THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

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 978-1-83862-810-9

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

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, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 1 GLOBAL OVERVIEW 1
Alan Charles Raul

Chapter 2 EU OVERVIEW 6
William R M Long, Francesca Blythe, Denise Kara and Alan Charles Raul

Chapter 3 APEC OVERVIEW 43
Ellyce R Cooper, Alan Charles Raul and Sheri Porath Rockwell

Chapter 4 ARGENTINA 59
Adrián Furman and Francisco Zappa

Chapter 5 AUSTRALIA 70
Gavin Smith and Emily Cravigan

Chapter 6 BELGIUM 85
Steven De Schrijver and Olivier Van Fraeyenhoven

Chapter 7 BRAZIL 101
Ricardo Barretto Ferreira, Lorena Pretti Serraglio, Camilla Lopes Chicaroni and Nariman Ferdinian Gonzales

Chapter 8 CHINA 117
Hongquan (Samuel) Yang

Chapter 9 DENMARK 143
Tommy Angermair, Camilla Sand Fink and Caroline Sylvester

Chapter 10 ESTONIA 161
Risto Hübner

Chapter 11 GERMANY 173
Olga Stepanova and Patricia Jechel

Chapter 12 HONG KONG 182
Yuet Ming Tham

Chapter 13 HUNGARY 200
Tamás Gödölle and Márk Pécsvárady

Chapter 14 INDIA 213
Aditi Subramaniam and Sanuj Das

Chapter 15 INDONESIA 227
Danny Kobrata and Rahma Atika

Chapter 16 JAPAN 241
Tomoki Ishiara

Chapter 17 MALAYSIA 264
Shanthi Kandiah

Chapter 18 MEXICO 281
César G Cruz Ayala and Marcela Flores González

Chapter 19 NETHERLANDS 297
Herald Jongen, Nienke Bernard and Emre Yildirim

Chapter 20 PORTUGAL 310
Jacinto Moniz de Bettencourt and Beatriz Assunção Ribeiro

Chapter 21 RUSSIA 322
Vyacheslav Khayryuzov

Chapter 22 SINGAPORE 332
Yuet Ming Tham

Chapter 23 SPAIN 351
Leticia López-Lapuente and Reyes Bermejo Bosch

Chapter 24 SWITZERLAND 366
Jürg Schneider, Monique Sturny and Hugh Reeves

Chapter 25 TAIWAN 389
Jaclyn Tsai, Elizabeth Pai and Jaime Cheng

Chapter 26 TURKEY 402
Susen Aklan, Kaan Can Akdere and Melis Mert

Chapter 27 UNITED KINGDOM 419
William R M Long, Francesca Blythe and Denise Kara

Chapter 28 UNITED STATES 449
Alan Charles Raul and Snezhana Stadnik Tapia

Appendix 1 ABOUT THE AUTHORS 487
Appendix 2 CONTRIBUTORS' CONTACT DETAILS 505

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

Privacy law has propagated impressively around the globe since the United States enacted the world's seminal statutes, namely the Fair Credit Reporting Act in 1970 and federal Privacy Act of 1974. While growth of the field has been steady, it has also been amazingly dynamic.

The top leaders of the free world signalled the essentiality of 'privacy' in the communiqué they issued at the conclusion of the Carbis Bay meeting of the G7 in the United Kingdom on 13 June 2021. Specifically, they committed to 'championing data free flow with trust, to better leverage the potential of valuable data-driven technologies while continuing to address challenges related to data protection'.

The Presidents and Prime Ministers of the world's most prosperous democracies, alongside the Presidents of the European Commission and Council, emphasised their strongly held, shared values on privacy and data protection. They expressed a mutual desire to enhance coordination, promote innovative technology, develop global norms and standards, and harmonise principles of data collection. These leaders said:

> *[w]e will work together . . . as part of an ongoing agenda towards a trusted, values-driven digital ecosystem for the common good that enhances prosperity in a way that is sustainable, inclusive, transparent and human-centric. In doing so we will make it a sustained strategic priority to update our regulatory frameworks and work together with other relevant stakeholders, including young people, to ensure digital ecosystems evolve in a way that reflects our shared values. We commit to preserve an open, interoperable, reliable and secure internet, one that is unfragmented, supports freedom, innovation and trust which empowers people. If used properly, technologies can help us strengthen health capacities, tackle environmental threats, widen access to education and open new economic opportunities. We will leverage these technologies to advance tech for the common good and promote digital literacy worldwide. We will strengthen coordination on and support for the implementation and development of global norms and standards to ensure that the use and evolution of new technologies reflects our shared democratic values and commitment to open and competitive markets, strong safeguards including for human rights and fundamental freedoms. We also affirm our opposition to measures which may undermine these democratic values, such as government-imposed internet shutdowns and network restrictions. We support the development of harmonised principles of data collection which encourage public and private organisations to act to address bias in their own systems, noting new forms of decision-making have surfaced examples where algorithms have entrenched or amplified historic biases, or even created new forms of bias or unfairness.*

