Book Reviews

The Book Reviews section will introduce you to the latest and most interesting books on a wide range of topics pertaining to the law and policy of data protection. For further information on the submission of reviews please contact the Book Reviews Editor Bart van der Sloot at b.vandersloot@uva.nl.

Reforming European Data Protection Law
by Serge Gutwirth, Ronald Leenes and Paul de Hert (eds.)
Springer, 2015, 406 p.
€ 137,79; Hardcover

*Bart van der Sloot**

Reforming European Data Protection Law is the conference book of the yearly Computers, Privacy and Data Protection conference held in Brussels. This is the conference book of the year 2014. The conference is by now the standard (legal/policy) conference to go to in Europe for everyone interested in privacy, data protection and technology. This book contains the best papers presented at the conference (and papers written in the conference's slipstream), which already hosts the fine fleur of international privacy scholars, regulators and activists.

The book is divided in five parts. The first part contains two chapters on profiling, the second part consists of four chapters on risk assessments, the third part offers three papers on the right to be forgotten, the fourth part provides the reader with two chapters on the balance of privacy and security and finally, part five contains five chapters on data protection by design and related issues. There are many contributions in the book that deserve careful reading, such as the first chapter (Bosco, Creemers, Ferraris, Guagnin and Koops) with a careful attempt to define profiling, the third chapter (Geminn and Rossnagel) laying down a systematic approach to the legal evaluation of security measures, chapter 9 (Zanfir) which discusses the origins of the right to be forgotten, chapter eleven (Leese) on the evolution of the conflict between privacy and security in Europe, chapter fourteen (Trepte, Teutsch, Masur, Eicher, Fischer, Hennhöfer and Lind) on empirical research on privacy awareness and chapter sixteen (Stevovic, Bassi, Giori, Casati and Armellin) on the use of privacy by design in medical records sharing. However, it goes too far to discuss each chapter in detail. Rather, three contributions will be reviewed in more detail, one from part two, one from part three and one from part four.

Part two, concerning risk assessments, contains an interesting chapter by Leon Hempel (Centre for Technology and Society, Berlin) and Hans Lammerant (Law Science Technology & Society, Brussel) titled "Impact Assessments as Negotiated Knowledge". As is well known, the General Data Protection Regulation, which will replace the current Data Protection Directive in time, specifies that data controllers may have the obligation to engage in risk assessments and impact assessments as part of their general duty of care. Impact assessments are generally seen as tools that enhance data protection by laying down an extra obligation for data controllers with an eye on preventing harm to data subjects. Hempel and Lammerant, however, take a more critical view. They engage with Ulrich Beck's theoretical approach proposed in his widely acclaimed book Risk Society. They argue that, first of all, risk assessments are not only legal or technical instruments, they should be approached rather as political instruments. Impact assessments decentralize power and responsibilities. Drawing from previous lessons learned in relation to Environmental Impact Assessments, on which the idea of Data Protection Impact Assessments (DPIAs) is based, they conclude that DPIAs are rather the outcome of a political process in which there are negotiations on what is considered a "risk", how this is measured and in what way this is assessed. These are not fixed principles, there is not one way to conduct DPIAs. Rather, every DPIA is the unique outcome of a political process and of the negotiations by the stakeholders. This also means that impact assessments do not bring the unbridled truth – they cannot be viewed merely as tools that bring transparency and knowledge to the often politicized decision making process with

* Bart van der Sloot is Researcher at the Institute for Information Law, University of Amsterdam; b.vandersloot@uva.nl.

regard to data protection. Rather, they must be regarded themselves as the outcome of a politicized decision making process. "Impacts", they conclude, "are not value-free notions but stand for impacts on recognized interests. As such, impact assessments are also derived in negotiations, and the knowledge produced on impacts is negotiated knowledge." This chapter is certainly worthwhile reading for everyone interested in DPIAs and for those looking for a slightly more critical approach. The chapter is very well written and offers a new perspective on a heavily debated topic.

Chapter 7 consists of a collaboration by the speakers of a panel at CPDP on the right to be forgotten. Consequently, there are seven authors, namely Paulan Korenhof (Tilburg Institute for Law, Technology, and Society), Jef Ausloos (Faculty of Law, Leuven), Ivan Szekely (Open Society Archives, Budapest), Meg Ambrose, (Communication, Culture & Technology Department, Washington), Giovanni Sartor (European University Institute, Florence) and Ronald Leenes (Tilburg Institute for Law, Technology, and Society). The chapter is titled "Timing the Right to be Forgotten: A study into 'time' as a factor in deciding about retention or erasure of data". It deals, as the title suggests, with the element of time in respect of the right to be forgotten. It draws lessons, among others, from the natural capacity of humans to remember and more specifically, the human tendency to forget (or even disregard) most information available to them. Whether a person remembers a particular fact, study shows, depends on the passing of time, the meaning of the information (the relevance) and the regularity with which the information is used. Of course, however, the internet is different from natural memory. First of all, it is an external memory, a tool used for remembering. Humans have of course used such tools since the dawn of time. However, different from other external memories (such as books), the internet is best defined as a transactive memory. This means that the content of the memory constantly changes and that it can be altered by many people; the memory, in this sense, is democratized and depended on many people, rather than on one single author. This means also that the claim that the internet is an archive is denied by the authors – at most it is a lazy historian, they claim. Subsequently, the authors analyze how the element of time already plays a role in current privacy and data protection rules. They discuss, inter alia, the notion of consent, the legitimate interests of the data controller, the purpose specification principle, the right to object, the storage of data and data retention, and show how time affects these doctrines. The authors continue with three very insightful graphs in which they demonstrate how the element of time and the impact of data processing affects, inter alia, the interests of the data subjects, of the uploaders of information and of the provider. For everyone interested in the right to be forgotten, this chapter is a must read – perhaps this is the best contribution of the book.

