25. MOVING BEYOND THE SPECIAL RAPPORTEUR ON PRIVACY WITH THE ESTABLISHMENT OF A NEW, SPECIALISED UNITED NATIONS AGENCY*

Addressing the Deficit in Global Cooperation for the Protection of Data Privacy

Paul De Hert** and Vagelis Papakonstantinou***

1. INTRODUCTION

While the protection of privacy is a global concern,[1] the new technologies or methods of processing of personal data – such as big data, the Internet of Things, cloud computing, or smartphone applications – might easily drive to despair any legislator attempting to apply local jurisdictional approaches to personal data processing. This is because this type of processing is by design addressed directly to individuals anywhere in the world, treating national borders as irrelevant.

Quite contrary to what is urgently needed, an entrenchment attitude may be identified even in regional and global data privacy models devised today at the level of the European Union (EU), the Council of Europe (CoE) and the Organisation for Economic Co-operation and Development (OECD). At state

---

* An earlier version of this contribution appeared as: Paul De Hert and Vagelis Papakonstantinou, 'Why the UN should be the world's lead privacy agency?', *IAPP Privacy Perspectives*, 28 April 2016, <https://iapp.org/news/a/why-the-un-should-be-the-worlds-lead-privacy-agency>.

** Research Group on Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel; Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University. E-mail: paul.de.hert@uvt.nl.

*** *Research Group on Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel.* E-mail: vpapakonstantinou@mplegal.gr.

1 See, for example, 'Privacy will hit tipping point in 2016', *CNBC*, 9 November 2015, <http://www.cnbc.com/2015/11/09/privacy-will-hit-tipping-point-in-2016.html>.

level, an increased interest in data privacy has been identified, with more than 100 countries having by now enacted some sort of data protection law within their respective jurisdictions.[2] However, this does not necessarily mean that they all approve of and subscribe to, for example, the EU model or any other of the above available global models. Regulatory approaches are diverging, failing to reach out to each other. Even compatibility among them is hard to achieve, as the recent Privacy Shield saga[3] demonstrates. While the right to data privacy is globally acknowledged as an important safeguard for individuals in the digital era, the way to protect it is understood differently in different parts of the world. To avoid legal fragmentation, it appears that global cooperation and coordination is imperative. However, the ways to achieve it vary considerably, and seemingly insurmountable obstacles lie ahead.

While the question whether an international treaty or convention, which would constitute the obvious policy option, is a viable solution has already been addressed in theory, mostly towards the negative,[4] some hope may come from the United Nations (UN). In July 2015, the UN Human Rights Council appointed Professor Joseph Cannataci as its first-ever Special Rapporteur on the right to privacy. His mandate is, among others, to gather information, identify obstacles, take part in global initiatives and raise awareness.

In order to address this global deficit in cooperation, the authors believe that a new, specialised UN agency for the protection of data privacy needs to be established.[5] We believe that the World Intellectual Property Organization (WIPO) could serve as useful inspiration to this end. The role of the global regulatory text of reference for data privacy, corresponding to the Paris and Berne Conventions within the global system for intellectual property protection, could be held by the UN Guidelines for the Regulation of Computerized Personal Data Files.[6] Despite their age, we believe that, if modernised, they could achieve global consensus and attain the basic data privacy purposes, constituting the global lowest common denominator.

---

2 See Greenleaf, G., 'Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority' (2015) 133 *Privacy Laws & Business International Report*, February 2015; UNSW Law Research Paper No. 2015-21, <http://ssrn.com/abstract=2603529>.

3 See, indicatively, Bracy, J., 'EU Member States approve Privacy Shield', *IAPP Tracker*, 8 July 2016, <https://iapp.org/news/a/eu-member-states-approve-privacy-shield/>.

4 Kuner, C., 'An International Legal Framework For Data Protection: Issues and Prospects' (2009) 25 *Computer Law & Security Review*.

5 De Hert, P. and Papakonstantinou, V., 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9(3) *I/S A Journal of Law and Policy for the Information Society*.

6 As adopted by General Assembly resolution 45/95 of 14 December 1990 (the 'UN 1990 Guidelines').

In the following section of this chapter, section 2, we briefly outline the deficit in global cooperation to the detriment of the level of data protection afforded to individuals. Then the UN initiatives for the global protection of data privacy are discussed (section 3). We then suggest that a new, specialised UN agency for data privacy be established, and we identify its potential benefits (section 4). Finally, we compare such an initiative with the WIPO and global intellectual property protection model that, to our mind, could serve as a useful role model for the development of a similar, global UN system for the protection of data privacy (section 5).

2. THE DEFICIT IN GLOBAL COOPERATION FOR THE PROTECTION OF DATA PRIVACY

It has become by now a self-evident truth that new personal data processing models transcend national borders and pay no respect to national jurisdictions. Because they are ultimately connected with the Internet, which enables the provision of services or the sale of products from anyone to anyone, anywhere in the world, new business models and technologies to serve them are designed exactly around this requirement: to be able to serve a global clientele directly, without local representatives, from a single location somewhere on the globe. It is in this light that recent technologies such as cloud computing, smartphone applications or geolocation services need to be viewed. It is by design that they disregard local legal regimes and constraints. This trend is not expected to change in the future. If one wished to add another trend to the picture, it would be that of ubiquitous processing: the continuous processing of information performed in the background, without individuals necessarily being aware of it. The Internet of Things broadly falls within the same category. If correlated with the internationalisation trend above, we would end up with ever-increasing volumes of personal data being transmitted directly by individuals, to be collected and processed anywhere in the world.

At the same time, the equally demanding security-related personal data processing requirements ought not be overlooked. International crime, as well as international terrorism, have made the global cooperation of national law enforcement authorities necessary, which is ultimately connected to the requirement that personal data be exchanged seamlessly among them.

