THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2022
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 LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGERS
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Leke Williams

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.TheLawReviews.co.uk

ISBN 978-1-80449-116-4

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:

ANDERSON LLOYD

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

KALUS KENNY INTELEX

KHODEIR AND PARTNERS

K&K ADVOCATES

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

At the time of this writing, the most important privacy and cybersecurity highlights of 2022 are the ones that haven't happened – they are the developments that are in process but have not yet concluded. In other words, 2022 is going to be a significant transitional year.

First, some big things did happen. In the United States, Colorado, Virginia, Utah and Connecticut joined California in adopting major, comprehensive privacy regimes modeled essentially on the California Consumer Privacy Act and its successor, the California Privacy Rights Act, and thus patterned as well on the EU's General Data Protection Regulation. The United States also adopted a new law, the CHIPS and Science Act, designed to promote US global leadership on semiconductors, among other things.

At the US federal level, Congress passed and, in March, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA will require the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware. CISA began its rulemaking process on the new mandatory cyber incident reporting in September with a Request for Information calling for input in November 2022.

In a ceremony held at the US Department of Commerce in April 2022, Canada, Japan, the Philippines, Singapore, South Korea, Chinese Taipei and the United States – seven of the nine economies participating in the Asia-Pacific Economic Cooperation (APEC) economies, Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) System for managing privacy and personal data flows across borders – released a declaration announcing the establishment of the Global CBPR Forum. The plan is to transition operations of those systems out of APEC and into the new CBPR Forum. This transition will initially entail little change; all approved accountability agents and certified organisations will 'automatically' be recognised in the initial iteration of the global systems 'based on the same terms that they are recognised within the APEC CBPR and PRP Systems'.

One of the primary benefits of the Global CBPR Forum will be the expansion of the US approach to data flows beyond the Indo-Pacific. Although the Forum currently consists of APEC economies exclusively, '[p]articipation in the Global CBPR Forum is intended to be open, in principle, to those jurisdictions which accept the objectives and principles of the Global CBPR Forum as embodied in [the] Declaration'. The ceremony in the United States was attended by representatives from 20 different jurisdictions from not only the Asia-Pacific region, but also Europe, Latin America and the Middle East, and involved multi-stakeholder discussions about the creation of the Global CBPR Forum.

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

China's Personal Information Protection Law came into effect in late 2021, but was significantly elucidated in regulations issued in 2022. These important new rules relate to required mechanisms for cross-border data transfers, such as approval of Security Assessment Measures by the Cyberspace Administration of China, approved third-party transfer certification, or adoption of approved standard contract clauses.

Over 2022 (and 2021), the European Data Protection Board (EDPB) provided guidance on, among other things, the right of access and dark patterns in social media platforms as well as draft guidance on international transfers. The EDPB also published, together with the European Data Protection Supervisor (EDPS), views on various aspects of European Commission data governance proposals including on Artificial Intelligence and the European Health Data Space. The Commission also published FAQs on the New EU Standard Contractual Clauses.

However, much of the action on privacy, cybersecurity and digital technology policy either didn't happen in 2022, or hasn't quite happened yet.

In the European Union, the various proposals addressed in opinions by the EDPB and EDPS, relate to measures that are still pending in various states of publication, review and approval: the Digital Markets Act, the Data Governance Act, the Digital Services Act, the Data Act, the Artificial Intelligence Act, and others.

In the United States, comprehensive privacy legislation has stalled again on the issue of providing a private right of litigation to data subjects – as opposed to limiting enforcement to the Federal Trade Commission (FTC) and State Attorneys General – and on the question of whether the new federal privacy law will 'preempt' state law; that is, supersede or displace the new comprehensive privacy laws adopted by California and other states.

While we wait for a new federal privacy law, or not, the FTC has not stood still. In August, the agency announced plans to commence a major new rulemaking on essentially all aspects of privacy, data protection, cybersecurity, and emerging technologies and automated decision-making.

The FTC signaled its perspective on current business practices by referring to the purpose of its advance notice of proposed rulemaking as 'cracking down on commercial surveillance and lax data practices'. Two Republican-appointed Commissioners dissented from the adoption of the advance proposal, with one Commissioner, Noah Phillips, observing that the majority had borrowed an academic pejorative to connote its intentions (presumably from Professor Shoshana Zuboff's books and articles on 'Surveillance Capitalism') and noted that the majority's proposal appeared to reflect a 'dystopic' view of modern commerce.

The other dissenting Commissioner, Christine Wilson, expressed particular concern that the FTC's behemoth of a proposal could actually serve to deter or delay adoption of the comprehensive privacy legislation pending in Congress.

