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 29

UNITED STATES

Alan Charles Raul and Snezhana Stadnik Tapia[1]

I OVERVIEW – THE 'CHANGING ZEITGEIST'

Nearly 130 years ago, two American lawyers, Samuel Warren and Louis Brandeis – the latter of whom would eventually become a Supreme Court Justice – wrote an article in the *Harvard Law Review* expressing their concern that technological advances like 'instantaneous photographs' and the 'newspaper enterprise' were threatening to 'make good the prediction that "what is whispered in the close shall be proclaimed from the house-tops"'.[2] To address this trend, Warren and Brandeis argued that courts should recognise a common law tort based on violations of an individual's 'right to privacy'.[3] US courts eventually accepted the invitation, and it is easy to consider Warren and Brandeis's article as the starting point of modern privacy discourse.

It is also easy to consider the article as the starting point of the United States' long history of privacy leadership. From the US Supreme Court recognising that the US Constitution grants a right to privacy against certain forms of government intrusion to the US Congress's enacting the Privacy Act to address potential risks created by government databases to US states adopting laws imposing data breach notification and information security requirements on private entities, the United States has long innovated in the face of technological and societal change.

---

1 Alan Charles Raul is a partner, and Snezhana Stadnik Tapia is an associate, at Sidley Austin LLP. The authors wish to thank Christopher C Fonzone, who co-authored the prior version of this chapter, for his extensive contributions to this current version. The authors also wish to thank Vivek K Mohan, Tasha D Manoranjan and Frances E Faircloth, who were previously associates at Sidley, for their contributions to prior versions of this chapter. Passages of this chapter were originally published in 'Privacy and data protection in the United States', The debate on privacy and security over the network: Regulation and markets, 2012, Fundación Telefónica; and Raul and Mohan, 'The Strength of the U.S. Commercial Privacy Regime', 31 March 2014, a memorandum to the Big Data Study Group, US Office of Science and Technology Policy.

2 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890). The piece by Warren and Brandeis is the second most cited law review article of all time. See Fred R. Shapiro & Michelle Pearse, *The Most-Cited Law Review Articles of All Time*, 110 Mich. L. Rev. 1483, 1489 (2012) (noting that the most cited is R.H. Coase's 'The Problem of Social Cost', which famously introduced 'The Coase Theorem'). It has also created an arms race among legal scholars to come up with new superlatives to describe it: 'monumental', Gordon, *Right of Property in Name, Likeness, Personality and History*, 55 Nw. U.L. Rev. 553, 553 (1960); an article of 'prestige and enormous influence', Robert C. Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 Case W. Res. L. Rev. 647, 647 (1991); the 'most influential law review article of all', Harry Kalven, Jr., *Privacy in Tort Law – Were Warren and Brandeis Wrong?*, 31 Law & Contemp. Probs. 326, 327 (1966); etc.; etc.

3 Warren & Brandeis, *supra* note 2, at 213.

In recent years, however, privacy commentators have painted the United States in a different light. Over the last generation, the United States has balanced its commitment to privacy with its leadership role in developing the technologies that have driven the information age. This balance has produced a flexible and non-prescriptive regulatory approach focused on post hoc government enforcement (largely by the Federal Trade Commission) and privacy litigation rather than detailed prohibitions and rules, sector-specific privacy legislation focused on sensitive categories of information, and laws that seek to preserve an internet 'unfettered by Federal or State regulation'. The new technologies that have changed the day-to-day lives of billions of people and the replication of US privacy innovations around the globe have – at least to US regulators – long indicated the wisdom of this approach.

But there is now a growing perception that other jurisdictions have seized the privacy leadership mantle by adopting more comprehensive regulatory frameworks, exemplified by the European Union's General Data Protection Regulation (GDPR). A series of high-profile data breaches in both the public and private sectors and concerns about misinformation and the misuse of personal information have also created a 'crisis of new technologies' or 'techlash' that is shifting popular views about privacy in the United States. In addition, the covid-19 pandemic, and the digital innovations being developed to mitigate the spread of the virus, have placed privacy at the forefront of public attention. Once again, it seems, the United States is starting to undergo a period of intense privacy innovation in response to a new technological world.

In short, the US privacy zeitgeist is shifting – and this chapter, while not providing a comprehensive overview of the rich US privacy and cybersecurity landscape, will attempt to show how that is the case. The chapter will begin with an overview of the existing US regulatory and enforcement framework – which exemplifies the balance between privacy protection and innovation described above. The chapter will then describe, with a focus on the concrete developments over the past year, the significant shift in how the United States is thinking about privacy and privacy regulation that appears to be underway:

a How the covid-19 pandemic – and the technological solutions being considered to help manage it – have placed issues concerning the collection and use of personal data front and centre in one of the biggest issues of this or any year, leading to intense discussions over privacy regulation.

b How all three branches of the federal US government are actively taking steps to confront the privacy and cybersecurity questions of the day.

c How the real action continues to be not in Washington DC, but rather in the 50 US states – as California's far-reaching comprehensive privacy bill called 'California's GDPR' went into effect on 1 January 2020, and numerous other states either have enacted or are considering substantial new privacy legislation. The locus of action may likely shift to Washington in 2021.

d And how, not to be outdone, companies are also increasingly recognising that they have to establish 'digital governance' at the board or C-suite level to address strategy and oversight for privacy, data protection, cybersecurity, and disruptive technologies.

The chapter then concludes by detailing a very significant change in the international data transfer framework between the EU and US, considerations for foreign organisations that must engage with the US privacy regime, and some thoughts on how that regime may continue to evolve going forward.

II THE US REGULATORY FRAMEWORK, INCLUDING PUBLIC AND PRIVATE ENFORCEMENT

As noted above, businesses in the United States are subject to a web of privacy laws and regulations at the federal and state level. Privacy and information security laws typically focus on the types of citizen and consumer data that are most sensitive and at risk, although if one of the sector-specific federal laws does not cover a particular category of data or information practice, then the Federal Trade Commission (FTC) Act, and each state's 'little FTC Act' analogue, comes into play. As laid out below, these general consumer protection statutes broadly, flexibly, and comprehensively proscribe unfair or deceptive acts or practices. Federal and state authorities, as well as private parties through litigation, actively enforce many of these laws, and companies also, in the shadow of this enforcement, take steps to regulate themselves. In short, even in the absence of a comprehensive federal privacy law, there are no substantial lacunae in the regulation of commercial data privacy in the United States. Indeed, in a sense, the United States has not one, but many, de facto privacy regulators overseeing companies' information privacy practices, with the major sources of privacy and information security law and standards in the US these regulators enforce – federal, state, private litigation, and industry self-regulation – briefly outlined below.

i Privacy and data protection legislation and standards – federal law (including general obligations for data handlers and data subject rights)

General consumer privacy enforcement agency – the FTC

Although there is no single omnibus federal privacy or cybersecurity law nor designated central data protection authority, the FTC comes closest to assuming that role for consumer privacy in the US.[4] The statute establishing the FTC, the FTC Act, grants the Commission jurisdiction over essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[5] And while the Act does not expressly address privacy or information security, the FTC has interpreted the Act as giving it authority to regulate information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities – and accordingly to play a leading role in laying out general privacy principles for the modern economy.