In view of the above, international coordination of legal regimes is urgently needed in order to provide individuals anywhere in the world with adequate protection of their rights. From their point of view, individuals engage in mainstream activities from the comfort of their homes or offices: they navigate the Internet, make purchases and use global services. The background of the global personal data processing involved in these simple and straightforward

activities largely escapes them. In other words, they are unaware (or at least do not fully grasp the implications) of their personal data being transmitted and processed anywhere (and by anyone) in the world. Being accustomed in their everyday (offline) lives to traditional legal systems and regimes, which provide for protection locally, they expect a similar level of protection while online. Consequently, the legal system needs to provide them with adequate means to do so. For the time being this has not been the case. The legal tools placed at the disposal of individuals in order to protect their right to data privacy until today have grossly failed to provide any meaningful protection against cross-border incidents.

This deficit is attributable to the legal regimes for the protection of data privacy that are in effect across the globe today. Rather than converging in order to address the internationalisation of personal data processing described above, differences in data privacy legal approaches across the globe have become increasingly entrenched over the past few years. In the EU, the model initially introduced by Directive 95/46[7] is furthered by its successor, the General Data Protection Regulation (GDPR)[8] that will come into effect in May 2018. Notwithstanding the strict and formal requirements it places upon EU Member States when it comes to personal data processing (application of processing principles, requirement for a legal basis for the processing, monitoring by a data protection authority), its approach towards international personal data transfers is straightforward: third countries, in order to be able to exchange personal data with EU Member States, need to adhere to the EU model through one of its provided alternatives.[9] Although these alternatives may come in different formats, their underlying idea is that third countries will need to accept and apply an equivalent to the EU approach on personal data processing. Such an approach may sound rigid or outright incompatible to the legal frameworks of several countries around the globe, which could explain the fact that over the past 20 years, only a handful of countries have been awarded with *adequacy* status by the European Commission.

A level of flexibility is allowed for in the Convention of the Council of Europe, which also is undergoing a modernisation process aimed at amending its text, which dates back to 1981.[10] Its Member States, which include all of the EU

7 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.

8 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

9 See Chapter V the General Data Protection Regulation.

10 See Council of Europe, Modernisation of Convention No. 108, <http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp>.

Member States but also several other countries as well, are required to implement an admittedly more relaxed model than that of the EU, due to the lack of many processing formalities present in the EU regulatory framework. A further difference involves the fact that the Council of Europe data privacy model never hid its ambition to become the global data privacy standard[11] – which indeed may constitute a possible, and perhaps even welcome, development, as will be discussed in the analysis that follows. In this context, it should be noted that the CoE Convention allows for ratification of its text by non-Members as well. While until recently, third countries used this option as a preparation exercise to seek an *adequacy* finding by the EU, the modernisation process has revealed a new dynamic for the Council of Europe efforts, with numerous countries being found at various ratification stages.

Other instruments in the field, such as the OECD Guidelines[12] or the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, are not binding. However, they too contribute to the picture of global fragmentation because they do not aim at compatibility, or even interoperability, with the above two (binding) regulatory instruments. This lack of a firm regulatory approach has permitted the development and proliferation of a multitude of 'soft law' approaches, which may take the form of anything between regional case-specific rules and regulations (for example, the Berlin Group),[13] international standards (for example, the International Standards Organisation),[14] international *fora* (for example, the International Conference of Data Protection and Privacy Commissioners), or global cooperation initiatives (for example, the Madrid Resolution).[15] All of the above, while welcome in promoting the global data privacy idea, unavoidably take place in, and aim to fill gaps in, the global regulatory void. The lack of a firm, globally acknowledged legal framework on data privacy makes all such initiatives appear disconnected from the real legal world, in the sense of granting rights and extracting obligations.

What we are therefore faced with is a diverging, rather than converging, approach on international data privacy. On the one hand, technologies and individuals act globally, disregarding any local notion such as legal jurisdiction,

---

11 See Greenleaf, G., '"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29(4) *Computer Law & Security Review*.

12 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013.

13 International Working Group on Data Protection in Telecommunications, <https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>.

14 See, for example, De Hert, P., Papakonstantinou, V. and Kamara, I., 'The New Cloud *Computing ISO/IEC 27018 Standard Through the Lens of the EU Legislation on Data* Protection' (2016) 32 *Computer Law & Security Review*.

15 International Standards on the Protection of Privacy with regard to the processing of Personal Data, Madrid, 5 November 2009.

court systems or data protection authorities. On the other hand, the legal instruments in effect disregard this reality, each one sticking to its own regulatory model: rather than trying to build regulatory bridges, each international organisation or country concerned seeks to export, if not impose, its own model onto others. A point in the not too distant future may easily be imagined when a truly global data breach or other data protection incident (Internet social networks are, after all, enterprises that may, at some point in the future, go bankrupt) will make all too obvious the shortcomings of this approach to each, mostly unsuspecting, Internet user on the globe.

3. PAST AND RECENT UN INITIATIVES IN THE DATA PRIVACY FIELD

Until today, the UN has not been particularly interested in global data privacy matters. With regard to protection of the general right to privacy, Art. 17 of the International Covenant on Civil and Political Rights of 1966,[16] and in particular its Comment No. 16,[17] as well as Art. 12 of the Universal Declaration of Human Rights[18] set the basic regulatory framework. Specifically with regard to data privacy, the UN issued in 1990 its Guidelines and, after a long period of silence, on 1 July 2015, at the alleged insistence of the civil society,[19] the UN appointed a Special Rapporteur on the Right to Privacy. Professor Joseph Cannataci took up this role on 1 August 2015.

This approach, while pointing in the right direction, appears limiting with regard to the contemporary global personal data processing environment. The UN Guidelines actually belong to the first generation of international data protection regulatory documents[20] and are in need of modernisation. The installation of a Special Rapporteur, while an important development in itself, is not enough. The Special Rapporteur role is a part-time, not fully UN-supported role. Even under its current, mostly consulting, mandate, the Special Rapporteur will struggle to execute it satisfactorily with his current infrastructure. On the

16 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.'

17 General Comment No. 16, Art. 17 (the right to respect of privacy, home and correspondence, and protection of honour and reputation), UN Human Rights Committee, HRI/GEN/Rev9 (Vol.1), 8 April 1988.

18 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

19 See 'UN Human Rights Council creates Special Rapporteur on right to privacy', *International Justice Resource Center*, 22 April 2015, <http://www.ijrcenter.org/2015/04/22/un-human-rights-council-adopts-resolution-to-create-special-rapporteur-on-the-right-to-privacy/>.

