EDITORIAL NOTE

Foreword*

In *The Right to Privacy*, one of the most influential law review articles of all times, two brilliant Boston lawyers named Louis Brandeis, the future Supreme Court justice, and his law partner Samuel Warren wrote in December 1890[1]:

> The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature. Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'.

Frustrated by the increasing intrusions into individual privacy by nineteenth century journalists who employed the latest technological innovations of their time,[2] such as photography, Warren and Brandeis argued that it was necessary for the courts to recognize the right to privacy (or the right 'to be let alone'). They described the right to privacy as the right of each individual to protect his/her inviolate personality, as information about an individual's private life, when disclosed to others, may 'influence and even injure the very core of an individual's personality – "his estimate of himself "'.[3]

Now, 130 years later, our privacy and data protection concerns are more intense.[4] Society, media, and technology have changed drastically. New technologies are capable of tracking our actions, our movements, our lives, even our thoughts and emotions.[5] The intimacies of our lives can be exposed to billions of people worldwide in an instant.[6] Deepfake technology has been increasingly used to swap people's faces into pornography,[7] misrepresent well-known politicians in videos,[8] or as part of social engineering scams.[9] Rapid advances in AI, robotics, and so-called 'autonomous technologies' (from self-driving cars to Lethal Autonomous Weapons) raise safety and security concerns.[10] Disturbing predictions in the dystopian Netflix series *Black Mirror*[11] are not that far-fetched.[12]

How should our laws and legal institutions respond to these threats? And, as the EU Commission asked in its report, how should they be 'redesigned to make them serve the welfare of individuals and society and to make society safe for this technology?'[13]

Notes

* Special thanks to Nick Potter (Linklaters, Madrid) for proofreading this editorial note.

1 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).

2 Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 Cath. Univ. L. Rev. 703 (1990).

3 Dorothy J. Glancy, *The Invention of The Right to Privacy*, 21 Ariz. L. Rev. 1 (1979), citing Warren & Brandeis, *supra* n. 1, at 197.

4 Samantha Barbas, *Saving Privacy from History*, 61 DePaul L. Rev. 973 (2012).

5 Jamie Fullerton, *'Mind-Reading' Tech Being Used to Monitor Chinese Workers' Emotions*, The Telegraph (2018).

6 Barbas, *supra* n. 4.

7 Danielle Keats Citron, *Sexual Privacy*, 128 Yale L.J. 1870 (2019).

8 Grace Shao, *Fake videos Could Be the Next Big Problem in the 2020 Elections*, CNBC (2019), www.cnbc.com/2019/10/15/deepfakes-could-be-problem-for-the-2020-election.html.

9 Jesse Damiani, *A Voice Deepfake Was Used to Scam a CEO Out of $243,000*, Forbes (2019), www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#351a2d032241.

10 European Group on Ethics in Science and New Technologies, European Commission, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems* (2018).

11 Television series created by Charlie Brooker.

12 Alice Vincent, *Black Mirror Is Coming True in China, Where Your 'Rating' Affects Your Home, Transport and Social Circle*, The Telegraph (2017), www.telegraph.co.uk/on-demand/2017/12/15/black-mirror-coming-true-china-rating-affects-home-transport/.

13 European Group on Ethics in Science and New Technologies, European Commission, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems* 8 (2018).

In the nineteenth century, according to Barbas, the right to privacy was envisioned by Warren and Brandeis 'as a means to address what were perceived as serious threats to privacy and identity posed by the new media of the day – yellow journalism, gossip columns, and Kodak photography'.[14]

Today, we are yet to find a means of addressing what we now perceive as serious threats to privacy and identity posed by ever-advancing technology. And this is no easy task.

We may (still) have 'zero privacy', as Sun Microsystems chief executive Scott McNealy famously said twenty years ago, but we have not yet 'gotten over it'.[15] The privacy and protection of personal data have never been more relevant or important than they are today. We need a serious debate and research into these topics. Only then, perhaps, just like Warren and Brandeis did in the well-known *Harvard Law Review* in 1890, can we, as lawyers, professionals, researchers or scholars, also come up with ideas and/or answers to the above questions and deal with the challenges of today and tomorrow.

With this aim and high ideal in mind, I am very proud to launch the *Global Privacy Law Review (GPLR).* This is a new law review dedicated to in-depth discussions of privacy, data protection, and cybersecurity. I believe that the GPLR fills a gap in the existing legal literature by providing a global forum for critical analysis and debate and offering top-quality scientific research articles and practical insights as well as thorough legal analysis.