The FTC has rooted its privacy and information security authority in Section 5 of the FTC Act, which charges the Commission with prohibiting 'unfair or deceptive acts or practices in or affecting commerce'.[6] An act or practice is deceptive under Section 5 if there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and the representation or omission is 'material'. The FTC has taken action against companies for deception when companies have made promises, such

4 This discussion refers generally to 'privacy' even though, typically, the subject matter of an FTC action concerns 'data protection' more than privacy. This approach follows the usual vernacular in the United States. See also Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 Columbia L. Rev. ('It is fair to say that today FTC privacy jurisprudence is the broadest and most influential force on information privacy in the United States – more so than nearly any privacy statute and any common law tort.') available at papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

5 See FTC, *What We Do*, www.ftc.gov/about-ftc/what-we-do. The FTC's jurisdiction spans across borders – Congress has expressly confirmed the FTC's authority to provide redress for harm abroad caused by companies within the United States. Federal Trade Commission Act, 15 U.S.C. § 45(a)(4) (1914).

6 id. at § 5.

as those relating to the security procedures purportedly in place, and then not honoured or implemented them in practice. An act or practice is 'unfair' under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition. The FTC thus understands unfairness to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context.

A few examples of what the FTC believes constitutes unfair or deceptive behaviour follow. First, the FTC takes the position that, among other things, companies must disclose their privacy practices adequately and that, in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses.[7]

Second, the FTC also takes the position that Section 5 generally prohibits a company from using previously collected personal data in ways that are materially different from, and less protective than, what it initially disclosed to the data subject, without first obtaining the individual's additional consent.[8]

Finally, the FTC staff has also issued extensive guidance on online behavioural advertising, emphasising four principles to protect consumer privacy interests:

a transparency and control, giving meaningful disclosure to consumers, and offering consumers choice about information collection;

b maintaining data security and limiting data retention;

c express consent before using information in a manner that is materially different from the privacy policy in place when the data were collected; and

d express consent before using sensitive data for behavioural advertising.[9]

The FTC has not, however, indicated that opt-in consent for the use of non-sensitive information is necessary in behavioural advertising.

In terms of enforcement, the FTC has frequently brought successful actions under Section 5 against companies that did not adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments, or failed to provide a 'fair' level of security for consumer information. Although various forms of relief (such as injunctions and damages) for privacy-related wrongs are available, the FTC has frequently resorted to issuing consent decrees. Such decrees generally provide for ongoing monitoring by the FTC, prohibit further violations of the law,

7 To this end, the FTC brought an enforcement action in 2009 against Sears for allegedly failing to disclose adequately the extent to which it collected personal information by tracking the online browsing of consumers who downloaded certain software. The consumer information allegedly collected included 'nearly all of the Internet behaviour that occurs on [. . .] computers'. The FTC thus required Sears to disclose prominently any data practices that would have significant unexpected implications in a separate screen outside any user agreement, privacy policy or terms of use. *See* Complaint, *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264, para. 4 (F.T.C. Sept. 9, 2009).

8 Complaint, In the Matter of Myspace LLC, Docket No. C-4369 (F.T.C. Sept. 11, 2012).

9 Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, at 39 (Feb. 2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

and subject businesses to substantial financial penalties for consent decree violations. These enforcement actions have been characterised as shaping a common law of privacy that guides companies' privacy practices.[10]

Cybersecurity and data breaches – federal law

Cybersecurity has been the focus of intense attention in the United States in recent years, and the legal landscape is dynamic and rapidly evolving. Nonetheless, at the time of writing, there is still no general law establishing federal data protection standards, and the FTC's exercise of its Section 5 authority, as laid out above, remains the closest thing to a general national-level cybersecurity regulation.

That said, recent years have brought a flurry of federal action related to cybersecurity. In 2015, Congress enacted the Cybersecurity Information Sharing Act (CISA),[11] which seeks to encourage cyberthreat information sharing within the private sector and between the private and public sectors by providing certain liability shields related to such sharing. CISA also authorises network monitoring and certain other defensive measures, notwithstanding any other provision of law. In addition to CISA, Presidents Obama and Trump have issued a series of executive orders concerning cybersecurity, which have, among other things, directed the Department of Homeland Security and a number of other agencies to take steps to address cybersecurity and protect critical infrastructure and directed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework.[12] The latter, in particular, has been a noteworthy development: while the NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, there is an increasing expectation that use of the framework (which is laudably accessible and adaptable) could become a best practice consideration for companies holding sensitive consumer or proprietary business data.

Specific regulatory areas – federal law

Along with the FTC's application of its general authority to privacy-related harms, the United States also has a number of specific federal privacy and data security laws for the types of citizen and consumer data that are most sensitive and at risk. These laws grant various federal agencies rule making, oversight, and enforcement authority, and these agencies often issue policy guidance on both general and specific privacy topics. In particular, Congress has passed robust laws that prescribe specific statutory standards for protecting the following types of information:

a financial information;
b healthcare information;
c information about children;
d telephone, internet and other electronic communications and records; and
e credit and consumer reports.

10 See, for example, Solove and Harzog, *supra* note 4.

11 Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114 – 113, 129 Stat. 2936 (codified at 6 U.S.C. §§ 1501–1510).

12 Exec. Order No. 13636, 78 F.R. 11737 (2013); Exec. Order No. 13718, 81 F.R. 7441 (2016); Exec. Order No. 13800, 82 F.R. 22391 (2017); Exec. Order No. 13873,84 F.R. 22689 (2019).

We briefly examine each of these categories, and the agencies with primary enforcement responsibility for them, below.