20 De Hert and Papakonstantinou, above n. 5.

other hand, global data privacy matters are complex issues, constantly in flux. They cannot possibly be followed by a single person or even a small team of experts, regardless of their best intentions.[21] In addition, they ultimately involve concrete cases, where individuals whose rights are infringed or data controllers wishing to process data in new ways ask for specific guidance and assistance. A watchdog function alone is not enough (and, in any event, is better carried out by civil society organisations). In other words, data privacy has an administrative nature that resembles better the subject matter of UN specialised agencies (the WIPO, the International Labour Organization, the World Bank, the International Monetary Fund) rather than that of UN Special Rapporteurs (freedom of opinion and expression, freedom of religion or belief, independence of judges and lawyers, migrants, minority issues).

4. SUGGESTING THE ESTABLISHMENT OF A NEW, SPECIALISED UN AGENCY ON DATA PRIVACY

The foregoing explains our belief that an adequate response would be for the UN to establish a new, specialised agency aimed at the protection of data privacy. UN specialised agencies

> are autonomous organizations working with the United Nations. All were brought into relationship with the UN through negotiated agreements. Some existed before the First World War. Some were associated with the League of Nations. Others were created almost simultaneously with the UN. Others were created by the UN to meet emerging needs.[22]

So far, the UN has operated 15 specialised agencies, including the World Intellectual Property Organisation, whose example could be followed in the case of data privacy as well, as will be demonstrated in the analysis that follows.

The mandate for such a new UN specialised agency could be similar to the one already in effect for its Special Rapporteur on Privacy. Its terms of reference, meaning the regulatory framework to be applied by such a new UN agency, need not be a comprehensive, detailed set of rules immediately after its establishment. A number of options are possible. While the authors have a preference for the UN 1990 Guidelines to be updated, alternatives could be to draft an additional protocol to Art. 17 of the Covenant, or to adopt the Council

---

21 In EU terms, the office of the European Data Protection Supervisor (EDPS) may serve as a good sample, or measure, for this task.

22 Cf. <http://www.un.org/en/sections/about-un/funds-programmes-specialized-agencies-and-others/index.html>.

of Europe Convention in one form or another. We believe that what is important here is the establishment of a new UN agency *per se*. Consequently, emphasis need not be placed, at least at the beginning, on devising a robust data privacy legal framework for it to apply. Instead, a global lowest common denominator regulatory framework, wherever this is to be found, could be used as a starting point, in order for regulatory work to start taking place at an international, rather than regional, level.

The benefits of establishing such a new UN agency would be substantial. First, such an agency would offer data privacy a global point of reference. Currently, different regions in the world cannot even agree on terminology, with Europeans speaking about data protection, others about data privacy, and a smaller, but no less important, group categorising everything under the general right to privacy. Similarly, individuals who believe that their rights have been infringed, particularly outside their national borders, need to navigate a multitude of agencies and authorities in order to find a remedy. A common point of reference provided by an organisation accessible to all, even if it would ultimately only refer the matter to competent national authorities, would be an indispensable contribution in a fragmented, and largely non- or even miscommunicating, global environment.

A second contribution would be the placement of the data privacy discussion on its proper basis. No agreement is found globally whether data privacy constitutes a basic human right or not – and, if so, whether it is independent from the right to privacy. While things are beginning to crystallise in the EU, elsewhere data privacy is viewed as an online business competitive advantage, or the means to equip electronic commerce with public trust.[23] Other countries fear that the data privacy discussion may affect adversely their information technology industry. A new UN agency would address this controversy by firmly placing protection within the UN and, thus, within the human rights context.

A third contribution would be the organisation's potential role as a global convergence mechanism. At present there exists no formal international forum for achieving convergence among the various data privacy models in effect across the globe. International instruments in effect today (the EU Regulation, the CoE Convention, the OECD Guidelines and the APEC Framework) unfortunately have not incorporated permanent administrative mechanisms with the mandate to achieve, if not coherence, at least basic understanding in their texts. On the contrary, lack of such mechanisms demonstrates regulatory competition and a struggle for global domination. A UN agency would provide the self-evident forum for such a mechanism to operate on a permanent basis.

---

23 See, for example, Online Trust Alliance (OTA), 'Social Media and eCommerce Sites Lead in Security and Privacy', 6 June 2012, <https://otalliance.org/news-events/press-releases/social-media-and-ecommerce-sites-lead-security-and-privacy>.

Finally, the new UN agency could act as the international last recourse, assuming the role of the global go-to organisation for these data subjects who may feel that their data privacy right has been infringed and who do not benefit from a national data protection authority (or, as the recent case in the UK has demonstrated, they do benefit from such an authority but feel that their views need to be heard elsewhere as well).

5. THE WIPO MODEL AS USEFUL GUIDANCE TOWARDS THE ESTABLISHMENT OF A UN SYSTEM FOR THE GLOBAL PROTECTION OF DATA PRIVACY

In our view, there exist definite parallels between 1873 in intellectual property law and 2016 in data privacy law. In particular, the need for international protection and the inability to conduct normal business otherwise were identified for each legal system at these respective dates. In the WIPO's words,[24] the Paris Convention, in 1883, was 'the first major step taken to help creators ensure that their intellectual works are protected in other countries' that came about only when

> the need for international protection of intellectual property (IP) became evident when foreign exhibitors refused to attend the International Exhibition of Inventions in Vienna, Austria in 1873 because they were afraid their ideas would be stolen and exploited commercially in other countries.

This is a more or less accurate description of global personal data processing circumstances met today: individuals are desperate to be assured that their personal data are protected in other countries, wherever the Internet has made it possible for their data to be freely and immediately transmitted. At the same time, exports of personal data are grossly curbed by the application of the EU *adequacy* criterion. In one or another way, this wording may be found in other international instruments as well, culminating in today's fragmented world of haves (data privacy national legislation) and have-nots – the latter being in essence penalised by the former by means of exclusion of any business involving personal data transfers.

