Editorial

With the rise of new technologies that enable big data, the internet of things, cloud computing and the quantified self, the processing of personal information is becoming increasingly prominent. Intelligence services and police forces collect metadata to combat global terrorism and prevent crime, and companies across sectors engage in targeted advertising and personalized profiling to optimize their services. Many of these data processing activities are not bound to specific regions or countries: governmental organisations share their data with their foreign counterparts, companies collect and store data in diverse jurisdictions, and citizens publish their own data and those of others on global Internet sites such as Facebook, Twitter and Instagram. However, transnational data flows create tensions, especially with respect to data transfers between the European Union (EU) and the United States (US). The two jurisdictions have a quite different approach to privacy protection and other rules that set limits on data processing activities. Although this tension has existed for decades, it has gained new momentum after the recent *Schrems* decision by the Court of Justice of the European Union (CJEU), which struck down the legal basis for transferring personal data from the EU to the US.

Because data processing has become so central to the operations of many private and public sector organisations, and because data processing is becoming increasingly transnational, the difference in approach to privacy protection in Europe and America is becoming a serious obstacle. However, finding a solution is proving difficult. On the one hand, too strict restrictions on transnational data flows may seriously hamper the fight against crime and terrorism, the possibility for businesses to operate on a global scale, and the freedom of citizens to share their data with friends around the world. On the other hand, lowering the level of protection or compromising the standards currently engrained in regulation might have a significant negative impact on both individual and societal interests. Although the goal is to produce a framework that facilitates transnational data flows while providing privacy and other interests with a high level of protection, recent developments on both sides of the Atlantic seem to suggest that the EU and US are adopting conflicting approaches, therewith deepening the regulatory divide.

The current tensions have various negative effects. On a diplomatic and political level, the revelations by Snowden have created distrust among parliaments. On an economic level, European companies complain of a competitive disadvantage in comparison to their American counterparts, because they have to abide by the strict European rules, and American companies increasingly face harsh economic sanctions for violating European privacy and data protection principles. On a technological level, double standards are sometimes adopted to make products and services suitable for both markets, and occasionally technologies that have already passed the initial roll-out phase need to be recalled, because they do not adequately meet the privacy and security standards in either Europe or the US. And on a societal level, citizens are los-

ing trust in governments and companies, and out of fear of being monitored, curtail their behaviour or use alternative means of communication.

Given these potential problems, the general consensus is that we need a balanced approach, one in which transatlantic data flows are facilitated, while sufficient respect is shown for the fundamental rights of citizens. For example, the European Commission (EC) issued a communication to the European Parliament and the European Council titled 'Rebuilding Trust in EU–US Data Flows'. It stressed the need for more cooperation between the US and the EU, called for more understanding of each other's positions and suggested that shared standards could be developed, resulting in a common international framework. A number of initiatives are being undertaken to improve the transatlantic relationship on this point, such as the negotiations over the Transatlantic Trade and Investment Partnership (TTIP) and over possible closer cooperation in the field of law enforcement. Perhaps most importantly, the Privacy Shield agreement is being negotiated. The agreement will replace the Safe Harbour framework that formed the basis for the transatlantic data flows, until it was struck down by the CJEU. In the beginning 2016, the EC released a press statement in which it made public that post-*Schrems* negotiations had led to the new Privacy Shield agreement, which featured enhanced privacy and data protection rules.

Although there are signs of rapprochement, it is uncertain how successful, stable and enduring new agreements will be. There is a lot of distrust on both sides of the Atlantic. For example, when the draft Privacy Shield agreement was published, EU parliamentarian and spokesperson in the field of privacy Sophie in 't Veld immediately issued a strong statement: 'This will not stand in court. The deal was made under immense pressure from the US, its secret service and American businesses. The European Court has been very clear where the boundaries lie, and the guarantees that are provided by this agreement have no legal value.'[1] Similarly, however, there is a sentiment among many American experts and officials that the European understanding of the US system is weak, one-sided and full of misconceptions. For example, David Bender wrote a very critical analysis of the *Schrems* decision and pointed out that the CJEU should have done more extensive and careful research to get a better grasp of the American privacy approach. After discussing a number of fundamental misconceptions, he concluded by stressing that: '… [w]e now find ourselves in a situation defined by a final and unreviewable CJEU decision, on an issue never presented to that court and which it went out of its way to appropriate, based on 'facts' established in a peculiar manner by essentially pulling them at face value out of incorrect news reports, by ignoring corrected new reports, by likewise ignoring significant changes that had occurred since the reported events, and by wearing blinders to the fact that EU surveillance is less privacy friendly than US surveillance.'[2]

1 'EU en VS sluiten politieke deal om je data te beschermen' [EU and US close a political deal to protect your data] *RTL nieuws* (2 February 2016) <http://www.rtlnieuws.nl/economie/home/eu-en-vs-sluiten-politieke-deal-om-je-data-te-beschermen> accessed 17 June 2016.

2 D Bender, 'Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective', *International Data Privacy Law* (13 May 2016).

This edition of EdpL focusses on transatlantic data flows between the EU and the US, in the hope to gain more knowledge and understanding of the supposed transatlantic privacy divide. It contains articles on this topic by Gloria Gonzalez Fuster, research professor at the Free University in Brussels and author of the standard book on data protection *The Emergence of Personal Data Protection as a Fundamental Right of the EU;* by Berkeley professor Chris J. Hoofnagle, author of the must-read on the FTC *Federal Trade Commission. Privacy Law and Policy;* by Franziska Boehm, professor at the Karlsruhe Institute of Technology and author of the book *Information sharing and data protection in the Area of Freedom, Security and Justice;* by Svetlana Yakovleva and Kristina Irion from the Institute for Information Law of the University of Amsterdam, both leading experts in the field of governing digital information; and an article by Helena Ursic and Bart Custers, both working at the University of Leiden and the latter being the first editor of the book *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases.*

As always, the reports section led by Mark Cole deserves special mention. It provides the reader with an almost complete and very insightful overview of the most important privacy and data protection developments in several European countries. It contains reports on the Netherlands, written by Sarah Johanna Eskens, on Hungary, written by Gergely Laszlo Szőke, on Italy, by our associate editor Alessandro Mantelero, two reports on the United Kingdom, by Lorna Woods, one report on Spain, written by Juan Jose Gonzalez Lopez and Julio Perez Gil, and finally, a report on the Review of the ePrivacy Directive by Jos Dumortier. The case note section contains comments on five cases by the European Court of Human Rights and the CJEU and the book review section offers a discussion of the book on the FTC by Chris J. Hoofnagle, mentioned earlier, and a book by one of our board members Orla Lynskey.

But before the articles, reports, case notes and book reviews, this edition is honored by two forewords by Max Schrems and Julie Brill.

Finally, we are proud to announce a new member joining our editorial board, namely Marc Rotenberg, who we are certain needs no introduction.

We hope you will enjoy reading EdpL's second edition of 2016!

Bart van der Sloot
Institute for Information Law
University of Amsterdam