Financial information

The Gramm-Leach-Bliley Act (GLBA)[13] addresses financial data privacy and security by establishing standards pursuant to which financial institutions must safeguard and store their customers' 'non-public personal information' (or 'personally identifiable financial information'). In brief, the GLBA requires financial institutions to notify consumers of their policies and practices regarding the disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties, unless consumers have the right to opt out or other exceptions apply; and to establish safeguards to protect the security of personal information. The GLBA and its implementing regulations further require certain financial institutions to notify regulators and data subjects after breaches implicating non-public personal information.

Various financial regulators, such as the federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency) and the Securities and Exchange Commission (SEC), have authority to enforce consumer privacy under the GLBA, while the FTC (for non-bank financial institutions) and the Consumer Financial Protection Bureau (CFPB) (for certain banks and non-bank financial institutions) do as well.

The SEC has also increasingly used its broad investigative and enforcement powers over public companies who have suffered cybersecurity incidents. In doing so, the SEC has relied on multiple theories, including that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to do so and that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. Of particular note, in 2018, the SEC published interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors.[14] The SEC suggested that all public companies adopt cyber disclosure controls and procedures that enable companies to:

a identify cybersecurity risks and incidents;
b assess and analyse their impact on a company's business;
c evaluate the significance associated with such risks and incidents;
d provide for open communications between technical experts and disclosure advisers;
e make timely disclosures regarding such risks and incidents; and
f adopt internal policies to prevent insider trading while the company is investigating a suspected data breach.

Healthcare information

For healthcare privacy, entities within the Department of Health and Human Services (HHS) administer and enforce the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[15] as amended by the Health Information Technology for Economic and

13 Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (codified and amended at scattered sections of 12 and 15 U.S.C. (2015)).

14 SEC Statement and Guidance on Public Cybersecurity Disclosures, 17 C.F.R. §§ 229, 249 (2018).

15 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified and amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

Clinical Health Act (HITECH).[16] Congress enacted HIPAA to create national standards for electronic healthcare transactions, and HHS has promulgated regulations to protect the privacy and security of personal health information. In general, HIPAA and its implementing regulations state that patients generally have to opt in before covered organisations can share the patients' information with other organisations.

HIPAA's healthcare coverage is quite broad. It defines 'protected health information,' often referred to as PHI, as 'individually identifiable health information . . . transmitted or maintained in electronic media' or in 'any other form or medium'.[17] 'Individually identifiable health information' is in turn defined as a subset of health information, including demographic information, that 'is created or received by a health care provider, health plan, employer, or health care clearinghouse'; that 'relates to the past, present, or future physical or mental health or condition of an individual', 'the provision of health care to an individual', or 'the past, present, or future payment for the provision of health care to an individual'; and that either identifies the individual or provides a reasonable means by which to identify the individual.[18] Notably, HIPAA does not apply to 'de-identified' data.

With respect to organisations, HIPAA places obligations on 'covered entities', which include health plans, healthcare clearing houses and healthcare providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.[19]

Moreover, HIPAA also places obligations on 'business associates,' which are required to enter into agreements, called business associate agreements, to safeguard PHI. A business associate is defined as an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities).[20] Such agreements require business associates to use and disclose PHI only as permitted or required by the agreement or as required by law and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement. The agreements also include numerous other provisions regarding the confidentiality, integrity and availability of electronic PHI.

HIPAA and HITECH not only restrict access to and use of PHI, but also impose stringent information security standards. In particular, HHS administers the HIPAA Breach Notification Rule, which imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI maintained by covered entities and their business associates. The HIPAA Security Rule also requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI.

16 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, 467 (codified in scattered sections of 42 U.S.C. (2009)).

17 45 C.F.R. § 160.103.

18 45 C.F.R. § 160.103.

19 45 C.F.R. § 164.504(f)(3)(iii).

20 45 C.F.R. § 164.103.

Information about children

The Children's Online Privacy Protection Act of 1998 (COPPA) applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. The FTC is generally responsible for enforcing COPPA's requirements, which include, among other things, that these website operators post a privacy policy, provide notice about collection to parents, obtain verifiable parental consent before collecting personal information from children, and other actions.[21]

Telephone, internet, and other electronic communications and records

A number of legal regimes address communications and other electronic privacy and security, and only the briefest discussion of this highly technical area of law is possible here. In short, some of the key statutory schemes are as follows:

a the Electronic Communications Privacy Act of 1986 (ECPA) protects the privacy and security of the content of certain electronic communications and related records;[22]

b the Computer Fraud and Abuse Act (CFAA) prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks;[23]

c various sections of the Communications Act protect telecommunications information, including what is known as customer proprietary network information, or CPNI;[24]

d the Telephone Consumer Protection Act (TCPA) governs robocalls;[25] and

e the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act governs commercial email messages, generally permitting companies to send commercial emails to anyone provided that: the recipient has not opted out of receiving such emails from the company, the email identifies the sender and the sender's contact information, and the email has instructions on how to easily and at no cost opt out of future commercial emails from the company. (Text messages generally require express written consent, and are thus a significant class action risk area.)[26]

The Federal Communications Commission (FCC) is the primary regulator for communications privacy issues, although it shares jurisdiction with the FTC on certain issues, including notably the TCPA.

21 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505.

22 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C. (1986)).

23 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1984).

24 Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified in scattered sections of 47 U.S.C. (1934)).

25 Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (codified at 47 U.S.C. § 227 (1991)).

26 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § § 7701–7713 (2003); 18 U.S.C. § 1037 (2003).

Credit and consumer reports

The Fair Credit Reporting Act (FCRA),[27] as amended by the Fair and Accurate Credit Transactions Act of 2003,[28] imposes requirements on entities that possess or maintain consumer credit reporting information or information generated from consumer credit reports. Consumer reports are 'any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility' for credit, insurance, employment or other similar purposes.

The CFPB, FTC, and federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency) share authority for enforcing FCRA, which mandates accurate and relevant data collection to give consumers the ability to access and correct their credit information and limits the use of consumer reports to permissible purposes such as employment, and extension of credit or insurance.[29]

ii Privacy and data protection legislation and standards – state law

Oversight of privacy is by no means exclusively the province of the federal government. All 50 US states also engage in some form of privacy and data protection regulation, with particular emphasis on data security and breach notifications. Moreover, state attorneys general have become increasingly active with respect to privacy and data protection matters, often drawing on authorities and mandates similar to those of the FTC. Of particular note, as the largest of the US states, the home to Silicon Valley, and a frequent regulatory innovator, California continues to be a bellwether for US privacy and data protection legislation, with businesses across the United States often applying its regulatory approaches, whether or not they are jurisdictionally required to do so.[30] (To this end, Section III, below, will discuss the highly significant California Consumer Privacy Act of 2018, which went into effect on 1 January 2020.)