Chapter 10 is written by Govert Valkenburg (Faculty of Arts and Social Sciences, Maastricht) and is titled "Privacy Versus Security: Problems and Possibilities for the Trade-Off Model". This chapter addresses the thorny issues of balancing or weighing different interests, which has been done to death in the privacy and security discourse. If the balancing approach is applied, it is mostly to argue that security interests outweigh privacy interests, as security is more important or because national security serves a general interest, while privacy only serves the personal interests of specific individuals. This, of course, to the dismay of privacy advocates, liberal politicians and many privacy scholars. The author of the chapter discusses the arguments often put forward against the balancing of interests, but also proposes new arguments for applying the metaphor of balancing. As an example, the chapter discusses the complexities of the practice of body scanners installed at airports for security purposes. The author argues that the balancing act is problematic only when it is used as a simple justification for imposing security measures that encroach privacy, for example, by using the argument "this small piece of privacy must be sacrificed in order to promote national security". The author argues that the trade-off model could still be used as a heuristic device to trace potential difficulties in the application of security technologies. In doing so, the author hopes to challenge two extreme positions, namely those who use the model to argue that privacy should by default be overruled by national security interests and those who say that the balancing act should be abandoned altogether, as both privacy and security should be retained without one being sacrificed for the other. Rather, the author urges the reader to take a nuanced approach and to acknowledge the complexities often at stake in these kinds of decision making process. This contribution is certainly well written and worthwhile reading. It

provides the reader with a good starting point for reading more about the quite elaborate scholarly discussion on the idea of balancing and of weighing interests as such. For example, how can moral interests be weighed in the first place (they have no weight, there is no uniform scale on which to weigh them and no commonly accepted/standard method of weighing)? Is the weighing of interests suitable with regard to human rights such as privacy (human rights were designed to protect the basic conditions of human existence, not as relative interests which can be overruled if the benefits outweigh the costs)? Etc. Consequently, the reader should use the insightful and very detailed work of Govert Valkenburg as an introduction in the wide literature skeptical of the idea of balancing moral interests as such.

The Black Box Society. The Secret Algorithms That Control Money and Information
by Frank Pasquale
Harvard University Press, 2015, 311 p.
€ 31,50; Hardcover

*Alessandro Spina**

A skeptical view holds that Big Data is only a commercial buzzword in the field of technology, the last in a series of similarly ambiguous and ephemeral concepts used to define potential revolutionary applications of digital innovation such as *2.0* or *crowd-intelligence*. However, the scale of data processing is unprecedented and extraordinary: it may suffice to recall that every minute there are approximately four millions searches on Google. Further evidence is in the way "connected" individuals access information and make decisions in everyday activities from purchasing goods or services to interacting with friends through social networks. The concept Big Data captures not only the immense quantity of data now available but also to the sophisticated analytical capacity of organisations to use the data and extract knowledge. This represents a new form of "algorithmic" power – as brilliantly exposed few years ago by Viktor Mayer-Schönberger and Kenneth Cukier in *Big Data. A Revolution that will transform how we live, work and think* (2013). While the implications of algorithmic power have been so far both under-explored and under-estimated in legal doctrine, however the book *The Black Box Society* fills this gap with an important, intelligent and timely contribution. The book will be an important reference for informing public debates about privacy and data protection, in particular in Europe where new legislation, the General Data Protection Regulation (GDPR), specifically conceived as a reform of EU data protection law in order to meet the challenges of the digital economy is currently under consideration. His Author, Frank Pasquale, a Professor of law at the University of Maryland, has written extensively on search engines and digital reputation, transparency and informationlaw; he is an active blogger (on www.concurringopinions.com) and tweeting scholar.

The book is composed of six chapters: in the first two chapters (I and II) the Author offers an introduction to and an overview of algorithmic power. The following two chapters (III and IV) present a more in-depth analysis of this emerging form of algorithmic power; chapter III is dedicated to the activities and practices of Internet companies, in particular operators of digital search engines, such as Google; chapter IV focuses on the the finance industry and how Big Data technologies have become embedded in its practices. The final two chapters (V and VI) would like to present the reflections of the Author for addressing the problems raised and discussed in the preceding chapters, setting out legal and political solutions for a re-balance of algorithmic power in our society.

In the introduction, the Author conveys two major ideas about the relevance of concepts such as information, knowledge and power in the era of Big Data. The first is that, at the core of the information economy, the success of individuals, business and their products is crucially based on reputation, and reputation depends heavily on the synthesis of data and perceptions. Therefore, those organizations that rank, index, or rate individuals or business (e.g. through credit scoring) yield a considerable and often unaccountable power – which can be captured by the metaphorical image of the "blackbox". The second point is that there are different strategies by which these organisations maintain this asymmetrical power. One obvious strategy is the use of secrecy, which can be declined either in the form of the "real" or "le-

* Alessandro Spina is Data Protection Officer at the European Medicines Agency, London; alessandro.spina@ema.europa.eu. The views expressed in this book review are those of the sole author.