The WIPO is, in its own words, 'a self-funding agency of the UN, with 188 member states'. It was established by means of a Convention (the WIPO Convention of 1967) but replaced its predecessor, the United International Bureaux for the Protection of Intellectual Property, which was established as

24 See <wipo.int>.

early as 1893, in order to administer the Paris and Berne conventions. While the details of these two instruments are of no relevance to the purposes of this analysis, it could be noted that the Berne Convention was the result of a campaign by Victor Hugo and his association of authors, and that each text has been amended several times (approximately every 15–20 years, since their release in 1883 and 1886, respectively). Consequently, they came as the result of a users' campaign (perhaps in the equivalent of today's civil society), and their finalisation was neither an easy nor a finite task. The WIPO was not set up as a UN specialised agency; however, it became one shortly after its establishment, in 1974.[25]

At any event, the WIPO mandate[26] could be applied *mutatis mutandis* in the data privacy context as well. After all, it does not lie far away from the mandate of the UN's Special Rapporteur on Privacy established today. Indeed, a new UN data privacy agency would need to promote data privacy purposes and issues globally, in cooperation with all other international organisations already active in the field. It would also be empowered to ensure administrative cooperation among the various data privacy national agencies to be found across the globe. Other tasks entrusted to the WIPO today (for example, the running of the patent cooperation treaty or the international trademark system) could be paralleled within the new UN agency on data privacy scope: running a global certification system, for these global data controllers that would need one, or offering an alternative dispute resolution mechanism. Because of the technical character of both rights, the scope of work for these international agencies entrusted with the task to promote their purposes and monitor their application in practice could constantly develop, following technological or other developments in their respective fields.

While a detailed roadmap on the establishment of a new UN specialised agency on data privacy would have to take into account internal UN procedures, we believe that the WIPO case could provide useful background to this end. There are two basic options for the establishment of a UN specialised agency: either setting up a new international organisation outside the UN and then

25 Although it is beyond the scope of this chapter to address the limitations or criticisms of WIPO, the following could perhaps serve as indicative literature in this regard: May, C., *The World Intellectual Property Organisation – Resurgence and the Development Agenda*, Routledge 2007; Cordray, M.L., 'GATT v. WIPO' (1994) 76 *J. Pat. & Trademark Off. Soc'y* 121; Boyle, J., 'A Manifesto on WIPO and the future of Intellectual Property' (2004) 9 *Duke Law & Technology Review*.

26 'The objectives of the Organization are: (i) To promote the protection of intellectual property throughout the world through cooperation among States and, where appropriate, in collaboration with any other international organization; (ii) to ensure administrative cooperation among the intellectual property Unions'. Convention Establishing the World Intellectual Property Organization, Art. 3.

applying for special organisation status within the UN (as was the case with the WIPO), or creating a new agency directly by the UN. In our mind, the second solution, the direct establishment of a new agency by the UN, is preferable – and the existing Secretariat of the Special Rapporteur could provide a useful starting point in this regard. Establishment of a new international organisation outside the UN could prove impossible in practice because it would essentially require a self-initiated new international convention on data privacy. Even if this was accomplished, there would presumably exist an intermediate period when it would antagonise existing (UN, Council of Europe, etc.) structures on data privacy. On the other hand, direct establishment of a new agency by the UN, equipping it with an existing UN regulatory framework (the amended Guidelines of 1990 or a new additional protocol) or using in one way or another the Council of Europe Convention would avoid any conflicts of interest among the organisations concerned and would signal in a positive way to everybody the UN resolution to engage, and dominate, the field globally.

6. CONCLUSION

The UN has remained idle on the issue of data privacy since 1990, therefore missing significant developments, including the Internet as well as the global war against terrorism. The world today is a very different place than it was in 1990, when the UN's last attempt to regulate on this issue took place. What then constituted a problem of a closed number of countries that were experimenting with new technologies now has global implications affecting directly the everyday lives of people living in industrialised countries, in the developing world, as well as people receiving humanitarian assistance. The processing of personal information has culminated in an independent human right, on a par with any other rights on the list, whose adequate protection occupies a leading position on concerns expressed by individuals anywhere in the world regardless of the different predicaments they may be in. It is therefore time for the UN to become active in the field once again.

The UN responded to these conditions by establishing a new Special Rapporteur on Privacy. This appointment is important, and the person entrusted with this role has already undertaken positive steps towards successful execution of his mandate. However, in this chapter we question whether this is enough. Incremental progress may be a cautious and reasonable approach but does little to address pressing global data privacy issues. A global problem affects everyone on a daily basis, international cooperation among the legal instruments at hand is not only missing but not even planned for, and regional half-measures aimed at resolving each new problem (the right to be forgotten against Internet searches, technical standards against cloud computing, etc.) only soothe but do not heal the wounds. A new UN specialised agency is urgently needed.

To this end, useful guidance may be provided by the UN model for the global protection of intellectual property: the World Intellectual Property Organisation is a specialised UN agency entrusted with the global protection and promotion of intellectual property rights. This model was initiated more than 100 years ago when cross-border problems not unlike the ones identified today in the data privacy field made international cooperation and the establishment of a global system of protection imperative. After decades of experimenting, the incorporation of a new, specialised UN agency was considered the preferred way forward; the WIPO thus joined the UN in 1970 and holds a similar role to what could be envisaged for a new UN specialised agency on data privacy.

In our opinion, the establishment of a new UN specialised agency does not necessarily require a robust new international treaty on data privacy. The legal framework that could support its operation, at least in the short term, is more or less already available: the amended UN Guidelines of 1990 could undertake this role, or, a new additional protocol to Art. 17 of the Covenant. What should be aimed at initially is flexibility and inclusiveness, even at the expense of effectiveness of protection. Effectiveness of protection is an abstract term perceived differently across the world. The UN model would not replace already existing national ones. It would formulate the global common lowest data privacy denominator. However, it would be a standard applicable by everyone.

INVITED COMMENT

26. CONVENTION 108, A TRANS-ATLANTIC DNA?

Sophie KWASNY*

The Convention for the protection of individuals with regard to automatic processing of personal data[1] ('Convention 108') was opened for signature in Strasbourg on 28 January 1981[2] and came into force on 1 October 1985. Thirty-five years after its opening for signature, the Convention applies to 50 countries.