Cybersecurity and data breaches – state law

The United States was unquestionably a world leader in establishing information security and data breach notification mandates, and the states played an integral, if not the integral, role. Although the federal government did not – and still has not – put in place a general national standard, all 50 states, the District of Columbia, and other US jurisdictions have imposed their own affirmative data breach notification requirements on private entities that collect or process personal data. California, as is so often the case, was the first: in 2003 the California legislature required companies to notify individuals whose personal information was compromised or improperly acquired. Other states soon followed, and companies who

27 Fair Credit Reporting Act, 12 U.S.C. §§ 1830–1831 (1970); 15 U.S.C. § 1681 et seq. (1970).

28 Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. §§ 1681c–1, 1681j, 1681 s–3 (2010)); 20 U.S.C. § 9701–9708 (2003)).

29 Fair Credit Reporting Act, 15 U.S.C. § 621.

30 State of California Department of Justice, *Privacy Laws*, oag.ca.gov/privacy/privacy-laws.

have had nationwide data breaches must now research a number of different laws – which are largely similar, but differ in subtle and important ways – to determine their notification obligations.

In addition to the data breach notification laws, states have also imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information.[31] For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls.[32] Likewise, as discussed below, the California Consumer Privacy Act contains security requirements, and a preliminary set of general safeguards went into effect this year in New York, to say nothing of the sector-specific cybersecurity rule issued by New York's Department of Financial Services (DFS). In short, absent pre-emptive federal legislation, we should expect to see states continuing to pass new legislation in this area, creating an increasingly complicated patchwork quilt of state laws for companies to navigate.

General consumer privacy enforcement – 'Little FTCA' analogues

Similar to the FTC, state attorneys general possess the power to bring enforcement actions based on unfair or deceptive trade practices. The source of this power is typically a 'Little FTC Act', which generally prohibits 'unfair or deceptive acts and practices' and authorises the state attorney general to enforce the law. In particular, the little FTCAs in 43 states and the District of Columbia include a broad prohibition against deception that is enforceable by both consumers and a state agency. Moreover, in 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

Thus, if one of the sector-specific federal or state laws does not cover a particular category of data or information practice, businesses may still find themselves subject to regulation. In fact, recent privacy events have seen increased cooperation and coordination in enforcement among state attorneys general, whereby multiple states will jointly pursue actions against companies that experience data breaches or other privacy allegations. Coordinated actions among state attorneys general often exact greater penalties from companies than would typically be obtained by a single enforcement authority. In recent years, attorneys general in states such as California, Connecticut and Maryland have formally created units charged with the oversight of privacy, and New York has created a unit to oversee the internet and technology.

Specific regulatory areas – state laws

While, as described above, the federal government has enacted a number of privacy and data protection laws that target particular industries, activities, and information types, the diversity of data laws is even greater at the state level. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues, such

31 National Conference of State Legislatures, *Security Breach Notification Laws*, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

32 201 Mass. Code Regs. 17.00 (West 2009).

as biometric information, cyberstalking,[33] data disposal,[34] privacy policies, employer access to employee social media accounts,[35] unsolicited commercial communications[36] and electronic solicitation of children,[37] to name just a few. State attorneys general also frequently issue policy guidance on specific privacy topics. For instance, like the FTC, California has also issued best-practice recommendations for mobile apps and platforms.

While a detailed discussion of all of the state laws and regulations is beyond the scope of this chapter, discussion of a couple of exemplary categories should illustrate their importance.

First, consider cybersecurity standards. New York's Department of Financial Services (DFS) is a key regulator here, recently promulgating safeguards that require banks, insurance companies and other financial service institutions it regulates to create and maintain a cybersecurity programme designed to protect consumers and New York's financial industry.[38] Thus, as of 28 August 2017, all financial institutions regulated by DFS – which is a wide-range of US financial institutions with a presence in many states – must create a cybersecurity programme that is approved by the board or a senior corporate official, appoint a chief information security officer, limit access to non-public data, and implement guidelines to notify state regulators of cybersecurity or data security incidents within 72 hours. Notably, the New York DFS filed its first enforcement action on 21 July 2020 against First American Title Insurance Company. Moreover, as described below, a number of states are promulgating similar or even broader cybersecurity requirements. For instance, New York has built upon the DFS standards by enacting the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which, among other things, requires entities that handle private information to implement a data security programme with 'reasonable' administrative, technical and physical safeguards. Second, consider privacy policies. As is typical, California plays an outsized role here, with its California Online Privacy Protection Act (CalOPPA) almost serving – as many of its laws do – as a de facto national standard and thus affecting businesses operating throughout the United States.[39] In short, CalOPPA requires operators to post a conspicuous privacy policy online that identifies the categories of personally identifiable information that the operator collects about individual consumers. The privacy policy must also detail how the operator responds to a web browser 'do not track' signal. California law also prohibits websites directed to minors from advertising products based on information specific to that minor, and the law further requires the website operator to

33 National Conference of State Legislatures, *Cybersecurity Legislation* 2016, www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx.

34 National Conference of State Legislatures, *Data Disposal Laws*, www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

35 National Conference of State Legislatures, *Access to Social Media Usernames and Passwords*, www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

36 National Conference of State Legislatures, *State Laws Relating to Unsolicited Commercial or Bulk E-mail* (SPAM), www.ncsl.org/research/telecommunications-and-information-technology/state-spam-laws.aspx.

37 National Conference of State Legislatures, *Electronic Solicitation or Luring of Children: State Laws*, www.ncsl.org/research/telecommunications-and-information-technology/electronic-solicitation-or-luring-of-children-sta.aspx.