Given the breadth of the FTC advanced rulemaking proposal, quoting some excerpts from the FTC about its actions helps demonstrate the intended direction of the agency under the leadership of Chair Lina Khan:

a Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Mass surveillance has heightened the risks and stakes of data breaches, deception, manipulation, and other abuses.

b The growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used—means that potentially unlawful practices may be prevalent. Our goal

today is to begin building a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices and what those rules should potentially look like.

c The business of commercial surveillance can incentivize companies to collect vast troves of consumer information, only a small fraction of which consumers proactively share. Companies reportedly surveil consumers while they are connected to the internet – every aspect of their online activity, their family and friend networks, browsing and purchase histories, location and physical movements, and a wide range of other personal details.

d Companies use algorithms and automated systems to analyze the information they collect. And they make money by selling information through the massive, opaque market for consumer data, using it to place behavioral ads, or leveraging it to sell more products.

e For example, some companies fail to adequately secure the vast troves of consumer data they collect, putting that information at risk to hackers and data thieves. There is a growing body of evidence that some surveillance-based services may be addictive to children and lead to a wide variety of mental health and social harms.

f While very little is known about the automated systems that analyze data companies collect, research suggests that these algorithms are prone to errors, bias, and inaccuracy. As a result, commercial surveillance practices may discriminate against consumers based on legally protected characteristics like race, gender, religion, and age, harming their ability to obtain housing, credit, employment, or other critical needs.

g Companies increasingly employ dark patterns or marketing to influence or coerce consumers into sharing personal information.

The United Kingdom, in contrast, may be interested in moving in another direction.

While retaining 'adequacy' for purposes of data transfers from the European Union – and perhaps proceeding quickly to grant UK 'adequacy' to the US and other important trading partners – is crucial for the UK going forward, the current government introduced a bill in Parliament, the Data Protection and Digital Information Act (DPDI), to 'boost British Business, protect consumers and seize the benefits of Brexit'.

Most mercifully, the bill would, among other things, reduce the need for incessant cookie banners to continuously pop up during web browsing. That alone could endear the proposal to legions of internet users.

Other provisions would 'make it easier for businesses and researchers to unlock the power of data to grow the economy and improve society, but retains our global gold standard for data protection'. Key objectives are said to be 'clamp[ing] down on bureaucracy, red tape and pointless paperwork' and 'cementing post-Brexit Britain's position as a science and tech superpower'. The DPDI would also modernise the Information Commissioner's Office by incorporating a chair, chief executive and board, and enhance the ICO's mandate to take account of economic growth, innovation and competition.

Specifically, the Department for Digital, Culture, Media & Sport (DCMS) described the benefits of the DPDI as achieving or correcting the following:

a reducing burdens on businesses;

b a lack of clarity in the legislation has led to an over-reliance on 'box-ticking' to seek consent from individuals to process their personal data to avoid non-compliance:

its largely one-size-fits-all approach, regardless of the relative risk of an individual organisation's data processing activities, puts disproportionate burdens on small businesses including startups and scaleups;

c the government's new data protection rules will be focused on outcomes to reduce unnecessary burdens on businesses;

d this bill will remove the UK GDPR's prescriptive requirements giving organisations little flexibility about how they manage data risks, including the need for certain organisations, such as small businesses, to have a Data Protection Officer (DPO) and to undertake lengthy impact assessments; and

e organisations will still be required to have a privacy management programme to ensure they are accountable for how they process personal data. The same high data protection standards will remain but organisations will have more flexibility to determine how they meet these standards.

As one can see, quite a bit of different agenda appears to be coming out of the UK's DCMS than from Lina Khan's FTC. However, given the new Prime Minister in the UK, and mourning the passing of the Queen, immediate parliamentary action on DPDI has been suspended.

In all, given how privacy, cybersecurity and digital tech policy is moving wildly around in 2022, stay tuned and buckle up to get ready for 2023 and beyond.

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 (and then independent) 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 has also served as a member of 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 Kennedy School of Government and Yale Law School. Mr Raul serves as a Lecturer on Law at Harvard Law School where he teaches a course on 'Digital Governance: Privacy and Technology Trade-offs'.

SIDLEY AUSTIN LLP

NEO Building
Rue Montoyer 51 Montoyerstraat
B-1000 Brussels
Belgium
Tel: +32 2 504 64 00
jquartilho@sidley.com

39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645 / 2509 7868 / 2509 7637

Fax: +852 2509 3110
yuetming.tham@sidley.com
linh.lieu@sidley.com
lester.fung@sidley.com

ISBN 978-1-80449-116-4