CONCLUSION
27. LANDSCAPE WITH THE RISE OF DATA PRIVACY PROTECTION

Dan Jerker B. SVANTESSON* and Dariusz KLOZA**

1. INTRODUCTION

It’s true that not a day passes without new pieces of paper entering the Registry, papers referring to individuals of the male sex and of the female sex who continue to be born in the outside world ....

José Saramago, All the Names (1997)¹

... a splash quite unnoticed this was Icarus drowning

William C. Williams, ‘Landscape with the fall of Icarus’ (1962)²

Perhaps the most common interpretation of Pieter Bruegel the Elder’s painting Landscape with the fall of Icarus highlights popular ignorance of and indifference to the drowning of Icarus.³ In Greek mythology, Daedalus and his son Icarus attempted to fly with the aid of wings they had made of both feathers and wax. Icarus recklessly flew too close to the sun, his wings melted and he drowned in the sea.⁴ In Bruegel’s painting, Icarus has already fallen, but he and his sad fate are hardly noticed. He disappears in the richness of the landscape shown, the crew

of a ship sailing by has not reacted to his fall and – as Bruegel’s contemporary fellows would have said – the farmer goes on ploughing.\(^5\)

Despite both the authenticity of the painting and its dominant interpretation being questioned,\(^6\) we have found this masterpiece of Bruegel a suitable allegory for our concluding idea for this book. The underlying observation that stands out from our reading of the foregoing 26 chapters to this volume is that of the entanglement of data privacy in the entirety of trans-Atlantic relations. Yet we have observed that in these relations the protection of data privacy – to a large extent – recklessly falls victim of ignorance and indifference, similarly to the fate of Icarus as painted by Bruegel.

We have explained in our Preface that our main impetus for this book had been the Snowden affair. We have aimed with this book to explore the status quo of trans-Atlantic data privacy relations challenging the notions of democracy, the rule of law (Rechtsstaat) and fundamental rights. The resulting anthology gives a snapshot of the ‘hottest’ issues as they look at the end of 2016. Hanneke Beaumont’s sculpture Stepping Forward – seen as an allegory of a brave leap of faith into the unknown – gave further impetus to reflect also on the future of these relations.\(^7\) We have thus re-read this book, spotted ‘hot’ topics and added a few of our own comments, ultimately offering a few modest suggestions as to the future of trans-Atlantic data privacy relations. Therefore, following the popular interpretation of Bruegel’s masterpiece – with the kind permission of the Musées royaux des Beaux-Arts de Belgique – we have reproduced Landscape with the fall of Icarus on the front cover of this book. As a clin d’œil, we have titled this concluding chapter ‘Landscape with the Rise of Data Privacy Protection’.

2. GENERAL OBSERVATIONS

2.1. NOVELTY OF THE CONCEPT OF DATA PRIVACY AND A GROWING NATURE THEREOF

A number of themes stand out when reading the 26 contributions we have had the pleasure of working with. Let us begin with a few all-encompassing observations.

\(^5\) This phrase in Dutch – ‘… en boer, hij ploegde voort’ (‘… and the farmer, he went on ploughing’) – popularised by a 1935 Werumeus Buning’s poem Ballade van den boer, has become in the Low Countries a widely accepted proverb pointing out people’s ignorance. Cf. Johan W.F. Werumeus Buning, Verzamelde gedichten, Querido, Amsterdam 1970, pp. 185–187.


\(^7\) Cf. Preface, in this volume.
The underlying reflection about data privacy is that of the dynamism of this concept. It might sound trivial prima facie – in fact, many aspects of life are dynamic – but this dynamism is caused by the relative novelty of data privacy, its uncharted scope and expeditiously growing nature. In terms of the law, the legal conceptualisation of data privacy is only 40–50 years old. This book confirms that many aspects thereof have not yet matured, and this includes even the very basic definitions. For example, having read the chapters of Mišek, Maurushat & Vaile and Wilson, we cannot help but recall the 2003 landmark judgment of the Court of Justice of the European Union (CJEU) in Lindqvist, delimitating the scope of European data privacy law, its 2016 decision in Breyer, ruling on the grounds of the 1995 Data Protection Directive that a dynamic Internet protocol (IP) address constitutes personal data, or the pending, very similar case before the Federal Court of Australia that is to decide whether, on the grounds of the Privacy Act 1988 (Cth), ‘personal information’ includes metadata. Higher-level courts are repeatedly being asked for authoritative definitions and this phenomenon has become frequent in the privacy universe.

We have started in the Preface with a story on inspirations for this book. Yet beyond their usefulness for our purposes, such diverse events – judgments of senior courts, international treaties, legislation and political and societal developments at numerous levels – crystallise the definition of data privacy, its scope, legal construction and permissible and acceptable interferences. It is an ongoing discourse, i.e. a careful consideration, in which multiple and – quite often – opposing viewpoints meet, with a view to make a determination that might be applied in practice. In this way the conversation on data privacy is maturing. This body of knowledge on data privacy that is being created is a product of trial and error. All this leads to the continuous re-definition, re-conceptualisation and re-delineation of boundaries of data privacy and its protection. These developments help make clear, for example, whether and when global mass surveillance practices can be considered ‘OK’ (‘OK’ stands here for an umbrella term for ‘fair’, ‘ethically sound’, ‘optimal’, ‘just’, ‘acceptable’, etc.).