My sincere gratitude and appreciation goes to the founding members of our top-notch editorial board: Boris Paal (University of Freiburg), Cecilia Álvarez (Facebook), Célia Zolynski (Université Paris 1 Panthéon-Sorbonne), Diego Fernandez (Marval, O'Farrell & Mairal), Jason Flint (Barclays), Jordan M. Blanke (Mercer University), Kaori Ishii (University of Chuo), Kirsty Hughes (University of Cambridge), Knut Mager (Novartis International), Leonardo Cervera, European (European Data Protection Supervisor), Leyla Keser Berber (Istanbul Bilgi University), Mark Keddie (formerly Dentsu Aegis), Michael Birnhack (Tel Aviv University), Nadya Purtova (Tilburg University), Nikolaus Forgó (University of Vienna), Oreste Pollicino (Bocconi University), Simon Chesterman (National University of Singapore), Sylvain Métille (University of Lausanne), Tanguy Van Overstraeten (Linklaters), Thiago Luís Sombra (University of Brasília), Viljar Peep (Estonian Ministry of Justice), and Vincent Gautrais (University of Montreal). And, of course, all the Wolters Kluwer International team, including, among others, Christine Robben, Laurien Roos, Claire Chouzenoux, and Anja Kramer. Without their amazing work, this would not have been possible.

We dedicate this first issue to new and emerging technologies, with seven scientific articles from excellent authors contributing to this debate at the highest level.

We start the review by paying tribute to European Data Protection Supervisor (EDPS) Giovanni Buttarelli, who sadly passed away on 20 August 2019. He was an inspirational and knowledgeable leader. His intellect, passion, and personal warmth made him an admired and beloved member of the international privacy and data protection community. Our editorial board member, Leonardo Cervera Navas, Director of the EDPS, who knew and worked very closely with Giovanni, shares his memories and thoughts.[16] Giovanni will be sorely missed. Our thoughts are with his family, colleagues, and loved ones.

Judge Carlota Cuatrecasas (*Legal challenges of AI*) analyses the effects of new technologies and AI in the legal field. She defines AI as a double-edged sword, which could have great benefit for humanity but could also pose an equally great threat to citizens' rights, including potential human rights violations. The author discusses the role that the Law should play in regulating the use of modern technology and guaranteeing citizens' rights. Judge Cuatrecasas highlights the risks that AI may bring when used by judges in legal proceedings, such as having a greater influence on judges than desired. She concludes that it is crucial for society to be informed and for policy-makers to take responsibility.[17]

Assoc. Prof. Dr Leyla Keser Berber and Ayça Atabey (*Addressable TV and Consent Sequencing*) discuss the opportunities that addressable TV brings to the advertising industry by allowing advertisers to purchase audiences, as opposed to traditional methods of buying based on programming. However, the authors find that the increasing popularity of addressable TV also raises concerns regarding the notion of 'consent'. Keser and Atabey note that such concerns are due to the intrinsic nature of addressable TV technologies, especially considering the targeted audience at household level and ads delivered to different individuals including children, who merit specific protection. The authors address the practical challenges that are likely to appear in the near future with regards to data protection and privacy laws and conclude by making tangible suggestions not only to protect users, but also to help addressable TV thrive even more in the future.[18]

Notes

[14] Samantha Barbas, *Saving Privacy from History*, 61 DePaul L. Rev. 973 (2012).

[15] The famous phrase, 'You have zero privacy anyway. Get over it' has been attributed to Scott McNealy, former CEO and co-founder of Sun Microsystems. Polly Sprenger, *Sun on Privacy: 'Get Over It'*, Wired (1999), www.wired.com/1999/01/sun-on-privacy-get-over-it/.

[16] Leonardo Cervera Navas, *In Memoriam: Giovanni Buttarelli*, in this issue, at 5.

[17] Carlota Cuatrecasas, *Legal Challenges of AI*, in this issue, at 6.

[18] Leyla Keser Berber & Ayça Atabey, *Addressable TV and Consent Sequencing*, in this issue, at 14.