Convention 108 is unique. It was unique over three decades ago, and remains the only legally binding international instrument in the field of data protection. Its legally binding force is a key element that makes it unique, but it is not the only one. Another key characteristic of Convention 108 is its unmatched potential for global reach: Convention 108 is open to any country in the world.

Is this opening to the world, aimed at affording protection to individuals when data concerning them flow across borders and oceans, with a particular focus on the trans-Atlantic dimension examined here, the result of genetic instructions which guided its development? Or is it instead the result of a genetic mutation or the result of the use of genetic engineering techniques?

Convention 108 was conceived, and delivered, with the idea that data protection should respect the principle of international free flow of information. Its trans-Atlantic nature in fact pre-dated the Convention itself, deriving from the identity of its parents and in the hopes they vested in the Convention.

On the life scale of an international treaty, a few decades of life amounts only to infancy, and the trans-Atlantic hopes that have started to materialise only recently are to be considered in a longer-term perspective, with a promising future.

---

* Data Protection Unit, Council of Europe. E-mail: sophie.kwasny@coe.int.

1 More information on Convention 108: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

2 28 January has been known for the past ten years as a 'data protection day', on an initiative of the Council of Europe to mark the anniversary of Convention 108, and is also celebrated outside Europe as 'privacy day'.

1. CONVENTION 108, TRANS-ATLANTIC AT BIRTH

The Committee that drafted Convention 108 had in its mandate the clear instruction 'to prepare a Convention for the protection of privacy in relation to data processing abroad and transfrontier data processing'.[3] It 'was instructed to do so in close collaboration with the Organisation for Economic Co-operation and Development, as well as the non-European member countries of that organisation, having regard to the activities which OECD was carrying out in the field of information, computer and communications policy.'[4]

The 'OECD, as well as four of its non-European member countries (Australia, Canada, Japan and the United States) were represented by an observer on the Council of Europe's committee.'[5]

While many other multilateral Conventions of the Council of Europe are titled 'European' Conventions, the drafters of Convention 108 decided not to use the European adjective in the title of the Convention, precisely to highlight the open nature of the instrument and 'to underline that there ought to be ample scope for accession to it by non-European States'.[6]

Accession to the Convention by non-Member States of the Council of Europe is regulated by Art. 23 of the Convention, which prescribes that:

> After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

As emphasised in the Explanatory Report[7] to the Convention, the immediate intention of the drafters was to enable accession by the four non-European countries already mentioned, that had participated in the work of the drafting Committee.

The drafters of the Convention had already envisaged accession to Convention 108 by, notably, the United States. A vision aimed at securing the protection of individuals in full respect of the principle of free flow of information.

Louis Joinet, Chair of the Committee that drafted the Convention, had underlined the emerging power constituted by information, the related risk of restrictions on transborder data flows, and strived to deliver an international instrument that would contribute to providing a legal solution to this emerging concern.

---

3 Explanatory Report to Convention 108, §13.
4 Ibid., §14.
5 Ibid., §15.
6 Ibid., §24.
7 Ibid., §10.

> Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows.[8]

2. DEFINITELY MORE TRANS-ATLANTIC 30 YEARS LATER

Despite an early active trans-Atlantic exchange at the drafting stage of Convention 108, participation in the work of Convention 108 by representatives from the western side of the Atlantic would not start before the beginning of the third millennium.

Trans-Atlantic participation in the work related to Convention 108 currently involves several countries from the Americas (Canada, Mexico, Uruguay and the US), as well as the regional network of Ibero-American data protection authorities.

Uruguay currently is the sole trans-Atlantic partner to have committed to be legally bound by the Convention, being party to it, while Canada, Mexico and the US participate as observers.

2.1. CANADA

Canada is the 'oldest' trans-Atlantic participant in the work of the Consultative Committee of Convention 108. It has been involved since 2004 under the status of observer foreseen in Art. 18.3 of Convention 108 regarding the composition of the Committee. To only refer to its most recent participation since the 30th anniversary of Convention 108, Canada attended the Plenary meetings of the Consultative Committee in 2011 and 2014. Its participation was ensured by a representative of the Ministry of Justice.

2.2. MEXICO

Mexico is the latest trans-Atlantic participant in Convention 108. It was granted observer status during the 33rd Plenary meeting of the Consultative Committee of Convention 108 (Strasbourg, 29 June to 1 July 2016), having previously participated in all meetings of the *ad hoc* committee on data protection entrusted with the task of finalising the modernisation of Convention 108. Mexico's

8 Louis Joinet, statement before the OECD Symposium on transborder data flows and the protection of privacy, Vienna, 20–23 September 1977.

participation was ensured by representatives of its data protection authority (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* – INAI) and of the Ministry of Foreign Affairs.

2.3. URUGUAY

Uruguay's became a fully fledged Party to the Convention on 1 August 2013. Uruguay was not only the first trans-Atlantic Party to Convention 108, but also the first non-Member State of the Council of Europe to accede to it. It has since regularly attended the annual Plenary meetings of the Consultative Committee. Uruguay also participated in all four meetings of the *ad hoc* committee on data protection held in 2013, 2014 and 2016, represented by its data protection authority (*Unidad Reguladora y de Control de Datos Personales* – URCDP).

2.4. UNITED STATES

After the early involvement of the United States in the life, or rather pre-life, of Convention 108, nearly three decades passed before a formal relation was established between Convention 108 and the US.

At the beginning of 2010, the Consulate General of the US requested that the US Government be granted observer status in the Consultative Committee of Convention 108. This status was granted in February 2010, thus allowing formal participation of the US representatives in the meetings of the Consultative Committee of Convention 108. US representatives attended several annual Plenary meetings (2010, 2011 and 2012) of the Consultative Committee of Convention 108, as well as several meetings of the Bureau of the Consultative Committee.

The US furthermore took part as observer in the 2013 and 2014 meetings of the *ad hoc* Committee on data protection, taking an active interest in the modernisation of Convention 108. Participation of the US in the meetings was ensured by representatives of multiple governmental sectors and institutions, i.e. by the Executive Office of the President, the Department of Homeland and Security, the State Department and/or the Federal Trade Commission.