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

To advance global norms and standards for privacy and digital regulation, the Digital Ministers of the G7 nations expressed a commitment 'to identify commonalities in regulatory approaches' and the following views, and tasked the UK's Information Commissioner to spearhead multilateral initiatives (in 2021) in support of international regulatory cooperation on privacy. The Digital Ministers agreed to:

- *BUILD on OECD analysis including 'Going Digital III - horizontal project on data governance for growth and well-being' and 'Mapping commonalities in regulatory approaches to cross-border data transfers'. We will highlight best practice case studies, enhance cooperation on data governance and data protection, identify opportunities to overcome differences, explore commonalities in regulatory approaches and promote interoperability between members.*
- *ORGANISE an event comprising, and developed in collaboration with, all G7 Data Supervisory Authorities and/or other competent authorities for data, led by the UK's Information Commissioner's Office. The event, to take place in 2021, will consider regulatory cooperation with a potential focus on innovative approaches, enforcement of regulation and regulation enabling cross-border data flows.*
- *ORGANISE a separate cross-sectoral regulators' event in 2021, that will bring together Data Supervisory Authorities and/or other competent authorities for data, and other regulators from across the digital sphere to share best practice and support international cooperation.*

The President of the United States and leaders of the European Union committed to regulatory cooperation on data governance, cybersecurity and privacy at their summit on 15 June 2021. They committed to work together 'to ensure safe, secure, and trusted cross-border data flows that protect consumers and enhance privacy protections, while enabling Transatlantic commerce'. The leaders also resolved to boost cybersecurity information sharing as well as cybersecurity certifications for products and software.

The joint summit statement provided numerous, encouraging signals regarding a strongly shared desire to ameliorate US–EU tensions on privacy and data protection and 'strengthen legal certainty in Transatlantic flows of personal data'. The statement promises to:

> *avoid new unnecessary technical barriers to trade; to coordinate, seek common ground, and strengthen global cooperation on technology, digital issues, and supply chains; … to cooperate on compatible and international standards development; to facilitate regulatory policy and enforcement cooperation and, where possible, convergence; to promote innovation and leadership by U.S. and European firms*

The statement, which describes the US and EU as a community of '780 million people who share democratic values and the largest economic relationship in the world', said that the two jurisdictions decided to kick-start effective cooperation by establishing a high-level US–EU Trade and Technology Council (TTC). The new TTC is intended to:

> *avoid new unnecessary technical barriers to trade; to coordinate, seek common ground, and strengthen global cooperation on technology [and] digital issues; [and] to facilitate regulatory policy and enforcement cooperation and, where possible, convergence; [and] to promote innovation*

The TTC will focus initially on technology standards cooperation for artificial intelligence, the internet of things, other emerging technologies, data governance and technology platforms.

Given this formidable attention and commitment from heads of state and ministers, privacy and digital governance are unmistakably ensconced among the top objectives of the free world. Moreover, the world's democracies are manifestly inclined to cooperate on finding commonalities and convergence, and 'strengthen[ing] legal certainty', to promote both privacy and innovation for their citizens. This is good news indeed for the future of international digital governance.

The world's leaders have also demonstrated that our current concept of privacy is broad and elastic: it subsumes far more than personal data protection. The world's policy leaders now look to privacy to provide the governance framework for addressing the broader social challenges of emerging technology.

Yet, in what may be among the year's most surprising twists, the People's Republic of China adopted a comprehensive privacy law this year. The Wall Street Journal's headline of 20 August 2021 described this shocking development as follows: 'China Passes One of the World's Strictest Data-Privacy Laws; China's once-freewheeling internet faces new rules protecting personal data, as the world's largest online population awakens to privacy concerns'.

China's new Personal Information Protection Law, which takes effect on 1 November 2021, is said to be patterned after the European Union's General Data Protection Regulation (GDPR) insofar as it entails prior consent to and minimisation regarding the collection of personal data. Based on press reports, the law apparently also requires prominent notice of public facial recognition cameras and transparency and fairness regarding automated decision-making. Supposedly it will require the ability to opt out of personalised marketing and addresses the issue of 'algorithmic discrimination'. Like the GDPR, the new Chinese law provides for potentially enormous fines for privacy violations, which apparently may go as high as 5 per cent of a company's business income for the prior year.

Time and actual experience will tell whether the privacy law enacted by perhaps the world's most intrusive surveillance state can be taken at face value and if it will live up to the *Wall Street Journal*'s advance billing. But the very fact that China passed a major law to protect personal data demonstrates there is no stopping the international movement toward privacy.

