Book Review

Reviewed by Knut Fournier

Email: knut.fournier@gmail.com

Data Protection Anno 2014: How to Restore Trust?
Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004–2014)
by: Hielke Hijmans and Herke Kranenborg
Published 2014
by Intersentia Ltd.
Sheraton House | Castle Park, Cambridge CB3 0AX, UK, 292pp
ISBN 978-1-78068-213-6

When Peter Hustinx retired in 2014 after ten years as the first head of the European Data Protection Supervisor (EDPS), he must have felt that the world data protection was even more at a crossroad than it was when he took office. Yet, a lot of work has been done in the decade where he was the top EU official for data protection. Three elements impacted both his tenure and the entire field of data protection: the continuous balancing of security and privacy in the fall back of the 9/11 attacks, the extensive and continuous debate over the new Data Protection Directive, and more recently the revelations of Edward Snowden that the US Government is spying on European Governments, EU institutions and citizens. In *Data Protection Anno 2014: How to Restore Trust?*, editors Hielke Hijmans and Herke Kranenborg paint a comprehensive picture of these past ten years of data protection advances, drawbacks and debates. The notion of trust, essential in a democratic society, is rightly put at the helm of the debate over data protection. Throughout the book, the various authors offer insight into the world of privacy enforcement and privacy policy professionals, in Europe and in the USA. Since the publication of the book, one could add to these motives the 'celebrity pictures scandal', in which nude pictures of actresses and models have been published on the web after their cloud accounts were hacked. Long gone is the time when Warren and Brandeis (1890, p.196) identified the press as the main threat to the right to privacy. Because data became a valuable asset for governments, companies and individuals alike, privacy is under attack from all segments of society. This last episode also turns back to the private sector and to the tech companies developing cloud computing products part of the public outrage and of the mistrust that had resulted from the NSA spying revelations. The issues of privacy and data protection in cloud computing have been addressed by a recent spade of scholarship (Nepal and Pathan, 2014; Millard, 2013; Zimmeck, 2012). Nonetheless, the book's focus on the role of the public sector is quite rightly timed, and usefully asks the questions of what has been done, and what could be done by governments, agencies and judicial institutions around the globe to reinforce data protection standards in a way that maintains the need for data exchange, while protecting the privacy of the individual. The book is written in honour of Peter Hustinx, admired and praised by the authors for

his relentless efforts towards the protection of privacy and the strengthening of data protection, during his ten years at the head of the EDPS.

Books on the right to privacy and data protection oscillate on a spectrum that begins with purely legalistic approaches, with a strong emphasis on the legal principles that underpin the protection and responsibilities enjoyed by individuals and companies, the scope of governmental powers in that regards, and the rulings of various jurisdictions that decide on these matters. On the other end of this spectrum, an entire branch of the privacy and data protection scholarship is searching in cross-disciplinary tools and methods the necessary answers to the shortcomings of legal enforcement of privacy rights (Catudal, 2001). *Data Protection Anno 2014: How to Restore Trust?* manages to avoid these two poles and rather seeks in actual narratives of practitioners the real issues and the proposed solutions to advance both privacy and data protection for the 21st century. In *How to Restore Trust?*, the notion of public confidence is tightly linked to the rule of the law and to the principles of transparency and accountability, which the authors see as the most convincing protections against privacy violations and unfair data processing.

The analysis of the 28 authors of the book takes place at three different levels. Domestic first, with a look at some developments at the national level (the USA or the Netherlands). At the European level then, where most of the authors are professionally active. And transatlantic finally, a central point in the book, as the authors make a compelling point that the future of privacy protection depends on the links across the pond. Some of the case studies at the Dutch level are particularly insightful, particularly the failed attempt to update the Dutch constitution to strengthen the right to privacy and specifically link data protection provisions to it. However, the real substance of *How to Restore Trust?* lies in the comparison of the different jurisdictions involved, in the variations across the borders between rights, level of enforcement, and political willingness to turn principles into binding rules.

