THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SEVENTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
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 MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Gavin Jordan

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Claire Ancell

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-485-9

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

© 2020 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

CTSU – SOCIEDADE DE ADVOGADOS

GREENBERG TRAURIG LLP

K&K ADVOCATES

nNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

Privacy, like everything else in 2020, was dominated by the covid-19 pandemic. Employers and governments have been required to consider privacy in adjusting workplace practices to account for who has fever and other symptoms, who has travelled where, who has come into contact with whom and what community members have tested positive or been exposed.

As a result of all this need for tracking and tracing, governments and citizens alike have recognised the inevitable trade-offs between exclusive focus on privacy versus exclusive focus on public health and safety.

Even the European Data Protection Board (EDBP) conceded that data protection measures like GDPR 'do not hinder measures taken in the fight against the coronavirus pandemic. The fight against communicable diseases is a valuable goal shared by all nations and … [i]t is in the interest of humanity to curb the spread of diseases and to use modern techniques.' Accordingly, the EDPB agreed that an '[e]mergency is a legal condition which may legitimise restrictions of [privacy and data protection] freedoms provided these restrictions are proportionate and limited to the emergency period.'

And while privacy is not considered an absolute right in any jurisdiction, it is important to acknowledge that no democratic country has taken the position, or acted in a manner, suggesting that individual privacy is irrelevant or dispensable – even during the pandemic emergency. To the contrary, privacy rights have been taken into account in fighting the virus nearly everywhere.

But covid-19 was not the only shock to the privacy system in 2020. On 16 July, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield framework agreed between the EU Commission and the US Commerce Department to facilitate data flows to the United States. While the CJEU upheld the validity of using 'standard contractual clauses' to transfer personal data to countries not yet deemed 'adequate' by the EU (such as the United States), the CJEU imposed considerable new obligations on organisations looking to transfer data and for data protection authorities to consider when approving such transfers.

Specifically, the Court agreed with Austrian privacy advocate Max Schrems that there is a theoretical possibility that users of social media networks could have their communications secretly transferred to the US National Security Agency (NSA) without the benefit of privacy protections available in Europe.

Never mind that there is no proof or reason to believe that the NSA is interested in collecting communications to or from average European social media users – in other words, from anybody other than a terrorist, spy or hostile actor. And never mind that the privacy protections and legal redress opportunities under US surveillance laws are considerably

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

stronger than those EU Member States accord their own citizens. In fact, Presidential Policy Directive 28 requires the NSA and other US agencies involved in signals intelligence to protect the privacy of persons outside the United States in a manner reasonably comparable to the protections US citizens receive. And, notably, the independent Privacy and Civil Liberties Oversight Board (PCLOB) provided a thorough assessment of the implementation of PPD-28 on 16 October 2018.

Remarkably, the CJEU deemed US surveillance safeguards and remedies to be less than 'essentially equivalent' to those of the EU without comparing EU Member State surveillance laws or practices to those of the US at all! While the Court's assessment of US surveillance safeguards was superficial and woefully incomplete, its treatment of EU surveillance was entirely absent. CJEU did not so much as ask whether any EU Member State has an oversight body to examine and judge the privacy or civil rights implications of electronic surveillance the way PCLOB and Foreign Intelligence Surveillance Court do – with full national security clearance to access the deepest secrets of signals intelligence.

Though the CJEU's decision may seem frivolous (to say nothing of dangerous) to many observers, its potential impact on trillions of dollars of transatlantic trade is anything but. The EU Commission and US Commerce Department are publicly committed to solving this judicial conundrum. In the meantime, companies are going through a metaphysical process of trying to demonstrate (to themselves, data protection authorities, and ultimately maybe Max Schrems) that, under the *Schrems* decision, they can transfer personal data to the United States – and other non 'adequate' countries – without such data being disproportionately accessible to national security surveillance by the data importing country. In other words, there are no real standards at all.

In contrast, the United States provided a model for international comity and respect for the rule of law in the 2018 CLOUD Act. The Act authorises US communications service providers to produce the contents of electronic communications they store outside the United States in response to US legal requests, and to do the same for foreign governments that have entered into executive agreements with the United States (which only the UK has done so far, effective July 2020).