Likewise, in the US, there has been no cessation of privacy developments throughout America. Indeed, privacy law has been a moving, and growing, target among the 50 states and federal government.

It was California that first imported the GDPR into American law. It started with the California Consumer Privacy Act in 2018, which was almost immediately substantially overhauled and tightened two years later by the California Privacy Rights Act.

In 2021, the states of Virginia and Colorado adopted comprehensive privacy laws based on the California and GDPR models. All of these laws entail similar individual (i.e., 'data subject') rights to access, delete, correct, port out their personal data, and to varying degrees, to opt out or limit the sale of personal data, targeted advertising, and legally or materially significant profiling.

The new laws generally obligate companies that control the collection and use of personal data to discharge the following duties: transparency (essentially, privacy notices that meaningfully describe what personal data is collected, for what purposes, and with what entities it is shared); purpose specification (i.e., the specific reasons why the data is collected); limitation of secondary uses that are incompatible with the specified purposes; data minimisation; avoidance of unlawful discrimination, heightened consent, assessment and documentation requirements for processing sensitive data; and, like the GDPR, requirements to memorialise controls imposed on third-party data processing in written contracts.

These new state laws will go into effect in 2023. Nevada also expanded its privacy law in 2021. Though Nevada's privacy law does not qualify as comprehensive, the amendments broaden consumers' right to block the sale of their personal information to third parties, and like in California and Vermont, Nevada's new law will regulate data brokers, namely 'persons whose primary business is purchasing covered information about consumers with whom the person does not have a direct relationship . . . and making sales of such covered information'.

Significantly, only California has created a new enforcement agency with jurisdiction over data protection, the California Privacy Protection Agency. And only California has granted individuals a private right of action to sue companies for violations of the state's privacy law. (Even then, California only provides a private right of action limited to suing over personal data breaches that result from a company's failure to implement reasonable data security practices.) The other states with new privacy laws will continue to rely on enforcement by existing officials such as attorneys general or, in the case of Colorado, local district attorneys in addition to the state attorney general.

It should also be noted that in 2021 the Uniform Law Commission in the US finalised its version of model legislation (i.e., a consensus template) that could be adopted in full by any state that chooses to do so. The Commission's Uniform Personal Data Protection Act (UPDPA) is generally comparable to the laws of California, Virginia and Colorado, but is considered to pose a somewhat lower compliance burden and, thus, may be more business- and innovation-friendly. The UPDPA is modelled to some extent on the federal Privacy Act of 1974, and only applies its data protection regulatory requirements to personal data that a company maintains in a 'system of records' that it uses to retrieve data about individuals for purposes of making individualised communications or decisions.

Interestingly, the UPDPA stipulates specific data practices that are prohibited. Providing a list of prohibited practices is useful because it could focus the regulator's mind on data-related risks that are truly injurious or actually unfair. Targeting regulation and enforcement at well characterised injuries, rather than at illusory or hyper-technical ones, helps avoid the risk of over-regulation. As the US Supreme Court confirmed again in 2021, in *TransUnion v. Ramirez*, some data practice failures (like inaccurate information that is never communicated outside of an internal database and never affects anyone) may not give rise to legally actionable harm.

The list of prohibited practices articulated by UPDPA is instructive as to what data practices could give rise to genuine harm to individuals:

Processing personal data is a prohibited data practice if the processing is likely to:

a subject a data subject to specific and significant: (1) financial, physical, or reputational harm; (2) embarrassment, ridicule, intimidation, or harassment; or (3) physical or other intrusion on solitude or seclusion if the intrusion would be highly offensive to a reasonable person;

b result in misappropriation of personal data to assume another's identity;

c constitute a violation of other law, including federal or state law against discrimination;

d fail to provide reasonable data-security measures, including appropriate administrative, technical, and physical safeguards to prevent unauthorised access; or

e process personal data without consent in a manner that is an incompatible data practice.

The Commission's effort could be significant. It is a highly respected body that previously drafted, for example, the Uniform Commercial Code and the Uniform Fiduciary Access to Digital Assets Act, both of which have been adopted in nearly every state.

In any event, with all this state by state and model law drafting activity, it can be stated with confidence that the US Congress will continue to cogitate over federal, comprehensive legislation.

During the next year we will see whether the US federal government can catch up with states and deliver comprehensive legislation, whether the UK's Information Commissioner will deliver on the G7's mandate to develop and harmonise global standards and norms for privacy and whether China will deliver on the potential of its strict new privacy law – or whether it will merely deliver more domestic surveillance and dominion over foreign and domestic technology companies.

As always, in the year ahead there will be both promise and peril for the future of privacy.

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. Mr Raul is a lecturer on law at Harvard Law School, where he teaches a course on 'Digital Governance: Privacy and Technology Trade-Offs'.

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 978-1-83862-810-9