It is important to note that the US, as Party to another Council of Europe treaty, could decide to follow a similar path in the field of data protection. After having contributed to its drafting, the US signed the Convention on cybercrime at its opening for signature in Budapest on 23 November 2001,[9] and ratified it

9 Convention on Cybercrime, ETS 185. Cf. further: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.

five years later with an entry into force in January 2007. The US acceded to the 'Budapest Convention' despite the difficulty raised by some of the provisions (in particular in light of the First Amendment's free speech principles)[10] and the concerns raised at the time by civil rights organisations. In February 2012 President Obama and his Administration released a framework for protecting consumer data privacy and promoting innovation in the global economy. The framework included a 'Consumer Privacy Bill of Rights', presented as 'a blueprint for privacy in the information age' which, while underlining the importance of 'improving global interoperability' remained silent as to any significant step of the US towards an international treaty in the field.

The calls of European Union (EU)[11] institutions, and the domestic action of civil society organisations (the US Privacy Coalition called for the US Government to support Convention 108 and proposed a resolution for the US Senate aiming at US accession to Convention 108)[12] should eventually be heard, considering in particular the precedent of the Budapest Convention, and the complementarity of both instruments in a human rights context.[13]

2.5. THE IBERO-AMERICAN NETWORK OF DATA PROTECTION AUTHORITIES (*RED IBEROAMERICANA DE PROTECCION DE DATOS*)

The rules of procedure of the Consultative Committee of Convention 108 also provide for the participation of non-state observers with a view to enabling the contribution to the work of the Committee of a wide range of actors (civil society and private sector representatives). The *Red* was granted observer status in 2009 and has since participated in meetings of the Committee, usually represented by its Presidency.

---

10 Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law*, 4th ed., Taylor & Francis, 2011.

11 See item 6 of the press release of 27 November 2013 and related Communication on 'Rebuilding Trust in EU–US Data Flows', <http://europa.eu/rapid/press-release_IP-13-1166_en.htm> and item 119 of the report of the European Parliament on 'the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs', <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN>.

12 See <https://epic.org/privacy/intl/coeconvention/>.

13 See the penultimate conclusion of the Chair of the June 2014 'Conference on Article 15 safeguards and criminal justice access to data', <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_art15Conf_Conclusions_v1e.pdf>.

3. A NEW LANDSCAPE: THE COMMITTEE OF CONVENTION 108

The Consultative Committee of Convention 108 which gathers all signatories and observers to the Convention (circa 70 participants in total)[14] is a unique forum of cooperation and exchange. Not only in the fact that it is neither a governmental committee, nor a committee of data protection authorities, but a mix of both, providing a balanced and nuanced take on current challenges. The geographic variety of its participants also enables a rich and diverse perspective on the topics discussed (such as, during the last Plenary meeting of the Committee, the automatic exchange of tax data, big data, passenger name records (PNR), health data, right to private life and freedom of expression, data processing in a law enforcement context, legal basis of cooperation between data protection authorities).

The Committee is not solely a forum of cooperation and exchange (see in particular the provisions of the Convention on mutual assistance); its policy-making role is also to be acknowledged as sectorial, and tailored guidance of the principles of the Convention has been provided in a number of fields under the impetus and productive work of the Committee.[15]

As was the case in the late 1970s and 1980s, parallel work undertaken in the Council of Europe (the modernisation of Convention 108) and in the OECD (revision of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)[16] in 2010 and the following years enabled closer exchanges between both organisations and respective experts.

4. TO ULTIMATELY TRANSCEND ALL BORDERS

Article 12 of Convention 108 on 'transborder flows of personal data and domestic law' provides for the free flow of data between Parties to the Convention. 'The aim of this article is to reconcile the requirements of effective data protection with the principle of free flow of information, regardless of frontiers ...'[17]

---

14 Fifty parties plus observers.

15 Recommendations of the Committee of Ministers of the Council of Europe in the field of data protection are prepared by the Consultative Committee (see e.g. the latest one: Recommendation (2015)5 on the processing of personal data in the context of employment). Other Recommendations can be consulted at <http://www.coe.int/dataprotection>.

16 For more information on the OECD privacy framework and the revision of the 1980 Guidelines see: <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

17 Explanatory Report to Convention 108, §62.

The authors of the Convention were concerned that

> controls may interfere with the free international flow of information which is a principle of fundamental importance for individuals as well as nations. A formula had to be found to make sure that data protection at the international level does not prejudice this principle.[18]

The 1981 text of Convention 108 was complemented in 2001 by an additional protocol to the Convention, regarding supervisory authorities and transborder data flows,[19] to specifically address the issue of data flows to non-state parties, allowed on the basis of the condition of an 'adequate' protection.

> The flow of information is at the very core of international co-operation. However, the effective protection of privacy and personal data also means that there should in principle be no transborder flows of personal data to recipient countries or organisations where the protection of such data is not guaranteed.[20]

In the context of the modernisation of Convention 108, the objective remains the facilitation of the free flow of information regardless of frontiers in full guarantee of an appropriate[21] protection of individuals. This protection has to be of such quality as to ensure that human rights are not adversely affected by globalisation and transborder data flows.

Data flows between Parties to the Convention remain free and cannot be prohibited, to the exception of what is now proposed, which corresponds to a change occurred since 1981: restrictions regarding flows of personal data relating to 'Parties regulated by binding harmonised rules of protection shared by States belonging to a regional organisation',[22] as is notably the case for the Member States of the EU. All members of the EU are also Parties to Convention 108 and the respective legal frameworks (the EU framework derives from Convention 108 and, as was expressly underlined in Directive 95/46, gives substance to and amplifies the principles of Convention 108) need to remain compatible and consistent.

The value of Convention 108 from an EU perspective is precisely linked to the adequacy[23] scheme of the EU, as underlined in Recital 105 of the General

---

18 Ibid., §9.

19 More information on the Additional Protocol at: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181>.

20 Explanatory Report to the 2001 Additional Protocol, §6.

21 The use of the word 'appropriate' instead of 'adequate' aims at distinguishing the European Union's adequacy scheme (see n 20) from that of Convention 108.

22 See modernisation proposals: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c> or at <http://www.coe.int/data-protection>.