Importantly, the CLOUD Act requires foreign governments wishing to enter into such agreements to demonstrate their respect for the rule of law and for international human rights, privacy, free speech rights, data minimisation (equivalent to what the United States applies under the Foreign Intelligence Surveillance Act), the principles of non-discrimination, accountability, transparency, independent oversight, and numerous other detailed safeguards. Moreover, where the requested data concerns a non-US person who is outside the United States, the relevant communications service provider is authorised to file a motion in federal court to quash the government request. The provider may do so if it believes the laws of the US and of the foreign government conflict – including privacy laws – with respect to the government's demand for the communications of its customers. Once the motion has been filed, the court must conduct a detailed 'comity' analysis to resolve the conflict of international laws concerning data privacy rights.

The legal standards for such comity analysis are set forth with considerable specificity in the CLOUD Act. Courts must consider the nature of the legal conflict at stake, the materiality of the alleged violation of the foreign law, the respective interests of the two countries in the matter at hand, the contacts of the service provider and the individual in question with the United States, and the importance of the individual's information to the criminal or national security interest at issue.

The thoughtful nature of this comity analysis required by the CLOUD Act is not reciprocated in the CJEU's *Schrems* decision or the EU's General Data Protection Regulation.

Europe, and the rest of the world, would be well served to study the US model of safeguards, checks and balance, independent oversight and international comity for government access to electronic communications.

In any event, privacy developments in the United States have not been all about government access to information. In this past year and a half, US regulators and litigators have obtained the largest fines and legal awards ever collected for alleged violations of privacy and data security requirements.

The Federal Trade Commission has obtained a US$5 billion settlement and imposed unprecedented corporate governance requirements following an investigation of the Cambridge Analytica affair. And private plaintiffs have obtained a settlement of over half a billion dollars in connection with alleged violation of state biometric information privacy law. The FTC and state attorneys general (and in some cases, private plaintiffs) have collected hundreds of millions of dollars in financial recoveries concerning data breaches as well as alleged violations of the Children's Online Privacy Protection Act. Significantly, many of these proceedings are predicated on the theory that the data 'controller' is legally responsible for the allegedly invasive or abusive practices of third parties that operate on or through the 'controller's' platform. This trend towards extended responsibility is well worth watching.

Even the US Securities and Exchange Commission (SEC) is increasingly focused on digital practices and risks. The SEC is now actively enforcing the accuracy and reliability of privacy and cybersecurity disclosures by public companies. Companies could face regulatory action if they materially understate their digital risks – or avoid discussing significant incidents they have already experienced – or if they publicly overstate their data security or privacy practices. As a result, many companies – especially tech companies – are considerably expanding their discussion of how US and international privacy laws like GDPR or the newly effective Brazilian privacy law (LGPD) are affecting or could affect their global regulatory risk profile, or the economic viability of their current and future business models.

But perhaps the most important US privacy development is the new California Consumer Privacy Act (CCPA). It took effect in 2020, and as of 1 July, may be enforced by the State's Attorney General.

Not only does the CCPA require privacy disclosures, grant privacy rights, and impose privacy restrictions comparable to GDPR. But, in typical American fashion, the CCPA dangles the prospect of statutory damages (regardless of actual injury) to incentivise lawyers to file litigation over data breaches affecting the personal information of California residents – but only if the breach results from a company's failure to implement and maintain 'reasonable security'.

Even the CCPA, however, may not be enough for California. Its progenitor, real estate executive Alastair Mactaggart, has already advanced a new privacy initiative that will replace and go beyond the CCPA – the California Privacy Rights Act. CPRA will be placed before the state's voters as part of the November 2020 election (bypassing the state's legislature entirely).

In the end, as groundbreaking for the United States as the CCPA has been, its most consequential impact may be to impel other states to act, and perhaps then the US Congress will finally enact a comprehensive national privacy law.

The most reasonable outcome for America would be the establishment of stable, federal privacy and security standards that identify and target actual injuries caused by abusive

data practices. If covid-19 has taught us anything about privacy, it is that there can be real trade-offs (for health, safety, innovation, the economy and security), on the one hand, as well as real harm (for pocketbooks, and personal dignity and autonomy), on the other, from regulating either too much or too little.

Appendix 1

ABOUT THE AUTHORS

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and leader 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. He also advises companies on their digital governance strategies and cyber crisis management. 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 Technology 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

an LBR business

ISBN 978-1-83862-485-9