38 N.Y. Comp. Codes R. & Regs. tit. 23, § 500.0 (West 2017).

39 See, for example, National Conference of State Legislatures, *Security Breach Notification Laws*, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, and National Conference of State Legislatures, *State Laws Related to Internet Privacy*; www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

permit a minor to request removal of content or information posted on the operator's site or service by the minor, with certain exceptions.[40] While California's privacy policy laws are likely the most prominent, they do not stand alone. For instance, Connecticut law requires any person who collects social security numbers in the course of business to create a publicly displayed privacy protection policy that protects the confidentiality of the sensitive number. Nebraska and Pennsylvania have laws that prohibit the use of false and misleading statements in website privacy policies.[41] And there are many other state laws concerning privacy policies, making this an excellent example of the many and diverse regulations that may be relevant to businesses operating across multiple US states.

iii Private litigation

Beyond federal and state regulation and legislation, the highly motivated and aggressive US private plaintiffs' bar adds another element to the complex system of privacy governance in the United States.

Many US laws authorise private plaintiffs to enforce privacy standards, and the possibility of high contingency or attorneys' fees highly incentivise plaintiffs' counsel to develop strategies to use these standards to vindicate commercial privacy rights through consumer class action litigation. A company may thus face a wave of lawsuits after being accused in the media of misusing consumer data, being victimised by a hacker, or suffering a data breach.

A full discussion of the many potential causes of action granted by US law is beyond the scope of this chapter, but a few examples will suffice to show the range of possible lawsuits. For example, plaintiffs often sue under state 'unfair and deceptive acts and practices' standards, and state law also allows plaintiffs to bring common law tort claims under general misappropriation or negligence theories. Moreover, as mentioned at the outset, US courts have long recognised privacy torts, with the legal scholar William Prosser building on the famed work of Brandeis and Warren to create a taxonomy of four privacy torts in his 1960 article, 'Privacy'[42] – a taxonomy that was later codified in the American Law Institute's famous and influential Restatement (Second) of Torts.[43] Thus, aggrieved parties can today bring a civil suit for invasion of privacy, public disclosure of private facts, 'false light', and appropriation or infringement of the right of publicity or personal likeness. Importantly, these rights protect not only the potential abuse of information, but generally govern its collection and use.

iv Industry self-regulation: company policies and practices

To address concerns about privacy practices in various industries, industry stakeholders have worked with the government, academics and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively developed accountability programmes establish expected practices for the use of consumer data within their sectors, which is then subject

40 Cal. Bus. & Prof. Code §§ 22580–22582 (West 2015).

41 National Conference of State Legislatures, *State Laws Related to Internet Privacy*, www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

42 William L. Prosser, Privacy, 48 Calif. L. Rev. 383 (1960).

43 Restatement (Second) of Torts § 652A (Am. Law Inst. 1977).

to enforcement by both governmental and non-governmental authorities. While there are obviously limits to industry self-regulation, these initiatives have led to such salutary developments as the Digital Advertising Alliance's 'About Advertising' icon and a policy on the opt-out for cookies set forth by the Network Advertising Initiative.[44]

Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. It should be noted that the same is true for companies that publish privacy policies – a company's failure to comply with its own privacy policy is a quintessentially deceptive practice. To this end, as noted above, California law requires publication or provision of privacy policy in certain instances, and numerous other state and federal laws do as well, including, inter alia, the GLBA (financial data) and HIPAA (health data).[45] In addition, voluntary membership or certification in various self-regulatory initiatives also requires posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on those policies.

III THE YEAR IN REVIEW – KEY REGULATORY AND ENFORCEMENT TRENDS

As noted at the outset, the privacy zeitgeist in the United States is shifting. The enactment of the European Union's General Data Protection Regulation, a series of high-profile data breaches, and concerns about misinformation and the misuse of personal information have created a 'crisis of new technologies' or 'techlash', which has shifted popular views about privacy in the United States and forced the hand of legislators and regulators. And the covid-19 pandemic has only heightened the importance of privacy considerations as technology advances. The United States is thus consequently undergoing a period of intense privacy innovation, with the federal government, state governments, and private industry all taking consequential steps to address this new world.

Given the sheer breadth and diversity of activity, this chapter cannot detail every key event in the US privacy and data protection landscape that occurred in the last year. Nonetheless, below we highlight the most important changes, which we believe more than demonstrate how dynamic this area is and will likely continue to be.

i Privacy and cybersecurity during the covid-19 pandemic

It is no understatement to say that the ongoing covid-19 pandemic has changed our world in ways that would have been unthinkable a year ago. And from the dramatic rise in teleworking to the need for employers to begin capturing significantly more health information about their employees as part of their back to work efforts to the use of novel technologies to track the disease, it is also no understatement to say that privacy and cybersecurity considerations have been central to the policy response to the crisis. This has led to a proliferation of federal, state, and local laws and guidance on how covid-19-related information is to be collected

44 See Digital Advertising Alliance (DAA), *Self-Regulatory Program*, www.aboutads.info; Network Advertising Initiative, *Opt Out Of Interest-Based Advertising*, www.networkadvertising.org/choices/?partnerId=1//.

45 National Conference of State Legislatures, *State Laws Related to Internet Privacy*, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

and used – with new directives being issued on almost a daily basis as this extremely dynamic situation unfolds and even Congress considering comprehensive covid-19-related privacy legislation.

First, one of the most immediate consequences of the covid-19 pandemic was that a large proportion of the US workforce was forced to begin teleworking almost overnight. This distributed environment raised the level of cybersecurity risk businesses face, as did the fact that cybersecurity criminals and scammers have increased their efforts to target vulnerable employers and workforces. Given this, several US federal agencies have issued guidance on cybersecurity risks in relation to covid-19 – for example, the Department of Homeland Security's Cyber and Infrastructure Security Agency (CISA) and the FTC have issued guidance on avoiding phishing and scam emails relating to covid-19.[46] And organisations have increased their preventative efforts, undertaking such tasks as reviewing and updating their incident response plans to address an increased attack surface resulting from remote work, ensuring regular patching and remote wiping, clarifying business continuity plans and processes with vendors and clients, and raising employee awareness about covid-19-related phishing emails.

