The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 2
(published in November 2015 – editor Alan Charles Raul)

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor

Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, Felicity Bown, Joel Woods

ACCOUNT MANAGER
Jessica Parsons

PUBLISHING MANAGER
Lucy Brewer

MARKETING ASSISTANT
Rebecca Mogridge

EDITORIAL ASSISTANT
Sophie Arkell

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Gina Mete

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-75-2

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ADVOKATFIRMAET SIMONSEN VOGT WIIG AS

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K.

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JUN HE LAW OFFICES

LEE & KO

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

PEARL COHEN ZEDEK LATZER BARATZ

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

Cybersecurity turned out not to be, after all, the privacy issue of the year. Rather, the decision of the Court of Justice of the European Union (CJEU) to invalidate the US-EU Safe Harbor Framework was the blockbuster development of 2015. On 6 October, the CJEU struck down Safe Harbor as an approved mechanism for the transfer of personal data from the EU to the United States. The Court found that the European Commission had not properly assessed the 'adequacy' of the US legal regime for data protection, neither in 2000 when the Safe Harbor Framework was first agreed, nor subsequently. The basis for the Court's concerns stemmed from allegations that the United States engaged in 'indiscriminate' surveillance for national security reasons, and that such surveillance could mean that data protection for information transferred there might not be 'essentially equivalent' to protection in the EU.

'Equivalence', then, is the challenge of global privacy law today. Data localisation mandates imposed in Russia, in particular, but also surfacing as a possibility in other jurisdictions, like Brazil, are threatening international data flows and impeding digital trade. Indeed, the EU's stringent restrictions against data transfers to the United States are themselves a significant manifestation of data localisation. With luck and goodwill, a new US-EU Safe Harbor 2.0 will be negotiated and put in place quickly, and other mechanisms to authorise international data transfers – such as EU Model Contract Clauses and binding corporate rules – will remain available. Moreover, perhaps the EU will even acknowledge that US checks and balances on government surveillance, and the privacy protections enforced by the Federal Trade Commission (FTC), the Federal Communications Commission, 50 plus state attorneys general and numerous other federal and state agencies are least substantially equivalent to those of the EU – especially with regard to government surveillance!

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

The other big privacy story of 2015 is the 'nearly baked' status of the proposed General Data Protection Regulation in the EU. The replacement of the existing framework Directive, dating back to 1995, with a new Regulation will mean that privacy law in the EU will be uniform in text (rather than implemented in various formats in each Member State's national law, as is the case today). The new Regulation, which is likely to be approved around the beginning of 2016, will also be subject to more consistent, coordinated interpretation and enforcement, and may impose both stricter standards and higher penalties for violations (and is likely to include enforcement via 'collective redress', a possible EU version of US class actions). In addition, the Regulation will finally bring the EU into line with US-style data breach reporting. Adapting international privacy compliance programmes to the new Regulation will surely need to be an important priority for global organisations beginning in 2016 (to be prepared for the Regulation's eventual effective date).

In the United States, a court of appeals decided in the *Wyndham* case that the FTC was authorised to enforce reasonable data security standards under its broad power to prohibit 'unfair or deceptive' business practices. This decision was a major development because it confirmed the FTC's authority over cybersecurity and personal information data breaches under the agency's general consumer protection power. Additionally, the FTC was permitted to litigate against a company that was itself the victim of a criminal hack, even though the FTC has not published any applicable standards defining what constitutes 'reasonable' or otherwise legally required cybersecurity standards.

Cybersecurity information-sharing legislation may finally be enacted after having been stalled for almost two years in the US Congress, and numerous government entities have announced new guidance and expectations regarding data security, including the Department of Justice, the Securities and Exchange Commission, state regulators and a variety of other agencies, and there have also been a number of significant court decisions involving major retailers and other parties involved in breaches. A number of states have further tightened their data security and data breach reporting requirements. All of these developments have led many US companies to initiate internal reviews of their cybersecurity governance and readiness programmes.

Significant privacy and data security developments are also taking place around the rest of the world. In particular, new data breach reporting obligations are taking root in many countries. New or significantly revised privacy laws have been adopted in a number of countries. In Japan, for example, revisions to its privacy law will apply to international data transfers and to big-data applications, online direct marketing and other matters. In Brazil, the fallout from the Snowden leaks continues, and the government is still implementing the 2014 Internet Act, which enhances privacy rights over personal and behavioural data. However, the mandatory data localisation provisions to store Brazilian-sourced data only on servers physically located in the country have been dropped. In Russia, much debate has gone back and forth regarding the new legal obligations to store the data of Russians on local servers, but the ultimate resolution appears to permit the same information also to be stored outside the country.

