The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 1 GLOBAL OVERVIEW 1
Alan Charles Raul

Chapter 2 EUROPEAN UNION OVERVIEW 6
William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul

Chapter 3 APEC OVERVIEW 25
Catherine Valerio Barrad, Ellyce R Cooper and Alan Charles Raul

Chapter 4 AUSTRALIA 38
Michael Morris

Chapter 5 BELGIUM 51
Steven De Schrijver and Thomas Daenens

Chapter 6 BRAZIL 64
Daniel Pitanga Bastos de Souza and Bruno Granzotto Giusto

Chapter 7 CANADA 73
Shaun Brown

Chapter 8 CHINA 89
Marissa (Xiao) Dong

Chapter 9 FRANCE 100
Dominique de Combles de Nayves & Pierre Guillot

Chapter 10 GERMANY 113
Jens-Marwin Koch

Chapter 11 HONG KONG 127
Yuet Ming Tham

Chapter 12 HUNGARY 142
Tamás Gödölle

Chapter 13 INDIA 159
Aditi Subramaniam

Chapter 14 IRELAND 170
Andreas Carney and Anne-Marie Bohan

Chapter 15 ITALY 184
Daniele Vecchi and Melissa Marchese

Chapter 16 JAPAN 199
Tomoki Ishiara

Chapter 17 KOREA 215
Kwang Bae Park and Ju Bong Jang

Chapter 18 MALAYSIA 229
Shanthi Kandiah

Chapter 19 MEXICO 242
César G Cruz-Ayala and Diego Acosta-Chin

Chapter 20 POLAND 256
Tomasz Koryzma, Marcin Lewoszewski, Agnieszka Besiekierska and Adriana Zdanowicz–Leśniak

Chapter 21 PORTUGAL 271
Magda Cocco, Inês Antas de Barros and Sofia de Vasconcelos Casimiro

Chapter 22 RUSSIA 282
Elena Kukushkina, Georgy Mzhavanadze and Vadim Perevalov

Chapter 23 SINGAPORE 294
Yuet Ming Tham

Chapter 24 SPAIN 310
Leticia López-Lapuente and Reyes Bermejo Bosch

Chapter 25 SWITZERLAND 322
Jürg Schneider and Monique Sturny

Chapter 26 TURKEY 341
Gönenç Gürkaynak and İlay Yılmaz

Chapter 27 UNITED KINGDOM 352
William RM Long, Géraldine Scali and Francesca Blythe

Chapter 28 UNITED STATES 370
Alan Charles Raul, Tasha D Manoranjan and Vivek K Mohan

Appendix 1 ABOUT THE AUTHORS 403

Appendix 2 CONTRIBUTING LAW FIRMS' CONTACT DETAILS 419

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

Transatlantic data protection tensions continue to characterise the privacy world in 2016. However, there have been more than enough actual substantive developments in the US, EU and the rest of the world to provide much to talk about beyond the EU's persistent concerns regarding the US government and private sector. Information law and digital policy privacy is currently so dynamic that it is difficult to predict future trends and key focal points for next year's global regulators and enforcers. The discussion below provides a whirlwind *tour de horizon* of leading issues during 2016. As one can see, the disparate policy developments around the world could benefit from international coordination at the ministerial level, as well as efforts to ameliorate tensions and promote greater understanding.

In the US, policy developments have focused in the past 12 months on both cybersecurity and privacy issues. Congress adopted the Cybersecurity Information Sharing Act (CISA) in December 2015. CISA facilitated two-way information sharing by insulating companies that provide cyber threat data to the government from potential liability and imposed certain personal information scrubbing obligations on the information exchange process. Significantly, CISA provided companies with enhanced 'notwithstanding any other provision of law' authority to engage in monitoring and operate defensive measures on their own networks to protect against cyber-risks and vulnerabilities. President Obama also issued Presidential Policy Directive 41, an order directing executive branch agencies to coordinate more effectively in responding to cybersecurity incidents, and to provide more concerted investigative and protective assistance to private-sector victims of cyberattacks.

On the privacy front, the Federal Trade Commission (FTC) issued an important report on Big Data that provides guidance and recommendations to companies using voluminous data and complex algorithms to make decisions about individuals. The FTC warned against basing credit and other financial decisions on data of untested, uncertain and unreliable quality, or on algorithms that could conceal hidden biases. In a nutshell, the FTC

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

admonished companies to monitor and second-guess the outcomes of their data analytic initiatives, and threatened to take action against practices that end up being discriminatory (even if companies do not actively intend to discriminate).

The most striking regulatory development, however, came from the Federal Communications Commission (FCC), which proposed broad new privacy rules on internet service providers (which were previously regulated by the FTC). The FCC initially proposed privacy rules that would have dramatically limited ISP online tracking and advertising practices relative to other internet companies (such as social media, search engines, ad networks, etc.). Remarkably, though, the FCC moderated its proposal in response to criticism – not only from ISPs – but also from the FTC. The latter agency, as well as ISPs, faulted the FCC for seeking to impose stringent privacy limits without drawing any meaningful distinctions based on the actual sensitivity of the personal data involved or on the likelihood the practices in question could lead to consumer harm. While the final rules were approved by a partisan vote of 3–2 on 27 October 2016, the text of the actual regulation had not been issued at the time of writing. It appears that the regulation may have moderated somewhat toward the FTC position.