In the same Preface, we stated our ambition for this book not to be just another publication on the Snowden affaire. Yet as many as 12 out of 26 contributions in one way or another make reference to it and discuss the extent to which the affaire is capable of altering the privacy universe. Regardless of
its actual impact, the Snowden _affaire_ has inserted itself into the perspective on data privacy as a phenomenon developed in reaction to the many threats to individual and collective interests posed by global mass surveillance practices. All in all, the growth of ‘privacy’ as a concept owes much to the development of invasive technologies. It was the need to address the widespread popularity of photo cameras that inspired Warren and Brandeis in 1890 to coin their famous ‘right to be let alone’.\(^\text{13}\)

2.2. THE RAPID AND CONTINUOUS CHANGE OF DATA PRIVACY, ITS DIAGNOSES AND SOLUTIONS

However, this is not to say that once data privacy comes of age, it would from then on remain constant. On the contrary, the ever-changing nature of society, of its needs and desires, on the one hand, and of innovation and technology on the other, continuously necessitates a _re-think_ of the concept of data privacy and of the system of its protection. In the privacy universe, things change rapidly. Many commentators recall here Collingridge’s ‘dilemma of control’ – i.e. it is hard to regulate something so unpredictable as technology\(^\text{14}\) – and give evidence of the 1995 Data Protection Directive that ‘lived’ for only 21 years until the General Data Protection Regulation (GDPR)\(^\text{15}\) was passed (if we look at their respective enactment dates). The need up to keep pace with technological and societal developments necessitated the revision of the law.

To further illustrate our point: we finished the Preface to this book in early September 2016. This concluding chapter was written in late November 2016. (It was a conscious choice for us to re-visit all 26 submissions while the publisher was typesetting the book and, in parallel, to write these remarks.) Over the period of these two months, on the European side of the Atlantic alone, we have witnessed multiple events impacting trans-Atlantic data privacy relations, and these include:

- the lodging with the CJEU of two actions for annulment of the Privacy Shield framework on the grounds of its incompatibility with the EU fundamental rights (16 September\(^\text{16}\) and 25 October, respectively);\(^\text{17}\)

---


\(^\text{16}\) Case T-670/16, _Digital Rights Ireland v. Commission_, CJEU.

\(^\text{17}\) Case T-738/16, _La Quadrature du Net and Others v. Commission_, CJEU.
a Swiss referendum on the new surveillance law that has received 65.5 per cent of popular support; the federal government had argued that ‘the new measures would allow Switzerland to “leave the basement and come up to the ground floor by international standards”’ (25 September);18

the Investigatory Powers Tribunal in the United Kingdom ruling on the incompatibility of British mass surveillance practices between 1998 and 2015 with Art. 8 of the European Convention on Human Rights (ECHR)19 (17 October);

the Walloon initial veto to the proposed Comprehensive Economic and Trade Agreement (CETA) between the EU and Canada, predominantly due to the failure of negotiating process to satisfy democratic requirements (17 October);20 Belgium withdrew its veto on 27 October, having attached to CETA a declaration giving it certain agricultural concessions and – more importantly for our analysis – promising to refer to the CJEU the compatibility of CETA’s investor dispute settlement provisions with the EU Treaties, this including the Charter of Fundamental Rights;21

presidential elections in the US, after which, media speculate – the new administration might intensify global mass surveillance practices to the detriment of the principles of democracy, the rule of law and fundamental rights (8 October);22

the French Constitutional Council declaring the unconstitutionality of a key clause of the 2015 surveillance law,24 which had allowed wiretapping without oversight, since the provision in question constituted a ‘manifestly disproportionate infringement’ (21 October);25

---


– the UK passing into law the Investigatory Powers Act 2016, nicknamed ‘Snooper’s Charter’, whose surveillance provisions have been dubbed ‘draconian and too intrusive’ by civil liberties advocates (16 November).26

The solutions currently in place to protect individual and collective interests related to data privacy offer a sufficient degree of protection in many situations, yet in many other situations still more is needed. Further, where solutions are currently satisfactory, they might quickly become outdated. When this is the case, the need for more (or less) protection, if ever, must be first diagnosed. Such a diagnosis often indicates that something does not work. The many problems of data privacy are well known: ‘the kinds of mass surveillance Snowden has revealed at the NSA do not work and also carry major risks for ordinary citizens’27 or – to paraphrase Saramago from the epigraph – ‘not a day passes’ without businesses doing nasty things with their customers’ information.28 In their contributions to the present book, Kovič Dine observes a need for an ‘international response’ to economic cyber-exploitation among states, and Gerry – in a similar vein – criticises the lack of global arrangement for effectively fighting ‘cybercrime’. Finally, Amicelle joins the critics of global mass surveillance practices and – using the example of the US Terrorist Finance Tracking Programme – asking ‘why does this kind of security programme … persist regardless of failures to achieve the stated goals concerning terrorism? Positions concluding that something does work are much less popular, but nevertheless they exist (cf. Swire and Czerniawski).

Alternatively, such an analysis can suggest there is a gap that urgently needs to be filled. The passage of time, for example, seems to be such undiagnosed need for more (or alternatively – less) privacy protection. The reading of Székely questions whether and how much ‘privacy’ should be asserted for a person after their death? He even projects that comparisons would be made in a quest for ‘the best countries to conclude our lives, if we care about having continuing protection for our personality and privacy after death’. How much privacy should be provided to an individual when a piece of their personal information loses its societal relevance? Miyashita sheds light on the influence of European ‘right to be forgotten’ (or a ‘right to de-listing’)29 on the Japanese judiciary and concludes that ‘human beings forget, but the Internet does not. This is why forgetting is universally demanding as a legal right in the twenty-first century’.

