THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK
© 2018 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of September 2018, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above.
Enquiries concerning editorial content should be directed
to the Publisher – tom.barnes@lbresearch.com

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

2018 has been a watershed year for the privacy field. This overview highlights some of the year's key developments that are discussed in detail in the succeeding chapters.

Obviously, the European Union's General Data Protection Regulation (GDPR) has been the main attraction. Companies subject to the GDPR have expended and will continue to expend enormous efforts and funds to understand and diagram their data-processing operations. They have also needed to design rigorous new compliance mechanisms, and to implement elaborate systems for providing data subject rights such as access, deletion, rectification and portability.

Now that the GDPR has gone live, as of 25 May 2018, it remains to be seen how the Member State data protection authorities will deploy their significant new penalty authority to enforce substantially more stringent standards. Will US tech companies continue to bear the brunt of EU enforcement wrath, or will the DPAs scrutinise inwards as well?

The world will also be watching to see whether enforcement by the various EU DPAs conforms to acceptable standards of transparency, fairness, due process and consistency. With potential penalties of up to 4 per cent of a company's global turnover at stake, it is likely that the new European Data Protection Board (EDPB) will have its work cut out to harmonise the data protection policies of increasingly fractious national governments. Will the full range of EU DPAs have the resources, legal authority and administrative experience to enforce the GDPR both fully and fairly?

Perhaps most importantly, will it turn out that the GDPR was worth it?

Given the burdens of complying with the GDPR and the potential for inhibiting technological and commercial innovation, will Europe's citizens be better or worse off under the GDPR? The correct judgement on this crucial point will depend on whether the privacy benefits of GDPR will outweigh its costs.

One hopes that someone is really paying attention to this question. It will require the acquisition of significant amounts of relevant empirical data to answer it. While privacy and data protection are fundamental rights in the European Union – as they are in most of the world – no society has concluded that privacy rights are absolute. Accordingly, the European Union's citizens will be well served if EU officials make the effort to monitor the full spectrum of GDPR costs and benefits, and then assess those impacts against the actual privacy risks the GDPR prevents or penalises.

1 Alan Charles Raul is a partner at Sidley Austin LLP.

In the United States, privacy regulation has also taken flight – in California. The 'Golden State' has adopted the California Consumer Privacy Act (CCPA). That statute will, in January 2020, become by far the most prescriptive privacy law in the United States (not counting federal financial, health, telecom and children's privacy laws).

The CCPA focuses on requiring explanation and transparency of data collection practices and data uses by companies operating in California (or processing the data of California residents). However, the CCPA is arguably somewhat more reasonable and less restrictive than the GDPR. The CCPA turns primarily on 'opt-out' rather than the GDPR's abiding preference for 'opt-in'. Moreover, the CCPA does not require burdensome logging of data-processing practices, and does not authorise enormous potential penalties or private litigation (except with regard to data breaches involving exfiltration of personal data). To be sure, however, the CCPA does authorise data subject rights similar to those of the GDPR, namely access, deletion and portability. Time will tell whether the CCPA constrains technological innovation as much as the GDPR certainly will. A final point to consider is that the CCPA may yet be subject to further legislative amendment prior to its 1 January 2020 date, and will in addition be subject to interpretative regulations by the state's Attorney General.

California is not the only US jurisdiction moving on privacy. Besides new legislation in other states, the cities of San Francisco and Chicago have also taken steps in the direction of regulating privacy and data protection at the municipal level. While little may come of the local policy idiosyncrasies, (and the CCPA would largely pre-empt the San Francisco ordinance), all this policymaking activity has inspired the federal government to consider proposing its own privacy legislation. Federal standards could pre-empt or obviate states from going in 50 different directions (as they have done on data breach notification laws).

At the time of writing, the White House had not yet released its privacy proposals, but they are expected to be published before 2019. In the meantime, the Federal Trade Commission (FTC) has embarked on a substantial series of hearings to examine privacy, big data, artificial intelligence and numerous other consumer protection and competition issues. The FTC is likely to consider very closely what 'information injuries' are sufficiently concrete to justify regulatory restriction or enforcement penalties in the realm of alleged privacy or data protection violations. Unlike the European Union, in the United States sanctions are typically only imposed or authorised where the injury at issue is (1) concrete and particularlised (i.e., experienced by specific individuals) and (2) *de facto* and real, rather than wholly abstract. While the United States recognises that intangible injuries may be real and not merely abstract, it will not necessarily be possible to predicate enforcement or private litigation on pure dignitary harm or mild emotional distress. Illusory, trivial or technical privacy harms would not generally support regulation or penalties.

India's Supreme Court recently held that privacy is a fundamental human right, and the national government is actively considering a comprehensive privacy and data protection regime. India's proposed new privacy framework is now embodied in draft legislation,which is open for public comment until 30 September 2018. The proposed law appears to follow the EU regime closely. If it is ultimately enacted in this form, we will see whether the new India law enhances or impedes India's rise as a major hub of technological innovation and digital commerce. India is also considering possible data localisation requirements for storage of personal data in-country and use of local service providers. This could obviously have international trade repercussions.

For the United Kingdom, the key data protection will be – as it will be for many regulatory policy issues – Brexit. In April 2018, the Information Commissioner, Elizabeth

Denham, stated that the Information Commissioner's Office (ICO) is preparing for the post-Brexit environment, 'in order to ensure that the information rights of UK citizens are not adversely affected' by Brexit.

In the meantime, the UK Data Protection Act 2018 came into force on 23 May 2018. It repealed the 1998 UK Data Protection Act, and introduced certain specific derogations that specify how the GDPR applies in UK law. The Act also addressed certain national security privacy provisions, as well as the powers and obligations of the ICO. The ICO has published extensive guidance on the GDPR.