From this state of things, the authors derive a series of themes that are quite intelligently treated all together rather than one by one [the Google case and Google Spain case had not been issued by the Court of Justice of the European Union at the time of writing of *How to Restore Trust?*, and therefore, the 'right to be forgotten' is not addressed in the book, with the exception of two authors who mentions the background of the case and the possible routes offered to the CJEU (pp.92–94)]. A foundational element of this work is the interplay between the right to privacy and data protection. The clarifications brought by the book and by chapter 7 in particular are extremely useful, not only in understanding the differences between the two concepts, but also their different scope (pp.89–91) and interplay (pp.91–92). These interactions are not described at the theoretical level, but rather with a practical perspective on the effects and the shortcomings of each of these two different but highly interlinked topics. In terms of scope, the definition of private data, found in the Data Protection Directive (European Council and European Parliament, 1995) is rather wide, and encompasses any information potentially that can be collected on the individual and which relates to the individual. The Data Protection Directive is a strong piece of legislation, notwithstanding the fact that it is outdated and not necessarily adapted to a world where the most significant data flows are cross-border, thus raising the issue of jurisdiction. Article 3 of the Data Protection Directive concerns "the processing of data wholly or partly by automatic means, and the processing otherwise than by automatic means of personal data which forms part of a filing system or are intended to form part of a filing system". In

effect, this extends the scope of European data protection rules to all computer systems, without any possibility of way around it [Bernal, (2014), pp.88–89] A contrario, privacy has not been defined by the legislator and is left to the courts, who added or removed elements of daily life from the plain English meaning of the term, to gradually delaminate privacy as a legal concept. The result of this judicial exercise is a scope that is much more restricted than the data protection concept. Although the two elements depend on, and possibly enrich each other, privacy has been an issue for the courts while data protection has been addressed at the legislative level, relieving judges from the tedious task of defining the concept. From these different scopes, and origin naturally results a vastly different level of protection. Juliane Kokott (Advocate General at the CJEU) and her Legal Secretary Christoph Sobotta provide in chapter 7 a clear and useful explanation of how the permissible interferences for privacy and data protection bring together the two concepts. When processing data under the data protection rules, actors must take into account the M.M. case of the European Court of Human Rights, which states that the level of justification to limit data protections (when governments or private actors collect personal data and make them readily available for disclosure) must be adequately tailored to the sensitivity level of the data collected. In this case, the Strasbourg court has ensured that security concerns could not simply be raised to restrict data protection rights when collecting and disclosing the data involved would in fact put privacy at risk.

The new reform of the Data Protection Directive is a recurring topic of the book. In 2012, the European Commission proposed a rewriting of the 1995 Data Protection Directive, to ensure a one-stop-shop for all privacy issues in Europe, a uniform law in all member-states, and an equal enforcement of rules against EU and non-EU companies under the jurisdiction model currently applied to competition rules. The issues raised by the proposed reform all revolve around the impact of the new directive. Quite rightly, the authors of *How to Restore Trust?* highlight the high level of uncertainty around the effect of the reform. The recurrent message from the book's authors is that the new data directive will not be a revolution. Rather, most authors agree that the new European framework for data protection is a difficult exercise. In addition to facing intense pressures from the private sector, the authors of the directive are pursuing two ambitious objectives. First, to harmonise data protection across 28 EU member states, when the current data protection rules have essentially been interpreted in 28 different ways. Secondly, the even more ambitious objective of ensuring EU citizens a high level of protection whenever their data is processed outside the EU.

Finally, this book will not be able to pretend to a positive impact on privacy and data protection scholarship without turning its focus to the relationship EU-US. Even in purely European matters, the spectre of the transatlantic relationship is hard to miss: the pressures from the US Government and American tech companies in the context of the reform mentioned above bring that home perfectly. This focus is particularly appropriate, because of the major event that preceded the publication of this book: the Snowden revelations and the accompanying documents leak. This exposed the across-the-board spying programmes of the US secret services, resulting in the tapping of European heads of state, EU institutions and officials, and the recording of virtually all voice and electronic communications from EU countries. Sophie in't Veld, MEP, writes about "mass surveillance, wiretapping, espionage, government surveillance of citizen making Big Brother look like an amateur" (p.175). With the limits that are inherent to a text written by an elected politician, her contribution nonetheless expresses perfectly the outrage and the resentment of Europeans that have been treated as a threat by one of their