Inés Isidro and I (*Blockchain and Data Protection: a compatible couple?*) discuss blockchain technology, which is best known as the underlying technology behind cryptocurrencies such as Bitcoin. Blockchain has emerged as one of the technological innovations with the greatest potential to transform the economy and society. As various European data protection authorities point out, in order to understand the risks that the use of blockchain technology could pose, it is necessary to examine the architecture and the specific characteristics of the technology in question, in particular the way in which personal data are stored or processed. Thus, the impact of blockchain on the privacy and personal data of data subjects generally requires analysis on a case-by-case basis. We conclude that, while there are some tensions to be resolved, blockchain technology is not per se incompatible with the GDPR.[19]

Prof. Fumio Shimpo (*The Importance of 'Smooth' Data Usage and the Protection of Privacy in the Age of AI, IoT and Autonomous Robots*) discusses the emerging technologies of AI and autonomous robots and the increasing need for research on the legal and ethical issues arising from such technologies. The author focuses on the possibilities of privacy violations and issues related to the processing of personal data with an introduction to the Japanese Personal Information Protection Act. He further discusses the mutual adequacy findings between Japan and the EU, the Data Free-Flow with Trust (DFFT) initiative and future legal discussions about the increasing use of AI. Finally, Prof. Shimpo points out the need to both clarify and streamline any related future regulations.[20]

Diego Fernández (*Where is online privacy going?*) examines the collection of large amounts of user data by means of digital devices. He argues that this poses critical questions about online privacy and the rights of individuals, especially regarding the data generated by mobile phones which allows these devices to be located accurately. He notes that such information, normally stored by wireless carriers, can have a great impact on criminal investigations, as it can help to pinpoint the location of people under investigation. Diego further examines the US Supreme Court's ruling in *Carpenter v. United States*, a leading case on geolocation through cell phones and privacy. He discusses the fact that this ruling was mirrored and cited by an Argentine court shortly after it was issued, and it is being replicated throughout multiple jurisdictions.[21]

Bartolomé Martín (*Google v. CNIL and the right to be forgotten: a judgement of Solomon*) examines the landmark ruling of the Court of Justice of the European Union (CJEU) in the *Google v. CNIL* case. He analyses the CJEU's interpretation of the territorial limits of the European right to be forgotten. He addresses the fact that, while the CJEU does not require a search engine operator to carry out a de-referencing on all versions of its search engine globally, a Member State supervisory or judicial authority is still able to order a de-referencing on all versions, after weighing up the legally protected interests. Bartolomé compares this to the Judgement of Solomon, as the CJEU's ruling is not likely to please either the search engines or data subjects, and it creates some legal uncertainty in the system.[22]

Finally, I have had the pleasure to coordinate and edit the *Global Privacy News*, which tracks significant developments in some of the key jurisdictions in the area of privacy, data protection, and cybersecurity. The aim of this article is to provide the reader with concise reports prepared by leading practitioners and law firms on some of the most important developments across the globe. Diego Fernández (*Marval, O'Farrell & Mairal*) from Argentina, Paulina Silva and María José Díaz (*Carey*) from Chile, Mauricio Jaramillo Campuzano and Andrés Fernández de Castro (*Gómez-Pinzón Abogados*) from Colombia, Sonia Cissé and Julia Loiseau (*Linklaters*) from France, Saverio Puddu (*Linklaters*) from Italy, Isabel Ortiz Monasterio Borbolla and Pablo Perezalonso Eguía (*Ritch, Mueller, Heather y Nicolau*) from Mexico, Oscar Montezuma (*Niubox*) from Peru, Michał Pękała and Jakub Kowal (*Linklaters*) from Poland, Andreia Amaral Santos (*Linklaters*) from Portugal, Jakub Brecka (*Linklaters*) from Singapore, Claudia Oteros (*Linklaters)* from Spain, Sylvain Métille and David Raedler (*HDC Law Firm*) from Switzerland, Burak Ozdagistanli and Hatice Ekici (*Ozdagistanli Ekici Attorney Partnership*) from Turkey, and Caitlin Potratz Metcalf (*Linklaters*) from the USA contributed to this *News* section.[23]

Enjoy your reading (in private)!

Ceyhun Necati Pehlivan

Editor-in-Chief

Notes

[19] Ceyhun Necati Pehlivan & Inés Isidro, *Blockchain and Data Protection: A Compatible Couple?*, in this issue, at 39.

[20] Fumio Shimpo, *The Importance of 'Smooth' Data Usage and the Protection of Privacy in the Age of AI, IoT and Autonomous Robots*, in this issue, at 49.

[21] Diego Fernández, *Where Is Online Privacy Going?*, in this issue, at 55.

[22] Bartolomé Martín, *Google v. CNIL and the Right to Be Forgotten: A Judgement of Solomon*, in this issue, at 61.

[23] Ceyhun Necati Pehlivan (ed.), *Global Privacy News*, in this issue, at 63.