Second, businesses have had to consider how to continue operating or reopen safely during the pandemic, which often involves or requires collecting sensitive health and related data (such as temperature and symptom checks, recent travel history, and contact with infected persons) before employees return to work and establishing protocols for symptom and exposure reporting. Various federal, state, and local agencies have issued mandatory or recommended guidance that touches on nearly every aspect of these 'return to work' issues – from what screening must and may be done, what information can and should be captured, and how long such information must and can be maintained. Indeed, the number of such mandatory or guidance documents is nearly as large as the number of jurisdictions in the United States. A good exemplar of what these directives and recommendations look like, and one that has had significant influence on many jurisdictions all over the country, is guidance from the Centers for Disease Control (CDC), which permits and encourages companies to take employee temperatures, while advising companies to act responsibly with regards to employees' privacy rights – for instance, by narrowly tailoring health questionnaires aimed to reduce the spread of covid-19 and ensuring that any retained medical information is stored securely.[47]

Federal, state, and local agencies have also promulgated guidance or released statements noting that they may modify their enforcement posture or reporting requirements during the pandemic. For example, the Department of Health and Human Services (HHS) has waived penalties and refrained from enforcing certain provisions under the HIPAA Privacy Rule, including the requirement to obtain patients' consent before speaking with family members or friends about patients' care, the requirement to distribute a privacy notice, and the patient's right to request privacy restrictions or request confidential communications.[48]

46 CISA Joint Alert, Avoid Scams Related to Economic Payments, COVID-19, https://www.cisa.gov/sites/default/files/publications/Avoid_Scams_Related_to_Economic_Payments_COVID-19.pdf; FTC, Coronavirus Advice for Consumers, https://www.ftc.gov/coronavirus/scams-consumer-advice.

47 *Guidance for Businesses & Employers*, CDC (May 6, 2020), https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html.

48 HHS, COVID-19 & HIPAA Bulletin Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency (Mar. 2020), https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf.

Third, besides having a substantial effect on how businesses operate, the covid-19 pandemic has prompted significant public and private sector efforts to develop technologies to help fight the spread of the virus. The list of such technologies is long: for example, researchers are examining how to leverage population data to help assess patients' symptoms;[49] artificial intelligence is being used to analyse medical images, such as chest X-rays and thoracic CT scans, in order to differentiate between diagnoses with covid-like symptoms;[50] and, most prominently, work is being done on how to use smartphones and their data to engage in contact tracing (i.e., using phones to alert people when they have come into contact with someone who has tested positive).

With respect to this last type of technology, opt-in contact-tracing applications are being built with a range of different functionalities. One common variation is an app that, using Bluetooth signals, would log other phones it comes into contact with that have also enabled the app in the form of random numerical ID codes. If an app user self-reports a positive test, anyone who had recently been near that user would receive an 'exposure notification' alert. Of course, using smartphones in this way, or many of the other ways under development, raises a number of questions under federal and state laws governing electronic communications (such as the Federal Wiretap and Stored Communications Acts), laws governing the privacy of health and medical information (such as HIPAA), and even more general privacy regimes like those enforced by the FTC and the California Consumer Privacy Act (CCPA). Businesses and other entities contemplating using such apps must also ensure that they are making appropriate disclosures to the employees that use them and obtaining any required consents to capture and use any information collected.

Fourth, and finally, the privacy and cybersecurity issues raised by the new information employers and technologies are gathering and may continue to gather is only heightening the perceived need for a national privacy framework, at least for regulatory clarity regarding how consumers' data can be collected and used in the context of the covid-19 pandemic. To that end, congressional Democrats and Republicans have both introduced bills to protect consumer data collected in coronavirus response efforts.

On 7 May 2020, Republicans introduced the COVID-19 Consumer Data Protection Act.[51] Aimed to protect personal health, geolocation and proximity data, the bill would require companies to delete or de-identify data after the pandemic ends. Notably, the bill carves out an exemption for employee screening data during covid-19. The Act would also require companies under the jurisdiction of the FTC to obtain affirmative express consent from individuals to collect, process, or transfer their personal health, geolocation, or proximity information for the purposes of tracking the spread of covid-19, and the bill specifies several covered purposes for the data.

Along the same lines, on 14 May 2020, Democrats in both the House and Senate introduced a competing bill, the Public Health Emergency Privacy Act.[52] The bill would also regulate what data companies can collect during the pandemic (including health and location data collected by contact-tracing apps), and require them to delete the data once

49 *A Renewed Call-to-Action*, Covid.joinzoe.com, https://covid.joinzoe.com/us.

50 Rob Mitchum, *Researchers to develop AI to help diagnose and Understand COVID-19 in lung damage*, UChicago News (May 6, 2020), https://news.uchicago.edu/story/researchers-develop-ai-help-diagnose-understand-covid-19-lung-images.

51 COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong. (2020).

52 Public Health Emergency Privacy Act, S. 3749, 116th Cong. (2020).

the crisis ends. Companies would be limited to collecting data for public health purposes, and prohibited from using health data for advertising, or to block access to employment, finance, housing or insurance. And not long after these duelling privacy proposals were introduced, the bipartisan Exposure Notification Privacy Act (ENPA) was introduced in the Senate, seeking to directly regulate contact tracing apps. It is simply too early to tell how consideration of these bills will unfold, but they demonstrate how the covid-19 pandemic may end up being an additional accelerant for further US privacy regulation.

ii Key federal government privacy and data protection actions

Over the past year, all three branches of the federal government have taken significant steps with respect to privacy and data protection, underscoring the current focus on these issues.

Executive branch – recent enforcement cases

The biggest news with respect to federal privacy regulation over the past year occurred on 24 July 2019, when the FTC announced that Facebook, Inc 'will pay a record-breaking US$5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy, to settle [FTC] charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information'.[53] This settlement exemplified the emerging new privacy zeitgeist – as the FTC noted, the US$5 billion penalty was the 'largest ever imposed on any company for violating consumers' privacy', 'almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide', and 'one of the largest penalties ever assessed by the US government for any violation'.[54]

The settlement followed on the heels of a year-long FTC investigation, which led to charges that Facebook 'repeatedly used deceptive disclosures and settings to undermine users' privacy preferences in violation of' a prior FTC consent order, which prohibited Facebook from 'making misrepresentations about the privacy or security of consumers' personal information, and the extent to which it shares personal information'. The FTC's press release further claimed that these allegedly deceptive 'tactics allowed the company to share users' personal information with third-party apps that were downloaded by the user's Facebook "friends"', and that 'Facebook took inadequate steps to deal with apps that it knew were violating its platform policies'.

In addition to the US$5 billion penalty, the FTC entered into a new 20-year settlement order with Facebook. This order was notable for how it required Facebook to put in place a new governance structure for managing privacy and data security issues. As the FTC noted, the settlement order 'overhauls the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance'.[55] In particular, governance aspects of the settlement order include:

a '[G]reater accountability at the board of directors level', including the establishment of an independent privacy committee of Facebook's board of directors, with an

53 Press Release, FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

54 id.