oldest allied. Behind her diatribe against American warrantless surveillance of European communication, one can feel a fundamental shift that is also visible in other chapters of *How to Restore Trust?*: before the Snowden revelations, the debates over data protection and privacy were shaped and defined by the relationship between the US and the EU. After the massive surveillance documents leak, it is on the contrary the future of EU-US relations that depend on, precisely, a new framework for data protection. In this context, the contribution of Julie Brill from the FTC in the following chapter is particularly welcome in explaining in detail the scope and the effects of the FTC's powers to enforce data protection rules. It also provides a solid basis for chapter 18, where Daniel Weitzner details the way privacy policies are implemented in the USA, the effect of laws and regulations, and the relationships between government and the private sector (pp.199–202). However, this part of the book also seems the most oblivious of the issue that is the reason for this book: the broken trust, and the need to find ways to rebuild it. Weitzner mentions for instance that "from the very first days of President Obama's first term in office, his Administration showed renewed commitment to privacy protection…" (p.203) a claim that will sound misleading to the half-billion Europeans who have been spied on by this very same administration. The differences and similarities between the two systems of data protection, originating not in the different conceptions of the right to privacy in the US and the EU as it is often believed, are highlighted in detail and in a constructive way. The practical approach taken throughout the book results in a very convincing picture of two systems that can, notwithstanding their differences, collaborate and result in mutually beneficial cooperation agreements and programmes. However, another picture emerges implicitly to the claims that the American judicial and administrative is designed to protect consumer's right to privacy through transparency and accountability: the picture of a two-tier privacy protection system, where the US Government, very active in data protection enforcement, is also the world's biggest threat to the right to privacy.

In 2014, data protection exists in a state of paradox: it is ubiquitous in the news, it is affecting the life of nearly every individual and it is present in the life of every company and in political debates. Yet, it is unclear whether this means that privacy is taken seriously or whether it is more threatened than before. The authors attempt to propose solutions to deal with these two contradicting trends, and by doing so identify another gap, more substantial in terms of concrete effects: the gap between laws and actual enforcement. In the course of their analysis, they deploy the argument that another perceived gap, between a supposedly government-centred US data protection framework and more private-centred EU privacy protection rules, does not sustain a close analysis.

There is an almost inevitable self-congratulating element in a book written by professionals. In the present collaborative work, nearly all the 28 authors are working in the field of privacy, data protection, or at domestic and European institutions with a mandate or an interest in enforcing and regulating data protection. Several authors are members of data protection authorities, the European Parliament, the EDPS, domestic or European courts, and the European Commission. Across the Atlantic, Julie Brill speaks for the Federal a Trade Commission. All the authors are of a very high calibre and are authorities in their field. Notwithstanding that academics are a minority among the authors, the very few chapters that are designed to present the work of an institution – to which the author belongs – are helpful and provide a welcome insight into, for instance,

the role and track record of the FTC in enforcing data protection rules in the USA (pp.179–190).

Hijmans and Kranenborg have undergone a tremendous piece of work, with a very practical focus that is often missing in the legal literature. The book would have greatly benefited from a solid discussion of the right to be forgotten, and of the fact that the upcoming data protection directive intends to codify this principle. However, the timing of the publication, right before the Google and Google Spain decision, made this difficult. The authors brought together the best minds of privacy and data protection of the continent and balanced their views with the US perspective. Their book calmly presents arguments from both sides of the Atlantic, at a time when the relationships between the EU and the US are endangered by, precisely, privacy concerns. Restoring trust was an ambitious task. Their work lays the foundations for the necessary healing and soul-searching, through two main findings: firstly, that "[t]rust amongst countries can be restored by developing more global solutions for data protection" (p.14). By addressing the issue from the perspective of judicial and administrative enforcement, the authors shed light on the most effective way towards these global norms: joint practice. Secondly, the notion of control must be placed at the centre of future policies, legislations, and enforcement efforts. Without regaining control on personal data at all levels, privacy fears will remain a scar in the EU democratic principle, and in the US-EU relationship.

References

Bernal, P. (2014) *Internet Privacy Right: Right to Protect Autonomy*, Cambridge University Press, Cambridge, UK.

Catudal, J.N. (2011) *Privacy and Rights to the Visual: the Internet Debate*, Rowman & Littlefield, Lanham, MD, USA.

European Council and European Parliament (1995) *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*, Official Journal L 281 of 23.11.1995.

Millard, C. (2013) *Cloud Computing Law*, Oxford University Press, Oxford, UK.

Nepal, S. and Pathan, M. (2014) *Security, Privacy and Trust in Cloud Systems*, Springer, Berlin Heidelberg, Germany.

Warren, S.D. and Brandeis, L.D. (1890) 'The right to privacy', *Harvard Law Review*, Vol. 4, No. 5, pp.193–220.

Zimmeck, S. (2012) 'The information privacy law of web applications and cloud computing', *Santa Clara High Technology Journal*, Vol. 29, No. 3, pp.451–487.