23 See Art. 45 of the General Data Protection Regulation.

Data Protection Regulation (GDPR) of the EU.[24] This recital, in relation to Art. 45.2.c of the GDPR, states that the 'third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account' by the European Commission when assessing the level of protection.

5. CONCLUSION

It remains to be seen if the hopes and visions of the fathers of the Convention and the benefits of accession to it[25] will lead to a continuation of the regular increase in the number of Parties, as was the case over past decades, with a clear impetus towards globalisation since the thirtieth anniversary of Convention 108. This impetus, and the shift in the geographic balance of the Parties to the Convention, may well be a further incentive to accession.

Presently, accession by several African countries is pending (Cape Verde, Morocco and Tunisia have already been invited to accede to Convention 108 and are in the process of finalising their ratification procedure), countries of other regions of the world are participating as observers (Australia, South Korea, Indonesia), and others have expressed interest in either requesting observer status or joining the Convention.[26]

For over ten years there have been calls for global standards in the field of data protection.[27] There are several paths to strengthen the recognition at global level of the data protection principles and one of those paths clearly is the increase in the number of Parties to Convention 108.

This increase does not need to follow a 'region-by-region' approach, as is actually demonstrated by recent accessions to the Convention, which would tend to make it look, at this particular moment in time, more trans-Mediterranean than trans-Atlantic. Interest in the Convention is witnessed across the globe.

---

24 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

25 See Graham Greenleaf, 'Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe', 23 June 2016, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2801054>.

26 Burkina-Faso is the latest non-European country having expressed interest in acceding to the Convention and its request is to be considered by the Committee of Ministers.

27 See the 2005 Declaration of Montreux of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf>.

based on a trans-Atlantic spirit, as much as a trans-Mediterranean or trans-Pacific one: countries are interested in forming part of a recognised space within which common data protection principles are enforced.

Convention 108 was born in Europe, conceived and moulded by individuals from several regions of the world who were dedicated to providing a legal framework that would protect people and respect the free flow of information. The further development of the Convention will eventually reveal its profound nature, and demonstrate whether its open character, including in its trans-Atlantic dimension, is a dominant gene capable of taking over its original European identity.

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

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

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

1 JOSÉ SARAMAGO, *All the Names*, trans. M.J. COSTA, Harvill Press, London 2013, p. 1.

2 WILLIAM C. WILLIAMS, 'Landscape with the fall of Icarus' in *Pictures from Brueghel and other poems: collected poems 1950-1962*, New Directions, New York 1962, p. 4.

3 Musées royaux des Beaux-Arts de Belgique, Brussels, *La chute d'Icare*, inv. 4030; 73.5 x 112 cm. *Bought from the Sackville Gallery, London, in 1912*; <https://www.fine-arts-museum.be/fr/la-collection/pieter-i-bruegel-la-chute-dicare>.

4 ROBERT GRAVES, *The Greek Myths*, Penguin Books, London 1955, ch. 92; OVID, *Metamorphoses*, trans. R. HUMPHRIES, Bloomington, London 1955, 8.183–8.235.

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 *affaire*. 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.

6 Cf. esp. Lyckle de Vries, 'Bruegel's 'Fall of Icarus': Ovid or Solomon?' (2003) 30(1/2) *Simiolus: Netherlands Quarterly for the History of Art* 5–18.

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 *Míšek*, *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,[8] its 2016 decision in *Breyer*, ruling on the grounds of the 1995 Data Protection Directive[9] that a dynamic Internet protocol (IP) address constitutes personal data,[10] 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),[11] 'personal information' includes metadata.[12] 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

8 Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping* (CJEU, 6 November 2003).

9 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, [1995] OJ L 281/31–50 (hereinafter: 1995 Data Protection Directive).

10 Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* (CJEU, 19 October 2016).

11 Privacy Act 1988, No. 119, 1988 as amended.

12 Federal Court of Australia, Victoria Registry, *Privacy Commissioner v. Telstra Corporation Ltd*, Case VID38/2016; cf. also the determination by the Australian Privacy Commissioner in *Ben Grubb and Telstra Corporation Ltd* [2015] AICmr 35 (1 May 2015).

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'.[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[14] – and give evidence of the 1995 Data Protection Directive that 'lived' for only 21 years until the General Data Protection Regulation (GDPR)[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[16] and 25 October, respectively);[17]

---

13 Samuel D. Warren and Louis D. Brandeis, 'The right to privacy' (1890) 4 *Harvard Law Review* 193–220.

14 David Collingridge, *The Social Control of Technology*, St. Martin's Press, New York 1980, p. 17.

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on* the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1–88.

16 Case T-670/16, *Digital Rights Ireland v. Commission*, CJEU.

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);[20]
- 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);[21] 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;[22]
- 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);[23]
- 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] or

18 Le Conseil fédéral suisse, *Votation no 607, Résultats finaux officiels provisoires, Loi fédérale du 25.09.2015 sur le renseignement (LRens)*, <https://www.admin.ch/ch/f/pore/va/20160925/det607.html>; 'Switzerland votes in favour of greater surveillance', *The Guardian*, 25 September 2016, <https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance>.

19 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, ETS 5.

20 Investigatory Powers Tribunal (IPT), *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al.*, [2016] UKIPTrib 15_110-CH, Judgment of 17 October 2016, §101.

21 'Le Parlement wallon a opposé son veto à l'adoption du Ceta', *France24*, 17 October 2016, <http://www.france24.com/fr/20161017-belgique-parlement-wallon-veto-adoption-ceta-tafta-union-europeenne-bruxelles>.

22 Statement (No. 37) by the Kingdom of Belgium on the conditions attached to full powers, on the part of the Federal State and the federated entities, for the signing of CETA; 13463/1/16, http://data.consilium.europa.eu/doc/document/ST-13463-2016-REV-1/en/pdf.

23 Spencer Ackerman and Ewen MacAskill, 'Privacy experts fear Donald Trump running global surveillance network', *The Guardian*, 11 November 2016, <https://www.theguardian.com/world/2016/nov/11/trump-surveillance-network-nsa-privacy>.

24 Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF n° 0171 du 26 juillet 2015, p. 12735.

25 Conseil Constitutionnel, Décision n° 2016-590 QPC, 21 October 2016. Authors' translation.

- 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'.