Surprisingly, in a long-awaited decision, an appellate court in New York ruled in favour of Microsoft – which was supported by other technology and telecommunications companies, and foreign governments – in a case involving a search warrant for customer data the company stored on servers in Ireland. The court held that the search warrant issued under the Stored Communications Act could not be used to compel a company to produce the customer data in question – stored emails – to law enforcement authorities in the US. This decision should help alleviate some of the transatlantic tensions referenced above, and may also motivate the US Congress to adopt a law that strikes a measured balance between the need for legitimate government access, respect for foreign sovereignty and data protection concerns (i.e., international comity) and the long-standing principle of the presumption against extraterritorial application of US laws. While Congress may take up legislation to strike a reasonable balance, the *Microsoft* case may yet find its way to the US Supreme Court.

It is also telling that 2016 is ending without any legislative requirement that technology or telecom companies be required to decrypt their customers' communications for government investigations of terrorism cases or serious crimes in the United States. In fact, the upshot of the FBI's effort to compel Apple to write code to grant the government decrypted access to iPhones, including the device owned by the gunman in the 2015 San Bernardino terror attack, was a court order narrowing the government's ability to buttress search warrants by invoking open-ended judicial powers under the All Writs Act (which provides courts with broad authority, and dates back to the original Judiciary Act of 1789).

At the Supreme Court, in a civil case known by the name of the defendant, Spokeo, an online 'people search engine', the Justices held that individuals were not entitled to sue for technical statutory violations unless they suffered some real or *de facto* harm or injury. The Court acknowledged that intangible injury could be real, and actionable, but conceded that it was often more difficult to recognise ethereal harms.

In the EU, policymakers were not utterly bogged down by the October 2015 *Schrems* decision that invalidated the US-EU Safe Harbour for transatlantic transfers of personal data. The EU institutions were able to finalise adoption of the General Data Protection Regulation (GDPR) that will come into effect throughout the EU in May 2018. The GDPR will not

only establish a more aggressive enforcement regime and ratchet up potential penalties for privacy violations to as high as 4 per cent of global annual revenue, or €20 million, whichever is higher – it also establishes a raft of considerably stricter privacy requirements.

The GDPR will require rapid data breach notification, tighter thresholds for obtaining consent from data subjects, consumer data portability, new restrictions on profiling and other automated processing, and new requirements for data protection officers, privacy impact assessments, and the right to be forgotten or the right of erasure. The GDPR will apply to a broader range of non-EU businesses that target or envision having European customers, and will also empower more private litigation to be conducted on a collective, or class action, basis.

The EU also spoke forcefully on cybersecurity, adopting a Network Information Security Directive that will require member states to develop national programmes to secure critical infrastructure, including the financial sector and other standard CI industries, as well as online organisations such as search engines and e-commerce platforms.

But the EU also did have to deal with *Schrems* and *Schrems* again. The invalidation of the Safe Harbour lead to intense and elaborate negotiations with the US resulting in the Privacy Shield, which was ultimately revised to take account of a range of intra-EU policy concerns. Ultimately, the Privacy Shield was opened for certification in the summer of 2016. Approximately 500 companies have elected to sign up for compliance with its principles. Those who do join will be subject to greater scrutiny and enforcement from the FTC in the US, and data protection authorities in the EU. In addition, the US State and Commerce Departments will play a role in the redress process for EU citizens who feel injured as a result of their data having been transferred to the US. Companies joining the Privacy Shield must also provide substantial access to the EU citizens about whom they hold data, arrange for alternative dispute resolution and possible arbitration, and enter into onward transfer and data processing agreements with their vendors and service providers.

In a new case filed by Mr Schrems against Facebook in Ireland, first the Irish High Court and then the Court of Justice of the European Union will be called up to judge whether the EU's standard contractual clauses should also be invalidated on the same grounds as was the Safe Harbour previously. The new litigation is likely to involve greater consideration of actual facts, and a more robust defence of the US legal position, given that the US government has received approval to participate in the Irish proceedings. Moreover, the new litigation may be obliged to consider the actual 'essential equivalence' of US privacy safeguards to those in force in the EU. To that end, Sidley Austin LLP prepared and provided to EU authorities a nearly two hundred page report entitled, 'Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States.'

On Big Data, the EU appears poised to allow data analytics that use information in a manner 'compatible with' the original disclosures and consents, even if not precisely contemplated at the time of collection. To be sure, however, the EU has also indicated that it intends to scrutinise data-intensive companies and transactions from a competitive perspective. The European Data Protection Supervisor (EDPS), Giovanni Buttarelli, continues to provide sophisticated thought leadership. He acknowledges there must be a balance between companies' legitimate interests in monetising their information, and individuals' rights to fair treatment. He notes that the ethical dimension of Big Data is unavoidable.