---

28 Above n. 1.
29 Case C-121/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (CJEU, 13 May 2014).
Finally, Spiekermann makes, to our knowledge, the first comparative analysis of the ethical nature of personal data markets. There is scope for abuse when personal data are seen as an economic asset, generated by identities and individual behaviours, tradable in exchange for e.g. higher quality services and products. Having looked at them through the perspectives of utilitarianism, deontology and virtue-ethics, she diagnoses the critical need for ‘careful crafting of technical and organisational mechanisms’ of such markets. Such crafting must include a possibility to opt-out with no negative consequences in order for personal data markets to maintain their ethicality.

When the diagnosis is more mature, we observe that a wide spectrum of concrete proposals to increase the level of privacy protection has already been tabled. The bravest ideas include, for example, a plea to change the paradigm of cross-border transfers of personal data from ‘adequacy’ to a ‘flagrant denial of protection’; an adaptation of a ‘death row phenomenon’ ground for refusal, a concept well known in extradition law (De Busser). More modest ideas suggest looking at other branches of law and policy, especially in the area of environmental protection, for an inspiration on how to protect best the many aspects of data privacy. This plea emerged in the early 2000s (e.g. Nehf30 and Hirsh)31 and is renewed in this volume by Emanuel. Among her propositions, she argues for the US legal concept of ‘mineral rights’ in property to be adapted to the needs and reality of the privacy universe as it might increase individual choice and control over their personal data. Even though consumers are rewarded in pecuniary terms, ‘in exchange for collecting and selling their personal information’, she considers this approach fair as individuals ‘are consenting to the transaction and benefit from it’. Emanuel underlines the importance of choice in data privacy, whose consequences, for such a transaction, including their unpredictability, must be fully understood.

Further, Kloza makes a suggestion to acknowledge and explore a new, fourth category of privacy protections – behavioural – alongside the three categories already well established, i.e. regulatory (legal), organisational and technological. He claims existing arrangements do not offer enough protection and resorting to own behaviour would offer some consolation. Finally, Goldenfein evaluates the enforcement of data privacy by means of technology and – more concretely – by automation. He gives the examples of authorisation schemes such as the Enterprise Privacy Authorisation Language (EPAL) and semantic web technologies such as the Transparent Accountable Data Mining Initiative (TAMI). Although these particular approaches ‘have not materialised into

functional examples, he concludes this field is ‘still in its relative infancy’ and pleads for further ‘research into automation of legal rights’.

Others look for more formal solutions. For example, De Hert & Papakonstantinou argue for the creation of a body of the United Nations (UN) to foster data privacy protection at an international level. They extend their early proposal from 2013,32 arguing that only an international organisation is capable of effectively setting ‘the global tone and minimum level of protection’. They recall the UN involvement in data privacy protection from 1966 (i.e. the International Covenant on Civil and Political Rights)33 to the 1990 Guidelines concerning computerised personal data files34 and evaluate it as rather obsolete and insufficient. The UN commitment was renewed with the 2015 appointment of the first special rapporteur on the right to privacy35 and the adoption of the 2016 resolution on the right to privacy in the digital age.36 They argue the recently revived UN involvement could constitute a solid basis for the establishment of an international data privacy agency.

In her contribution to the present book, Kwasny struck the same chord as earlier e.g. Greenleaf37 and foresees that the Council of Europe’s ‘Convention 108’38 – from its inception open to any country in the world – could become a standard beyond the geographical borders of Europe. However, we agree with Kuner that realisation of any such proposition would be a laborious exercise, requiring many factors to be taken into consideration, e.g. form, contents and institutional set-up.39

2.3. ENTANGLEMENT OF DATA PRIVACY IN THE ENTIRETY OF TRANS-ATLANTIC RELATIONS

On a more conceptual level, we observe that data privacy is entangled with any aspect of trans-Atlantic relations. Be it national security or international trade, questions ranging from cross-border transfers of money with the aid of financial institutions to civil aviation to international trade, the provision of digital services or the enforcement of intellectual property rights would always raise an issue of data privacy. This is a direct consequence of globalisation and the growth of the quaternary economy, which runs on handling information. (Many have dubbed this phenomenon as ‘data’ being the ‘new oil’ or the ‘fourth industrial revolution’.)

In consequence, the governance of such relations always affects, to various degrees, the protection of data privacy. Its impact could be either direct (cf. e.g. 2016 Privacy Shield),\(^\text{40}\) either indirect (e.g. 2012 EU–US agreement on the use and transfer of Passenger Name Records).\(^\text{41}\) In the latter case, the main objective of an arrangement is different than the regulation of data privacy, but nevertheless, such an arrangement touches thereon. In any case, data privacy has become an indispensable ingredient of contemporary international relations. The question remains as to the level of protection of data privacy that could be afforded as a result of dynamics between multiple actors on the international arena.

2.4. INTERMEZZO: AUDIATUR ET ALTERA PARS\(^\text{42}\)

Finally, we have observed that a vast majority of contributions to this book diagnose some form of defect in trans-Atlantic data privacy relations and the authors of these contributions – either explicitly, either implicitly – argue for stronger protection of data privacy. Consequently, there are only few chapters that conclude the status quo of such relations is ‘OK’ and not much should be changed. (The contributions of Swire and Czerniawski stand out in this category. Yet the reader should note that nobody has argued for less data privacy.) Therefore, some readers might see this book as a form of advocacy for more data privacy. We hasten to recall our earlier point that ‘privacy’ is being created by discourse and thus we explain that our intentions here were purely academic,


\(^{42}\) Latin for ‘let the other side be heard as well’.
i.e. to provide an objective account with a critical comment. However, this book is a result of a call for papers supplemented by a few invited contributions, and simply we have not received, even for consideration, contributions arguing otherwise. We acknowledge this shortcoming of this book and we would have liked to see authors with opposite viewpoints, as long as their contributions satisfy the academic criteria of ethics and quality. (Consequently, we would not have liked to see any form of lobbying in the present book.)