---

26 Warwick Ashford, 'Investigatory Powers Bill looks set to become law', *Computer Weekly*, 17 November 2016, <http://www.computerweekly.com/news/450403089/Investigatory-Powers-Bill-looks-set-to-become-law>.

27 David Lyon, *Surveillance After Snowden*, Polity Press, Cambridge 2015, p. vii.

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. Nehf[30] 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

30 James Nehf, 'Recognizing the Societal Value in Information Privacy' (2003) 78 *Washington Law Review* 5.

31 Dennis Hirsch, 'Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law' (2006) 41(1) *Georgia Law Review* 1–63.

functional examples', he concludes this field is 'still in its relative infancy' and pleas 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 files[34] 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 privacy[35] 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. Greenleaf[37] 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]

---

32 Paul De Hert and Vagelis Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9 *I/S: A Journal of Law and Policy for the Information Society* 272–324.

33 International Covenant on Civil and Political Rights, New York, 16 December 1966. Cf. Art. 17.

34 United Nations guidelines concerning computerized personal data files, New York, 14 December 1990.

35 Cf. <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/JoeCannataci.aspx>.

36 United Nations, General Assembly, *The right to privacy in the digital age*, resolution A/C.3/71/L.39, New York, 31 October 2016, <http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39>.

37 Graham Greenleaf, '"Modernising" data protection Convention 108: A safe basis for a global privacy treaty?' (2013) 29(4) *Computer Law and Security Review* 430–436; Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2(2) *International Data Privacy Law* 68–92.

38 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, Strasbourg, 28 January 1981, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

39 Christopher Kuner, 'An international legal framework for data protection: Issues and prospects' (2008) 25(4) *Computer Law & Security Review* 307–317.

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),[40] either indirect (e.g. 2012 EU–US agreement on the use and transfer of Passenger Name Records).[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*[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,

40 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield, [2016] OJ L 207/1–112 (hereinafter: *Privacy Shield*).

41 Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, [2012] OJ L 215/5–14.

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'.[43] 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[44] 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>.

44 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L 215/7–47.

'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.

46 Colin J. Bennett, 'So Who is Actually "Shielded" by the Privacy Shield?', 2016, <http://www.colinbennett.ca/data-protection/so-who-is-actually-shielded-by-the-privacy-shield>.

47 [2012] OJ C 326/391–407.

48 Cf. further e.g. Orla Lynskey, 'From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis' in Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht 2013, pp. 59–84; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht 2014.

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'.[49] 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.[50]

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'.[51] 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.[52]

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

---

49 Francesca Bignami, *The U.S. Privacy Act in Comparative Perspective*, European Parliament, 2007, <http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf>.

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.

52 Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council, [2016] OJ L 344/83–91. Cf. esp. Recital 8.

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'[53] 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 gets 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.[54] 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.[55] 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

53 Peter Blume, 'Dan Jerker B. Svantesson, Extraterritoriality in Data Privacy Law [Review]' (2014) 4(2) *International Data Privacy Law* 171.

54 Cf. <http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>.

55 European Parliament, 'EU–US deal on law enforcement data transfers backed by Civil Liberties Committee', press release 20161124IPR53009, Strasbourg, 24 November 2016, <http://www.europarl.europa.eu/news/en/news-room/20161124IPR53009/eu-us-deal-on-law-enforcement-data-transfers-backed-by-civil-liberties-committee>.

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 out-dated, pre-Internet 'use of equipment' criterion determining the applicably 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.

57 L. Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1 *International Data Privacy Law* 33.

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

---

58 In the context of environmental protection, Rachel Carson popularised Jean Rostand's argument that 'the obligation to endure gives us the right to know'. Cf. Rachel Carson, *Silent Spring*, Penguin Books, London 1962, p. 30.

59 Cf. e.g. Colin J. Bennett, *The Privacy Advocates. Resisting the Spread of Surveillance*, MIT Press, Cambridge MA 2008; David Wright, Raphaël Gellert, Serge Gutwirth and Michael Friedewald, 'Minimizing Technology Risks with PIAs, Precaution, and Participation' (2011) 30 *IEEE Technology and Society Magazine* 47–54; Dariusz Kloza, 'Public voice in privacy governance: lessons from environmental democracy' in Erich Schweighofer, Ahti Saarenpää and Janos Böszörmenyi (eds.), *KnowRight 2012. Knowledge Rights – Legal, Societal and Related Technological Aspects. 25 Years of Data Protection in Finland*, Österreichische Computer Gesellschaft, Vienna 2013, pp. 80–97.

60 For TTIP, cf. <http://ec.europa.eu/trade/policy/in-focus/ttip>, and for TiSA, cf. <http://ec.europa.eu/trade/policy/in-focus/tisa>.

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, *Schaake*, 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

61 As cited in: Lee A. Bygrave, 'International agreements to protect personal data' in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham 2008, p. 15.

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 foreseen '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

64 Helen Roberts, 'Can the Internet be regulated?,' Australian Parliament, Research Paper No. 35, 1995, <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/RP9596/96rp35>.

65 Danny Yadron, 'Does Encryption Really Help ISIS? Here's What You Need to Know', *The Wall Street Journal*, 4 December 2015, <http://blogs.wsj.com/digits/2015/12/04/does-encryption-really-help-isis-what-you-need-to-know>.

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

66 Michael Kirby, 'Privacy protection, a new beginning: OECD principles 20 years on' (1995) 6(3) *Privacy Law Policy Report* 25–34.

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.

68 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1–88; Art. 32.

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

70 EDPS, *Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)*, Opinion No. 5/2016, Brussels, 22 July 2016, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf>.

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.

72 Daniel Ellsberg, 'Snowden would not get a fair trial – and Kerry is wrong', *The Guardian*, 30 May 2014, <https://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act>.

73 Council of Europe, Parliamentary Assembly, *Improving the protection of whistle-blowers*, Resolution 2060 (2015), Strasbourg, 23 June 2015, <http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=21931&lang=en>.

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

74 Ulrich Beck, 'The Cosmopolitan Condition: Why Methodological Nationalism Fails' (2007) 24(7–8) *Theory, Culture & Society* 288.

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'.[75] '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 statue (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.