China continues to release numerous national standards regarding cybersecurity for public comment. These regulatory provisions include 'Measures on Security Assessment of the Cross-Border Transfer of Personal Information and Important Data' (which incorporate requirements regarding data localisation and security) as well as the 'Regulations on Security Protection of Critical Information Infrastructures'. Certain cybersecurity standards are already effective, however, and government agencies are becoming more active in enforcement. To be sure, many specific requirements, procedures and details are still waiting to be developed. Nonetheless, companies are proceeding to implement internal compliance programmes for cybersecurity and the protection of personal information. Under the existing Cybersecurity Law of China, companies are well advised to consider how and whether their existing business operations and practices warrant modification to ensure the requisite level of cybersecurity protection.

In Russia, the requirements for data localisation remain an important concern for international businesses. All personal data of Russian citizens must be stored and processed in the territory of Russia, and the location of such databases must be reported to the Russian data protection authority. Greater stringency of enforcement and more litigation are expected in the years ahead. The 'Yarovaya Law' also continues to pose concerns for telecom and internet companies. They are now required to store the contents of telephone calls and text messages for six months, and metadata for one year, and they must also provide significant additional assistance for government access and surveillance.

On 5 February 2018, the Asia Pacific Economic Cooperation (APEC) data protection framework saw Singapore join the United States (2012), Mexico (2013), Japan (2014), Canada (2015), and South Korea (2017) as an approved APEC economy participating in the APEC Cross-Border Privacy Rules system. APEC continues to grow slowly as countries and companies wait to see what develops.

Japan and the European Union announced on 17 July 2018 that they had agreed to grant reciprocal adequacy to their respective data protection regimes. To achieve this mutual recognition, the European Union had established certain conditions, including that Japan agree to treat trade union membership and sexual orientation as sensitive information categories; that data subject rights be accorded to information deleted within six months; and that original purpose limitations be respected; that Japan ensure that EU data transferred out of Japan to non-EU countries retain the same level of protection outside of Japan as in Japan. Also of note in Japan is a pending judicial ruling regarding a data breach case (*Benesse Corporation*). The decision here may define the obligations of businesses to protect personal information and the resulting damages from data breaches.

In addition to joining APEC, Singapore passed the Cybersecurity Act, which is primarily a criminal statute. However, it also created a new Commissioner of Cybersecurity with significant powers to prevent and respond to cybersecurity incidents. It also set up a licensing scheme for providers of certain cybersecurity services. As yet, no regulations or guidance have been provided for general business cybersecurity practices.

Canada finalised regulations to provide additional detail regarding the privacy breach notification requirement under the federal Personal Information Protection and Electronic Documents Act (PIPEDA). From 1 November 2018, private companies subject to PIPEDA will be required to notify affected individuals and report to the Privacy Commissioner where a breach of security safeguards would result in a real risk of significant harm to individuals. In 2018, the Federal Court of Canada also affirmed that PIPEDA applies to commercial entities outside Canada if they process personal information about Canadians. Privacy-related litigation in Canada is also expected to grow in the near term.

In Mexico, a significant cyberattack on financial institutions in 2018 is being investigated by the Attorney General. The national data protection authority (INAI) is also investigating to determine whether this incident constitutes a data breach. In addition, INAI has provided non-binding guidance on the status of biometric data as sensitive when (1) it refers to the most intimate sphere of the data subject, (2) can lead to discrimination, and (3) illegitimate use could result in material risk to the data subject. INAI also provided non-binding guidance for protecting personal data on social media.

In July 2018, Brazil adopted a comprehensive data protection law, known as the LGPD. This omnibus privacy regime is modelled closely on the GDPR. The LGPD also established a National Data Protection Authority. Significantly, an important case is pending before the Supreme Court regarding the legality of encryption technology. The issue concerns the role of encryption technology in preventing disclosure of communications content to law enforcement.

And, of course, much privacy and cybersecurity policymaking activity is taking place around the rest of the world as well.

* * *

The outline above highlights the in-depth treatment of the different jurisdictions discussed in detail below. As noted at the outset, 2018 may prove to be a turning point in global privacy and data protection policymaking. 'Cambridge Analytica' – shorthand for the active measures of Russia, and perhaps other geopolitical actors, to manipulate social media to interfere with the political processes of Western democracies – will likely become rallying cry for advocates on a par with the 'Snowden' impact on the privacy community in 2013.

In order to ensure that policymakers do not learn the wrong lessons from these dramatic events, it will be important for governments to focus precisely on combating real rather than imagined (or negligible) privacy risks. Such calculations are essential to achieve smart regulation rather than foolish over-regulation.

While privacy is, naturally, a fundamental right in democratic countries, governments must nonetheless justify their privacy regulations to their citizens. Without such rigorous justification, which entails a careful balancing of fundamental rights and other important social objectives, data protection policy could end up not actually being beneficial to society. Bad policy will delay or even deny technological development and deployment, thereby stunting social advancement and restricting consumer choice and economic options. 'Artificial intelligence' applications are likely to become the next proving ground for how smart regulators are. In all, however, the nurturing and preservation of human dignity and liberty will remain essential – of course.

Appendix 1

ABOUT THE AUTHORS

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP's highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Data Security, Privacy & Intellectual Property Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves as a member of the American Bar Association's Cybersecurity Legal Task Force by appointment of the ABA president. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

SIDLEY AUSTIN LLP

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com

www.sidley.com

ISBN 978-1-912228-62-1