3. SPECIFIC OBSERVATIONS

3.1. REGULATION OF CROSS-BORDER DATA FLOWS

Let us now move to some more concrete themes that stand out when reading this book. The debates on trans-Atlantic data privacy relations concentrate on a few critical topics. Perhaps the most obvious, but perhaps equally the most important theme is the regulation of cross-border flows of personal data. Six chapters of this book are devoted to this matter (Weber, Schweighofer, Lindsay, Swire, Vermeulen and Doneda). The tension between the societal usefulness of such transfers, not to say the need for them, on the one hand, is contrasted with the societal usefulness of, not to say the need for, data privacy on the other hand. The need for restricting cross-border data flows is obvious: the value of domestic data privacy protection is severely undermined when personal data are exported without adequate safeguards. At the same time, it is equally clear that there are societal functions that are critically dependent on cross-border data flows. Doneda further observed that in many jurisdictions in Latin America, the proliferation of data privacy regulation, which allows for such transfers, brought positive effects as it led these counties to search for ‘innovative ways of making its own economy more competitive’. Other jurisdictions around the world follow this trend, with a view to receive and – nowadays – maintain the ‘adequacy’ of the level of protection to the EU standards.

In the past two years, much ink has been spilled over the regulation of transborder data flows between the EU and the US. This saga seems to be never-ending. The 2000 Safe Harbour arrangement was found in October 2015 not to be offering the adequate level of protection of data privacy. In July 2016 the very similar Privacy Shield framework replaced it. The new European

43 These countries constitute the vast majority of members of La Red Iberoamericana de Protección de Datos (RIPD), cf. <http://www.redipd.es>.

‘adequacy decision’ has been severely criticised for its illusion of protection – i.e. insufficiency, lack of credibility and misleading character (Vermeulen). Lindsay further observed that Privacy Shield ‘necessarily embodied compromises between the parties’ and the arrangement ‘cannot disguise the hallmarks of haste’, and not even a year has passed before two actions for annulment have been lodged with the CJEU.\(^45\)

The main underlying problem is that ‘the US privacy protection regime is not functionally equivalent to [this] in Europe’.\(^46\) The contemporarily dominant narrative of data privacy law at the European Union level is that of fundamental rights. Wiewiórowski, Assistant European Data Protection Supervisor (EDPS), argued in the Foreword to this book that

> the European Union regards itself as a distinct political entity, which is not a federation of Member States, but it is held together … with a ‘unique, invisible glue’. This connection is grounded with shared goals. One of them … is a unique obligation to protect personal data. Stating that everyone has the right 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.

From 2009, the Charter of Fundamental Rights of the European Union (CFR)\(^47\) guarantees two separate rights to privacy and personal data protection. It is a qualitative change from the predominantly economic narrative that was driving the harmonisation of national data privacy laws in early 1990s. While then the main idea was to harmonise the diverse laws in the EU Member States in order to ensure the free flow of personal data, this qualitative change came with the jurisprudence of the CJEU which emphasised the fundamental rights dimension of data privacy. The entry into force of the Lisbon Treaty (2009), to which the Charter of Fundamental Rights forms a part, concluded this development.\(^48\)

This is structurally and essentially different from the narrative in the United States. Only a few readers would disagree with Swire that both the EU and the US are constitutional democracies built on the same shared values. Yet this observation is valid only on the most abstract level and – when it comes to data privacy – the devil lies in the detail. Contrary to the EU, the constitutional protection of data privacy in the US is far from being comprehensive (e.g. the

\(^45\) Above nn. 16 and 17.
Fourth Amendment to the US Constitution protections only against ‘searches and seizures’ originating from the federal government) and the homologue of the 1995 EU Data Protection Directive, i.e. Privacy Act of 1974, has been found ‘ineffective in curbing government data processing’. The Snowden affaire only demonstrated further the insufficiency of the protections available. The subsequent actions of the US Congress and the President – Swire lists 24 ‘significant actions to reform surveillance laws and programmes’ – no matter how plausible, did not alter the essence of the US data privacy regime.

The next underlying problem is that both sides at the negotiating table – the European Commission and the US Secretary of Commerce – have been fully aware not only of the structural differences between their respective data privacy regimes but also of the practice of the US regime. Yet their awareness has not been reflected in policy-making. These differences existed equally in 2000 (when the first adequacy decision was issued) and 2013 Snowden affaire only confirmed them. Advocate General Ives Bot, in his opinion to the Schrems case heard by the Luxembourg Court, observed that after 2013 the trans-Atlantic data privacy relations have changed significantly. Despite the European Commission being ‘aware of shortcomings in the application of [the Safe Harbour decision]’, it ‘neither suspended nor adapted that decision, thus entailing the continuation of the breach of the fundamental rights of the persons whose personal data was and continues to be transferred under the safe harbour scheme’. The CJEU judgment in Schrems resulted in the European Commission revisiting in late 2016 all ‘adequacy decisions’ issued thus far. The relevant jurisdictions would now be ‘check[ed] periodically whether the finding relating to the adequacy … is still factually and legally justified’ with a view to suspend or limit the free flow of personal data thereto should the need be.

The Commission was equally aware of the many inadequacies of the final text of the Privacy Shield framework – at the end of the day the Commission’s officials follow the debate in the media or in academia. Nevertheless, an ‘adequacy decision’ was issued. (We refrain from commenting here on the legal technique of the whole arrangement – a voluntary self-certification of compliance to the

---


50 For the comprehensive overview, cf. e.g. Nadezhda Purtova, Property rights in personal data: a European perspective, Kluwer Law International, Alphen aan den Rijn 2012, pp. 92 et seq.