55 id.

independent nominating committee responsible for appointing the members of the privacy committee and a supermajority of the Facebook board of directors required to fire any of them.[56]

b Improved 'accountability at the individual level', including by requiring Facebook to 'designate compliance officers who will be responsible for Facebook's privacy program' and by requiring Facebook's CEO and the designated compliance officers independently 'to submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, as well as an annual certification that the company is in overall compliance with the order', with false certification subjecting them to individual civil and criminal penalties.[57]

c 'Strengthen[ed] external oversight of Facebook', by enhancing the 'independent third-party assessor's ability to evaluate the effectiveness of Facebook's privacy program and identify any gaps'.[58]

d Various additional privacy and data security requirements, including, among other things, the need to conduct and document privacy reviews of all new or modified products, services, or practices before they are implemented; additional privacy reporting and documentation requirements; a requirement to exercise greater oversight over third-party apps; a requirement to 'implement procedures designed to ensure that Covered Information entered by the User (such as User-generated content) is deleted from servers under [Facebook]'s control, or is de-identified such that it is no longer associated with the User's account or device, within a reasonable period of time (not to exceed 120 days) from the time that the User has deleted such information, or his or her account' subject to certain exceptions; and a requirement to 'establish, implement, and maintain a comprehensive data security program'.[59]

Moreover, the Facebook settlement was not the only record-setting FTC action of the past year. In September 2019, the FTC and New York's Attorney General announced a record-setting fine of US$170 million on Google and its subsidiary YouTube to settle allegations that they violated the Children's Online Privacy Protection Act (COPPA).[60] This is the largest civil penalty for violations of COPPA to date, exceeding the previous record US$5.7 million fine handed to TikTok's parent company in February 2019.[61] Of note, the FTC and New York Attorney General alleged that numerous YouTube channels were 'directed to children,' in part because they self-identified as being for children in the 'About' section of the channel webpages, and that, as such, YouTube did not put in place the protections COPPA requires on such sites. In addition to the historic fine, YouTube also agreed to take several remedial and risk mitigation steps to protect children's privacy on the site. Moreover, in June 2020,

56 id.

57 id.

58 id.

59 id.

60 Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *Federal Trade Commission, et al., v. Google LLC, et a*l., No. 1:19-cv-02642 (D.D.C. 2020).

61 Press Release, FTC, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law*, (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc; Proposed Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, *United States of America v. Musical.ly, et al.*, No. 2:19-cv-01439 (U.S. Dist. Ct. C.D. of Cal. 2019).

the FTC demonstrated its continued focus on children's privacy by fining an app developer, HyperBeard, under COPPA for allowing third-party advertisers to collect information from children using its app.[62]

The FTC was also not the only federal regulatory agency that had an active year. The SEC has been exercising increasingly aggressive oversight regarding cybersecurity compliance in recent years and the past year was no exception. Building on the SEC's 2018 issuance of new interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors,[63] the SEC's Office of Compliance Inspections and Examinations (OCIE) issued guidance in 2019 identifying the multiple steps it is taking to heighten its enforcement presence for cybersecurity matters.[64] In April and May 2019, the OCIE further issued two risk alerts providing regulated entities with details on its privacy and cybersecurity focus areas during examinations.[65] More recently, the SEC's OCIE and Financial Industry Regulatory Authority (FINRA) issued 2020 examination priorities for broker-dealers and investment advisers, which, among other priorities, included cyber and information security risks, issues concerning digital assets, and the provision of electronic investment advice.[66] Finally, earlier this year, the OCIE released a report on 'Cybersecurity and Resiliency Observations', providing an overview of best practices based on prior exams to help organisations when considering 'how to enhance cybersecurity preparedness and operational resiliency'.[67]

The SEC has also backed this guidance up with action on the enforcement front. For example, on 24 July 2019, the SEC joined the FTC in announcing a settlement with Facebook – in the SEC's case with Facebook agreeing to pay US$100 million to settle charges for 'making misleading disclosures regarding the risk of misuse' of 'user data'.[68]

62 Proposed Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *United States of America v. Hyperbeard, Inc., et al.*., No. 3:20-cv-3683 (U.S. Dist. Ct. N.D. of Cal. 2020).

63 The SEC suggested that all public companies adopt cyber disclosure controls and procedures that enable companies to: identify cybersecurity risks and incidents; assess and analyse their impact on a company's business; evaluate the significance associated with such risks and incidents; provide for open communications between technical experts and disclosure advisers; make timely disclosures regarding such risks and incidents; and, adopt internal policies to prevent insider trading while the company is investigating a suspected data breach.

64 SEC, *Office of Compliance Inspections and Examinations: 2019 Examination Priorities* (2019), https://www.sec.gov/files/OCIE%202019%20Priorities.pdf. The OCIE's 2019 Exam Priorities emphasise proper configuration of network storage devices, information security governance, and policies and procedures related to retail trading information security.

65 SEC, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies* (Apr. 16, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf; SEC, *Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features* (May 23, 2019), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf.

66 See OCIE, 2020 *Examination Priorities*, https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf; FINRA, *2020 Risk Monitoring and Examination Priorities Letter,* https://www.finra.org/sites/default/files/2020-01/2020-risk-monitoring-and-examination-priorities-letter.pdf.

67 SEC, *Office of Compliance Inspections and Examinations: Cybersecurity and Resiliency Observations*, https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

68 Press Release, SEC, *Facebook to Pay $100 Million for Misleading Investors About the Risks it Faced from Misuse of User Data*, (Jul. 24, 2019), https://www.sec.gov/news/press-release/2019-140.

