by Design</td>
</tr>
<tr>
<td>PCLOB</td>
<td>Privacy and Civil Liberties Oversight Board</td>
</tr>
<tr>
<td>PD</td>
<td>personal data</td>
</tr>
<tr>
<td>PET</td>
<td>Privacy Enhancing Technologies</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PI</td>
<td>personal information</td>
</tr>
<tr>
<td>PIA</td>
<td>privacy impact assessment</td>
</tr>
<tr>
<td>PII</td>
<td>personally identifiable information</td>
</tr>
<tr>
<td>PNR</td>
<td>passenger name record</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol 3</td>
</tr>
<tr>
<td>PPD</td>
<td>Presidential Policy Directive</td>
</tr>
<tr>
<td>RCEP</td>
<td>Regional Comprehensive Economic Partnership</td>
</tr>
<tr>
<td>RFID</td>
<td>radio-frequency identification</td>
</tr>
<tr>
<td>RTBF</td>
<td>right to be forgotten</td>
</tr>
<tr>
<td>SAARC</td>
<td>South Asia Area of Regional Cooperation</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as Service</td>
</tr>
<tr>
<td>SIGINT</td>
<td>signal intelligence</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for Worldwide Interbank Financial Telecommunication</td>
</tr>
<tr>
<td>TAMI</td>
<td>Transparent Accountable Data Mining Initiative</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>TFTP</td>
<td>Terrorist Finance Tracking Programme</td>
</tr>
<tr>
<td>TISA, TiSA</td>
<td>Trade in Services Agreement</td>
</tr>
<tr>
<td>TPP</td>
<td>Trans-Pacific Partnership</td>
</tr>
<tr>
<td>TRIMS</td>
<td>Trade Related Investment Measures</td>
</tr>
<tr>
<td>TRIPS</td>
<td>Agreement on Trade-Related Aspects of Intellectual Property Rights</td>
</tr>
<tr>
<td>TTIP</td>
<td>Transatlantic Trade and Investment Partnership</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
</tr>
</tbody>
</table>
List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UKSC</td>
<td>United Kingdom Supreme Court</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>URL</td>
<td>uniform resource locator</td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>VIS</td>
<td>Visa Information System</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organization</td>
</tr>
<tr>
<td>WP29</td>
<td>Article 29 Working Party</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organisation</td>
</tr>
<tr>
<td>XACML</td>
<td>eXtensible Access Control Markup Language</td>
</tr>
</tbody>
</table>