51 Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, Opinion of Advocate-General Bot (CJEU, 23 September 2015), §95.

rules set out in a unilateral, regulatory instrument with seven annexes, mostly an exchange of polite letters, printed in the Official Journal of the European Union on 112 pages.) Put simply, ‘law depends on it being taken seriously’ and this whole EU–US transborder data flows saga cannot be regarded as ‘taken seriously’.

Therefore we sympathise with Schweighofer’s proposition for a bilateral treaty – in the meaning of public international law – on personal data transfers for ‘commercial’ purposes. Such a treaty would govern these transfers and would restrict access of US law enforcement authorities to personal data exchanged, providing sufficient legal remedies in case of violation. This would constitute a qualitative change from the Safe Harbour or the Privacy Shield arrangements as this way ‘the procedural guarantees can be placed at a much higher level: from administrative law to U.S. federal treaty law and thus get binding nature’. Schweighofer yet recognises the minimal chances of realisation as ‘the U.S. government is not willing to change its position to data protection regulation’.

However, such a treaty is not unimaginable. From 2006 the EU and the US have a long track record of bilateral treaties – in the meaning of public international law – on personal data transfers for the ‘law enforcement’ purposes. These include, for example, multiple iterations of agreements on Passenger Name Records and Terrorist Finance Tracking Programme. In June 2016 both parties signed the so-called Umbrella Agreement on the protection of personal data exchanged in the context of prevention, investigation, detection, and prosecution of criminal offences. It now awaits the consent of the European Parliament in order to be ratified after having been backed by the Parliament’s Civil Liberties Committee on 24 November 2016. We are thus of the opinion that nothing precludes that the Privacy Shield ‘elevated’ to the level of an international treaty complements the Umbrella Agreement. (We refer here only to the form of such an arrangement, refraining from commenting on the actual contents of any such arrangement.)

3.2. TERRITORIAL REACH OF DATA PRIVACY LAW

A second recurring theme we see is the question of jurisdiction and applicable law. Bentzen & Svantesson in their chapter overviewed ‘which laws to comply

---

with and where disputes should be settled’ when information arising from deoxyribonucleic acid (DNA) is being handled in transnational computing clouds. Although they discuss a particular type of data handling, their observation about ‘jurisdictional complexity’ is valid for the entire universe of privacy. Nevertheless, they claim such a complexity, from one perspective, can be regarded as a positive phenomenon. In the times of uncertainty, those who handle personal data will opt for compliance with the strictest standards in line with the popular adage ‘better safe than sorry’.

A moderate degree of extraterritoriality of data privacy law is necessary in order to efficiently protect individuals and their interests in the digital, interconnected and globalised world when their data are being handled. In the absence thereof, the system would have gaps, allowing for example ‘forum shopping’ to the detriment of data privacy protection. We therefore observe that the extreme attachment to territoriality-thinking is counter-productive to the efficiency of such protection in the cross-border setting. Using the location of the server as the jurisdictional focal point has been discredited in most legal fields, but in the context of data privacy law such territoriality-based thinking is still widespread.

As a proof of this point, Czerniawski argues in his chapter that the jurisdictional scope in the 2016 General Data Protection Regulation,56 based on targeting and market access trigger, seems to be more reasonable for the territorial applicability of the EU personal data protection law than the outdated, pre-Internet ‘use of equipment’ criterion determining the applicability of the 1995 Data Protection Directive. (His argument does not concentrate on the place of establishment criterion or the redirection to EU law by international law.) As nowadays almost any technological artefact could constitute ‘equipment’, e.g. a cookie file, this approach results in jurisdictional overreach. In other words, the EU laws currently in force could be invoked even when there is no real connection between those who handle personal data and an individual in the EU or these laws could be invoked when remedies are impossible to enforce. Therefore the new Regulation sets relatively clear limits to its extraterritorial scope, thus adding to legal certainty. Despite Czerniawski’s analysis being rather formal, it writes itself into the bigger dilemma of how to ensure legal certainty in the ‘length’ of the ‘arm of the EU data protection law’57 together with the efficient protection of individuals.

In Czerniawski’s conclusion, the territorial scope of the General Data Protection Regulation would require relevant authorities on both sides of the Atlantic not only to monitor the handling of personal data or, should the need be,

56 Above n. 15.
to co-operate to enforce their data privacy laws. It would also require to, simply, raise awareness: ‘although you are a US business, you might fall into the scope of the GDPR!’. The absence of these measures might lead to a situation in which the Regulation would become a ‘whim of Europeans’: uncharted, unenforceable and thus ignored beyond European borders.

3.3. FREE TRADE AGREEMENTS AND DATA PRIVACY

A third recurring theme is free trade agreements and data privacy. This book analyses this matter from two viewpoints. One of them is the role of multi-stakeholderism. The discussions about the regulation of data privacy usually lack the voice of those who ‘endure’.58 The public is often either omitted from deliberations (intentionally or not), either not willing to partake therein. The calls to include public voice in the regulation of data privacy in a meaningful way – or even in the regulation of technology and innovation – are not new per se.59 In this volume, Meyer & Vetulani-Cęgiel, building on the fall of the multilateral Anti-Counterfeiting Trade Agreement (ACTA) in 2012 discuss, inter alia, the neglected public voice in free trade negotiations. In the case of ACTA, they concluded that the relevant dialogue ‘certainly could not be described as open and participatory’. As far as transparency is concerned, they have observed some progress with the negotiation process of subsequent agreements, such as the EU–US Transatlantic Trade and Investment Partnership (TTIP) and multilateral Trade in Services Agreement (TiSA), where the European Commission’s Directorate General for Trade publishes, on dedicated websites, non-confidential updates on the progress of the negotiations.60

As the public voice in free trade negotiations is often neglected, so is the protection of data privacy in free trade agreements. Greenleaf has surveyed the existing and proposed bilateral and multilateral free trade agreements to see how they limit the operation of data privacy laws. Attempts to relax the restrictions on cross-border data flows or to prohibit the handling of certain categories of

data solely on local servers (‘data localisation’) constitute the most prominent examples. He eventually compares such agreements to a pact with the devil in which data privacy is bartered for the promised benefits of the liberalisation of trade. However, as he quotes Spiros Simitis, ‘this is not bananas we are talking about’:61 data privacy not only enjoys fundamental rights protection, but also is not ethically neutral and therefore cannot be easily merchandised.