In a September 2016 opinion, the EDPS 'recognise[d] the potential of data-driven technologies and services as a catalyst for economic growth,' but also expressed concerns over covert tracking, potential unfairness and exploitation. In addition, he recommends development of personal information management systems (PIMS) to help individuals

manage and control their online identity. PIMS could help give individuals more control of their personal data, and advance ethical use of big data and the principles recently adopted in the GDPR.

On 15 April 2015, Canada joined the United States (2012), Mexico (2013) and Japan (2014) as an approved Asia-Pacific Economic Cooperation (APEC) economy participating in the APEC Cross-Border Privacy Rules (CBPR) system. This system is growing slowly, as some economies are waiting to see interest from business, and some businesses are waiting for member economies to join. The FTC has started to bring enforcement actions with respect to APEC-related claims. On 29 June 2016, the FTC issued its first enforcement decision under the CBPR against Very Incognito Technologies Inc for misrepresenting its compliance and on July 2016, the FTC announced that it had sent warning letters to 28 companies that claimed compliance with the CBPR.

In the UK, the Court of Appeal of England and Wales considered whether Google had violated the rights of users whose Safari cookie settings had allegedly been overridden and browser information collected. The Court recognised an arguably new privacy tort based on misuse of information. Moreover, this privacy tort could be enforced by individuals who suffered no financial loss, but only anxiety, distress and 'intrusion upon autonomy'. Interestingly, the Court of the Appeals in the US that considered the same core facts dismissed all federal claims but allowed California state privacy claims to survive.

It is notable that the English case was allowed to proceed as a class action. Also significant is that the English court considered it immaterial whether Google had actually used its aggregated data to personally identify the plaintiffs. Rather, 'What matters is whether the defendant has other information actually within its possession which it could use to identify the subject of the [browser information], regardless of whether it does so or not.' Ultimately cases on both sides of the Atlantic were resolved by settlement among the parties. Google had also already paid fines to the FTC and US state attorneys general.

Significantly, Germany has also authorised privacy class actions. In February 2016, it adopted a Law to Improve the Civil Enforcement of Consumer Protection Rules of Data Protection Law. This allows consumer associations to challenge violations of the German Data Protection Act and EU regulations including the General Data Protection Regulation.

Korea issued Guidelines on Personal Information De-identification Measures and a Comprehensive Guide to Data Protection and Privacy Laws and Regulations. These guidelines are non-binding, but may help clarify procedures for Big Data purposes. Hong Kong issued guidelines on workplace monitoring. Both Singapore and Japan have promulgated certain significant new guidelines and interpretations. And Turkey has adopted a new privacy law that is modelled on the EU legislation.

In September 2015 Russia required personal data of Russian citizens to be maintained on servers located in Russia. Online communication service providers are now required, under new counter-terrorism laws, to retain data on internet communications of Russian users, and to store this information in Russia for six months and disclose it to Russian authorities on request. As of July 2016, online communication service providers will also be required to provide the government with decrypted communications of their users. Moreover, starting in July 2018, online communication service and telecom providers may be required to retain and store the contents of internet communications for up to six months.

China released the second draft of its Cybersecurity Law for comment in July 2016. This draft specifies requirements for network operators regarding social and commercial

moral standards, cybersecurity obligations, government supervision, social responsibility and retention of network logs for at least six months. Providers of instant message services will also be required to verify users' identities.

In addition, China has introduced interim measures regarding the administration of internet advertising and mobile network information service applications. These standards include protection for personal information. A draft of the Implementing Regulation of the Consumer Rights Protection Law may include data protection obligations and data breach notification requirements.

In India, there is pending litigation regarding the status of privacy as a fundamental right. The question arises in connection with the privacy policies of a technology company's privacy policies. India and the US also advanced mutual cybersecurity cooperation by signing a framework for the 'US-India Cyber Relationship,' addressing internet governance, cybersecurity and state norms.

* * *

Given the extent of policy development around the world, and the fact that many objectives for protecting the privacy and security of personal data are shared by most democratic countries, the world could benefit from greater international discussion and coordination at the ministerial level. Currently, privacy regulators and data protection authorities have relatively narrow mandates, and do not necessarily hold the institutional competence to address broad questions of social welfare, economic growth and technological innovation. They also do not hold responsibility for national security or law enforcement matters.

Perhaps the new administration in the United States could undertake a global initiative to promote greater international understanding of the commonalities inherent in the world's different privacy and data protection regimes. This could lead to enhanced interoperability and wider distribution of the consumer and business benefits accruing from the digital age. US leadership on privacy is by no means an oxymoron. Indeed, a US-initiated dialogue could inform citizens of the world that privacy protections and safeguards in America are at least 'essentially equivalent' to those of the EU and other countries. This is especially true with regard to the constraints on, and checks and balances applicable to, governmental access to personal data. US leadership could help abate international concerns and, ultimately, lead to the expansion of digital trade benefiting the world's internet users and information gatherers.

As more and more devices are connected to the internet, and as sensors, data analytics and complex algorithms about human behaviour become even more ubiquitous than they are today, a global digital dialogue could be increasingly imperative, or at least valuable.

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, data security and information law 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 has also served on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President, and currently remains an *ex officio* member. 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