Like numerous other countries, the Republic of Korea has amended its privacy law to increase potential penalties and continue aggressive enforcement of data breach and other violations. In Hong Kong, new privacy guidance has been provided for international

data transfers, surveillance tools like CCTV, and for collection and use of biometric data. Singapore has also amended its privacy law significantly, and included new provisions and guidance regarding marketing, data breaches and securing electronic data.

Some countries, like Turkey, have been considering adoption of new privacy laws based on the EU's 1995 Data Protection Directive. In the meantime, Turkey has adopted laws on processing personal data and privacy protection in the telecom sector, and established new requirements for e-commerce. Israel has seen the development of new guidelines regarding the use of cloud services in the financial sector.

China, too, has been debating whether to follow the US or EU model. No final approach has been decided, but the practice to date represents a mix of both. For example, personal privacy is expressly protected in a 2010 'Tort Liability Law,' as it would be under the US model. Government rules, judicial consideration, corporate practices and public expectations about privacy and data protection are changing fast. Administrative guidance has recently been issued on cloud computing and big data, and new policies are expected on e-commerce and internet law. Most significant, for the rest of the world, are draft provisions that could require mandatory data localisation for telecom operators and internet service providers, obligating them to retain users' data in China, as well as possibly requiring certain companies to provide technical interfaces to enable government access. Other draft provisions would also require companies to share software source code and file encryption plans with the government. International concern has been conveyed to Chinese authorities, and it is not clear what impact this will have on future Chinese deliberations and drafts regarding these laws and potentially troubling provisions. The meeting in September 2015 between Presidents Xi Jinping and Barack Obama concluded with an agreement to collaborate on cybersecurity and efforts to crack down on cybercrime. They also jointly embraced a July 2015 United Nations accord to desist from targeting each other's critical infrastructure during peacetime. President Obama, however, spoke much more forcefully and specifically about stopping cyber-espionage used for commercial gain. The practical impacts of the September agreement between the two leaders remain to be seen, of course.

India also does not have comprehensive legislation directed towards data protection or cybersecurity. However, rules regarding 'reasonable security practices and procedures and sensitive personal data or information' have been issued under the Information Technology Act. These rules are intended to guide corporate practices. The rules call for companies to maintain privacy policies and transfer personal data outside India only to countries where there is an assurance of a level of protection equivalent to that provided by the company itself. Given the absence of a specific legislative mandate, however, there has been no significant litigation addressing corporate practices under these rules. Nonetheless, courts have been considering a constitutional right to privacy derived from the country's express guarantees for free expression and movement, and there is a common law right to privacy under India's tort regime.

In sum, the world is converging on more privacy laws that cover more areas of business and are subject to more enforcement. However, there are few efforts to harmonise the laws to promote interoperability and enhance digital trade and unfettered international data flows. The United States significantly leads the world in data protection enforcement, but many countries considering adopting new laws look to the EU model of omnibus and detailed regulation.

Fairly or otherwise, the ongoing impacts of the Snowden leaks still drive a wedge between the United States and the EU on privacy issues. 'Even' in the United States, however, it has been just about one year since the Chief Justice of the Supreme Court upheld the privacy of smartphone data that could have been useful to law enforcement because 'privacy comes at a cost'. For the private sector, prospective privacy constraints on big-data applications and other new technologies will also need to be looked at carefully so that the impacts on innovation, personalisation and consumer convenience are not unduly limited.

Given the increasing challenges of providing notice and obtaining consent with respect to data collection and use for ubiquitous connected technologies, new models for ethical data stewardship are likely to emerge soon. Indeed, in his Opinion of April 2015, 'Towards a New Digital Ethics', European Data Protection Supervisor (EDPS) Giovanni Buttarelli has proposed that an ethical framework needs to be at the foundation of the current digital ecosystem comprising big data, the internet of things, ambient computing, cloud and autonomous computing, artificial intelligence and many other new technologies. The EDPS considers that better respect for and safeguarding of human dignity would be at the heart of a new digital ethics.

By next year, privacy and cybersecurity developments will surely reveal whether the data protection paradigm has shifted to any significant degree, and whether businesses and the public continue to be able to develop and embrace technological innovation in socially useful ways that respect dignity as well as progress.

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 chairman 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 Privacy, Intellectual Property, Technology and Antitrust Litigation Advisory Committee of the National 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. He is 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