Eventually, Schaeke, a Member of the European Parliament, gives her nine suggestions for how to shape of free trade negotiations when these intersect with innovation and technology, especially highlighting that such agreements must not result in a reduction of the level of protection of fundamental rights. She further sees an opportunity to ‘improve digital rights’ or to set ‘information and communications technologies (ICT) standards’.

No matter how participatory and transparent the negotiating process of a free trade agreement is and no matter how much these agreements advance or limit data privacy protection, what further scares people with the recently negotiated free trade agreements is their comprehensiveness. There are good reasons to be afraid of a potential abuse of – to give a few examples – federated identities, national identity cards, centralised databases, non-anonymous censuses and uniform privacy policies of global technology giants. Greenleaf joins the many commentators in viewing any free trade agreement as an easy way to ‘smuggle’ regulatory solutions otherwise impossible.62 This threat is elevated to another level with free trade agreements that aim at addressing all trade-related aspects of bilateral or multilateral relations between states.

Comprehensive free trade agreements touch upon matters ranging from international trade, sanitary and phytosanitary measures, customs and trade facilitation, subsidies, investment, trade in services, entry and stay of natural persons for business purposes, mutual recognition of professional qualifications, domestic regulation (licensing, etc.), financial services, international maritime transport services, telecommunications, electronic commerce, competition policy, privileged enterprises, public procurement, intellectual property, regulatory cooperation, to trade and sustainable development, labour and environment. (Data privacy is entangled with some of these matters.) We deliberately reproduced here the entire list of substantive matters of the Comprehensive Economic and Trade Agreement (CETA) – by copying the captions of its relevant chapters – to give the reader a glimpse of the Agreement’s complexity.63 In all the comprehensiveness of

---

62 Cf. also Czerniawski, Ch. 10, in this volume.
63 Eventually, the text of the CETA spans 1,528 pages, comprising 30 chapters (230 pages) and an uncountable number of annexes (1,298 pages), full of technical jargon. It took us around four hours just to browse it. Cf. <http://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf>.
such agreements, there is a reasonable fear that data privacy matters can often be interwoven with other matters and can frequently be ‘blurred’ among them to the detriment of its protection.

3.4. REGULATION OF ENCRYPTION

A fourth recurring theme is the regulation of encryption. No chapter in this book treats this matter directly and exhaustively, although a few authors do deal with it in passing. The problem was observed already in the early days of the popular use of the Internet. In particular, Gerry recalls the 1995 Helen Roberts’ report to the Australian Parliament on the regulation of the Internet, in which the latter has foresaw ‘the availability of encryption’ as a regulatory challenge.64 Like with many technologies, the problem lies in the ambivalence of the use of encryption: it could be used both for good and bad purposes.

It is thus not surprising the state has always been interested in having, at its disposal, a possibility to decrypt the contents of a message for national security and similar purposes. Early ‘crypto-wars’ have oscillated around ‘key escrows’ (a regulatory requirement for users and/or technology developers to obligatory deposit decryption keys with law enforcement bodies) or – later – import/export controls and the use of ‘back doors’ (a way of bypassing encryption for these bodies). The demand for keys was for many years a dominant policy of the United States, nowadays abandoned. (Weber although recalls a recent development of such nature in China.) The Snowden affaire demonstrated that the third solution became a widespread practice for all digital communications that is not publicly available. That is to say, ‘back doors’ have been frequently used to access any information that has been otherwise protected by a password, regardless if encrypted or not. It was not surprising that the use of encryption proliferated around the world. The terrorist attacks in Paris, France on 13 November 2015 drew public attention to the drawbacks of the use of encryption, as allegedly these attacks had been plotted with the use of encrypted instant messaging software.65

At the same time, encryption was heralded as an adequate means of protecting data privacy against abusive practices of both public authorities and businesses. It is therefore not surprising that a market for encrypted services – e-mail, cloud computing or instant messaging software – proliferates. In this book, Bentzen & Svantesson suggest ‘adequate encryption’ could mitigate risk of


Intersentia 561
handling DNA information in a computer cloud. Yet Wilson observes correctly ‘we simply cannot encrypt everything’; there are instances when our life would not function if all were encrypted.

The regulation of encryption – or, more accurately, the limitation of its use – once again entered the political agenda. All in all, these developments beg a question whether the use of encryption and restrictions thereof conform to the requirements of democracy, rule of law (Rechtsstaat) and fundamental rights.

One of the very first attempts to legally safeguard the use of encryption was a 1999 plea of Justice Michael Kirby, the leading author of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, to include ‘a right to encrypt personal information effectively’ in their revision in the future.66 (Eventually, their revision, concluded in 2013, contains nothing about encryption.)67 The General Data Protection Regulation does not take any particular stance on the use of encryption, except for heralding it as a security measure.68 In July 2016 Buttarelli, European Data Protection Supervisor (EDPS), commenting on the launch of the reform process of the ePrivacy Directive,69 struck a similar chord: ‘The new rules should also clearly allow users to use end-to-end encryption (without “back-doors”) to protect their electronic communications. Decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.’70 We, however, do not support such a black and white approach. There are situations, although very few, in which encrypted contents must be decrypted.

3.5. REGULATION OF WHISTLE-BLOWING

We mentioned in the Preface that the Snowden affaire had two dimensions: (1) the relationship between a layman on the street and the state, and (2) the

---

67 Earlier, the OECD issued Guidelines for Cryptography Policy in 1997. They address the need to access encrypted data for public security purposes, suggesting the use of ‘third trusted party’ to deposit the encryption key.
relationship between the states at the international level. Actually, there is also a third dimension: the relationship between a whistle-blower and the state. The point of departure here is the legal qualification of the actions of a whistle-blower. In the US, where the history of whistle-blowers disclosing misconduct of the federal government is rather remarkable (cf. e.g. Daniel Ellsberg disclosing the ‘Pentagon Papers’ in 1971), whistle-blowers end up being charged under the Espionage Act of 1917,71 which many commentators judge as denying fair trial.72 Edward Snowden’s situation is no different. On 14 June 2013 – on the sixth day after The Guardian and other newspapers made public his revelations – he was criminally charged with espionage. It is therefore no surprise that in 2015 the Council of Europe called on ‘the United States of America to allow Mr Edward Snowden to return without fear of criminal prosecution under conditions that would not allow him to raise the public interest defence’.73

We see in whistle-blowing – and in other recognised forms of civil disobedience – a commanding tool to exercise public control over state’s power and over the abuse thereof. As such, these merit protection by the law and should be both exercised and limited – similarity to the ‘right to encrypt’ – in accordance with requirements of the rule of law (Rechtsstaat), fundamental rights and democracy.

A good deal of the answer to the questions of encryption or whistle-blowing lies in the principle of proportionality as known predominantly from fundamental rights law. This legal principle has many faces, bears a lot of uncertainties and thus has been widely contested. Yet – thus far – it seems to be the tool that allows drawing a ‘thin red line’ between competing interests, as its modus operandi permits to ‘ask the right questions’. Born ‘in eighteenth and nineteenth-century Prussia as a limit on the nascent growth of the administrative state in the absence of democratically imposed constraints’, the principle of proportionality has an important role to play in filling this gap in contemporary circumstances (Lindsay). In order both to better protect individuals and to ensure legal, ‘commercial’ and ‘political’ certainty, Lindsay claims, the principle still needs to be ‘appropriately defined and rigorously applied’. He further vests the proportionality test in the courts of law, as – in the time of emergency – these ‘are the main candidate for imposing limits on state power’, yet bearing in mind the danger of ‘judicial over-reach’. We agree, yet we also see the principle of proportionality widely used in the parliaments, where the relevant testing

71 Espionage Act of 1917, Public Law 65-24, 18 USC §792.

Intersentia 563
is a genuine part of *ex ante* studies and evaluations of any regulatory measure proposed. This way, a good deal of the work of a court of law would be done long before such a measure is even applied.

4. A FEW MODEST SUGGESTIONS AS TO THE FUTURE SHAPE OF TRANS-ATLANTIC DATA PRIVACY RELATIONS

This essay-style chapter has highlighted the most ‘hot’ issues at the end of 2016 in which the protection of data privacy on both sides of the Atlantic touches upon the notions of democracy, rule of law (*Rechtsstaat*) and fundamental rights. Some of these issues can easily be translated into a few modest suggestions as to the future shape of trans-Atlantic data privacy relations. Therefore, we conclude therewith:

1. The answer to Snowden *affaire* – and more broadly: to global mass surveillance practices – lies in the concept of the rule of law (*Rechtsstaat*) *sensu largo*. It is not sufficient to establish rules on national security, free trade or transborder personal data flows with due respect for formal and procedural requirements. The contents, and the application, of these laws must also conform to the same substantive standards.

2. Regulation of data privacy is a global concern. As Beck puts it, ‘no nation can cope with its problems alone’, implying that global risks require global responses.74 Ideas for a worldwide convention on data privacy or for an international organisation overseeing its regulation are not new. Yet they would work smoothly only when substantive laws converge and this would not be a case in the foreseeable future. What is understood as ‘privacy’ in Europe is different from the understanding in other parts of the world. Even within Europe, perceived by many as having homologous views on ‘privacy’, its perception is not uniform. (For example, the Scandinavian openness of public life, manifested by public access to individual tax records, is not shared in the rest of the continent. Allowing for such differences is simply respectful for diverse cultural and legal heritages.) Achieving an international consensus beyond the mere need for the protection of privacy (with possible agreement on the most obvious topics) and enacting it into binding legal norms is rather difficult to imagine. It would be not only formally difficult to achieve but also might be detrimental to the diversity of cultural and legal heritages. Thus, we remain sceptical as to the success of

---

such all-encompassing, global-reaching proposals for a (binding) standard on data privacy regulation.

3. A reminder: regulation of data privacy is a serious matter. To once again quote Simitis: ‘this is not bananas we are talking about’. Privacy’ is both a fundamental right and an ethical concern that requires adequate and efficient protection. It is also a central matter in the information economy and the importance of data privacy as an enabler, and as an obstacle, to economic growth must be part of the calculation. So must be the centrality of data privacy in security practice – be it national or urban. The legal principle of proportionality is to guide the drawing of a ‘thin red line’ between such competing interests. In parallel, legal certainty warrants smooth operation of both information economy and security practices.

4. It will sound trivial, but new data privacy problems will be emerging every day and new solutions thereto will be proposed at an almost equal pace. What is required is a transparent, multi-stakeholder and critical debate as to linking these problems with appropriate solutions.

5. The public voice should be carefully and meaningfully listened to in the regulation of data privacy, regardless whether data privacy is a direct object of regulation (such as transborder data flows) or indirect (such as governance of free trade). Many legal frameworks in multiple domains require asking the public at large and/or their representatives (e.g. national parliaments, regional councils, non-governmental organisations, etc.) to express their views (e.g. environmental law). We argue for this phenomenon not only to become a standard in governance of technology and innovation – this including data privacy, but also to ensure that their views are actually taken into account.

6. New, comprehensive free trade agreements set up a dangerous, wrong precedent. This is not an opposition to free trade, but rather a plea – from a formal viewpoint – for a ‘stepping stone’ rather than a ‘stumbling block’ policy. Further, many commentators discussed the need for more transparency and more public participation – in other words, for more democracy – and we cannot but agree with them. We just add here a plea for ‘slow’ politics and some ‘sectorial’ approach. In bilateral and multilateral relations, the reduction of tariffs should be a subject matter of one arrangement, and investment partnership of other arrangement.

7. The EU and US data protection regimes – for ‘commercial’ purposes – cannot be bridged simply by means of ‘adequacy decisions’. Declaring the US regime ‘adequate’ in the EU will always infringe the EU Charter of Fundamental Rights. Any such move will be judged as political, acting in a particular interest of sustaining the digital market for the price of

75 Above n. 61.
deterioration of fundamental rights. It will only bring more work for the judges of the CJEU in Luxembourg. We do not have yet any golden means for the EU–US cross-border data flows problem, pointing out only that the means of ‘adequacy decisions’ should be abandoned in order for a serious, durable solution respecting EU fundamental rights to be put in place. A bilateral treaty in the meaning of public international law could constitute an appropriate means to that end.

8. It has long been recognised that the territoriality focus that characterises our current paradigm is a poor fit with the reality of the online environment. It is also a poor fit with numerous other areas of law with cross-border interaction, such as environmental law. While the territoriality focus – such as focusing on the location of data – has been discredited and abandoned in many legal settings (including areas, such as defamation, closely related to the right of privacy), it appears harder to shake in the data privacy universe. This is partially understandable. Yet we argue that the time has come to reconsider our reliance on territoriality also, in the data privacy context. After all, as a filtering mechanism distinguishing between situation in which a state legitimately may claim jurisdiction and situations where a state’s jurisdictional claim would lack such legitimacy, the territoriality scores few victories apart from in the most obvious cases.

9. In the case there is an opportunity to reconsider how we approach jurisdiction in the context of data privacy, we must avoid overly broad – and practically unenforceable – jurisdictional claims resulting in a discretionary enforcement. Such an approach might simply undermine the efficiency of protection.

10. Encryption should be protected as an enforceable right. We make this proposition very carefully: a right is a very precise concept, at least in European human rights law, whose features make it suitable for the regulation of encryption. A right is rarely absolute and thus it is subjected to some limitation criteria, exhaustive and to be interpreted narrowly. Yet we do not claim here how such protection should be afforded or where it should be placed in the hierarchy of legal norms. It could be either a new fundamental right or a data subject right within a bundle of her other relevant rights. It could be spelled out by a legal statute (e.g. introduced, in the EU, in the reform of the ePrivacy Directive, as proposed by Buttarelli) or – equally – interpreted by a senior court (as the CJEU did with the right to de-listing).

76 It is then for the technology experts to offer technological solutions, in accordance with the state of the art, for the limitation of the enjoyment of such a right. One thing is yet sure: ‘back-doors’ and ‘key escrows’ do not constitute a lawful way to limit the use of encryption. In any

76 Above n. 29.
case, it is a task of central importance and one associated with considerable urgency.

11. A key issue in all this is the tension between the need for transparency on the one hand, and the need for some data collection and use within the national security arena to remain secret. After all, the only way to know that our data is not misused is through complete transparency, and such complete transparency is neither possible nor desirable when it comes to security, equally national or urban. Here we hit a dead end. But perhaps the Snowden affaire has brought to the attention a way to cut the Gordian knot. The security agencies’ compliance with law is monitored not only by designated bodies but also, at least some of, the very people working in the intelligence community. The key would then seem to be to construct a legal framework that (1) allows us to trust the reports by whistle-blowers, (2) that provides safeguards for whistle-blowers, and (3) that ensures that information revealed by whistle-blowers is used to address violations without jeopardising security and individual lives. To this end, whistle-blowing and other recognised forms of civil disobedience should become a standalone means of protection against the abuse of the requirements of fundamental rights, the rule of law (Rechtsstaat) and democracy by global mass surveillance practices.

To use again Saramago, it is true that ‘not a day passes’ without personal data flowing between both sides of the Atlantic. Data privacy and its protection are therefore entangled in the entirety of political relations between the EU and the US. (This observation is actually valid for political relations between almost any jurisdictions.) Yet the handling and the flows of these data – in Williams’ words – remain rather ‘unnoticed’. The protection of individuals whose personal data are handled and flown often fall victim to recklessness, indifference or ignorance. Data privacy is a serious matter, it grows and matures rapidly, but nevertheless it is still blurred in the complexity of trans-Atlantic relations. It seems not to be the main concern when for example personal data transfers, jurisdictional scope, free trade, encryption or civil disobedience are being regulated. We have therefore made these few modest suggestions for data privacy protection in the trans-Atlantic setting to adhere to requirements of democracy, rule of law (Rechtsstaat) and fundamental rights so that data privacy does not share the fate of Icarus. The green cover of this book was chosen to underline this hope.