Another financial regulator that has recently adopted a more aggressive enforcement posture with respect to cybersecurity matters is the Commodity Future Trading Commission (CFTC). On 12 September 2019, the CFTC issued an order filing and settling charges with Phillip Capital Inc, fining it US$1.5 million and finding that it had failed to supervise its employees with respect to its cybersecurity policies and procedures and had not provided timely notice to its customer about a cyber incident.[69]

The FTC's, SEC's, and CFTC's enforcement emphasis in this area exemplifies a broader executive branch focus on privacy and data protection issues. Indeed, numerous other federal agencies are actively engaged – often through their contacting requirements – such that businesses operating in the United States should consider casting a wide net when determining whether they are subject to privacy or cybersecurity regulation. For example, on 31 January 2020, the Department of Defense (DOD) released its latest version of the Cybersecurity Maturity Model Certification (CMMC) for defense contractors. Under the CMMC plan, DOD contractors will be required to obtain a cybersecurity rating from Level 1 through Level 5, and self-certification will not be permitted.[70] Similarly, on 5 March 2020, the Office of the Comptroller of the Currency (OCC) issued updated guidance regarding risk management in national bank relationships with third parties, elaborating on a wide range of topics, including the scope of third-party risk management obligations and oversight of cloud computing providers and data aggregators.[71]

Finally, in addition to promulgating policies regarding privacy or data security, federal regulators are also increasingly interested in studying and regulating digital innovation and artificial intelligence. The examples of this trend are numerous, with some of the highlights being the following:

a In August 2019, NIST released a draft guide with security feature recommendations for internet of things (IoT) devices.[72]

b In May 2020, the National Telecommunications and Information Administration (NTIA) published a notice seeking comments regarding the development of an implementation plan for the national strategy to secure 5G, a component of the 'Secure 5G and Beyond Act of 2020' that was signed into law on 23 March 2020.[73]

c In June 2020, FINRA issued its 2020 Artificial Intelligence Report for industry comment.[74] The report is a culmination of FINRA's Office of Financial Innovation review of emerging challenges and legal considerations confronted by the securities industry as broker-dealers introduce AI-based applications into their businesses.

69 Press Release, CFTC, *CFTC Orders Registrant to Pay $1.5 Million for Violations Related to Cyber Breach* (Sept. 12, 2019), https://www.cftc.gov/PressRoom/PressReleases/8008-19.

70 Office of the Undersecretary of Defense, *Cybersecurity Maturity Model Certification (CMMC)* (Jan. 31, 2020), https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf.

71 Office of the Comptroller of the Currency (OCC), *Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29* (March 5, 2020), *available at* https://www.occ.treas.gov/news-issuances/bulletins/2020/bulletin-2020-10.html.

72 NIST, *NIST Releases Draft Security Feature Recommendations for IoT Devices* (Aug. 1, 2019), nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices.

73 Meeting Notice, 85 Fed. Reg. 103 (May 28, 2020), https://www.ntia.doc.gov/files/ntia/publications/fr-secure-5g-implementation-plan-05282020.pdf.

74 Financial Industry Regulatory Authority (FINRA), *Artificial Intelligence (AI) in the Securities Industry* (June 2020), https://www.finra.org/sites/default/files/2020-06/ai-report-061020.pdf.

d The same month, the OCC sought comment – by issuing an Advance Notice of Proposed Rulemaking (ANPR) – on how best to accommodate new technology and digital innovation in the business of banking.[75]

Legislative branch

The popular focus on privacy and cybersecurity matters has prompted Congress to join the party. Multiple congressional committees – from the House and the Senate, chaired by Republicans and Democrats – have held high profile hearings on the possibility of enacting comprehensive federal privacy legislation, and both industry and civil society are urging Congress to act. There is also widespread support in Congress for action, especially (as discussed above) in light of the privacy implications of the covid-19 pandemic, such that federal privacy legislation is probably more likely now than it has been at any time in the past generation.

Despite the consensus that something needs to be done, however, the support at the time of writing appears to cleave between those who want to enact legislation that pre-empts state law such that US businesses are not subject to a patchwork quilt of privacy regulation and those who (mirroring civil society) want to allow states to provide additional privacy rights above a federal floor. The enactment of federal privacy legislation rests on the resolution of this debate, as well as agreement on the particulars of the regulatory scheme. It is possible that after the 2020 US presidential election, legislators may be in a better position to resolve these issues.

In addition to comprehensive privacy legislation, in the past year, Congress has also focused on several more targeted issues, such as facial recognition.[76] Indeed, the currency of this issue increased in the wake of civil unrest and protests regarding police reform, with some cities having banned the use of the technology and several companies calling on Congress to issue rules on the use of the technology and halting sales of facial recognition technology to US police.[77] Other recent issues that have attracted congressional attention – and led to proposed legislation – are encryption[78] and potential reforms to Section 230 of the Communications Decency Act, which shields tech companies that provide online platforms from civil liability stemming from third-party content.[79]

75 OCC, *National Bank and Federal Savings Association Digital Activities* (2019), https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76a.pdf.

76 *Facial Recognition Technology (Part I): Its Impact on our Civil Rights and Liberties*, House Committee on Oversight and Reform (May 22, 2019), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and; *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, House Committee on Oversight and Reform (June 4, 2019), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-ii-ensuring-transparency-in-government-use; *Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy,* House Committee on Oversight and Reform (Jan. 15, 2020), https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-iii-ensuring-commercial-transparency.

77 Tom Simonite, *A Bill in Congress Would Limit Uses of Facial Recognition*, Wired.com (June 12, 2020), https://www.wired.com/story/bill-congress-limit-uses-facial-recognition/.

78 S. 4051, 116th Cong. (2020).

79 PACT Act, S. 4066, 116th Cong. (2020). A competing proposal is Senator Hawley's Ending Support for Internet Censorship Act, which has been praised by President Trump. See Ending Support for Internet Censorship Act, S. 1914, 116th Cong. (2019).

Judicial branch, including key developments with discovery and disclosure

Finally, as they do every year, the federal courts decided a number of important cases relevant to privacy and data security. Indeed, while none of the cases were a blockbuster like the Supreme Court's 2018 decision in *Carpenter v. United States*,[80] which held that the Fourth Amendment protects an individual's historical cell-site locational information (CSLI), federal courts decided numerous cases with widespread relevance to businesses. Some of the highlights are detailed below.

On 8 August 2019, the Court of Appeals for the Ninth Circuit allowed a privacy-related class action litigation to move forward, when it held, among other things, that Facebook's alleged violations of the procedural requirements of the Illinois Biometric Information Privacy Act (discussed below) constituted a concrete and particularised harm sufficient to demonstrate standing.[81] The court cited *Carpenter* for the proposition that 'advances in technology can increase the potential for unreasonable intrusion into personal privacy' in holding that the Act protected the plaintiff's concrete interests in biometric privacy.[82] The court then held that violations of the Act's procedures – which require, among other things, establishing a retention schedule and guidelines for permanently destroying biometric information – actually harmed or materially risked harming those interests. This case thus demonstrates how plaintiffs may have more success establishing privacy harms sufficient to get into court when their allegations concern sensitive information gained via advanced technologies – a point further reinforced on 5 May 2020, when the Court of Appeals for the Seventh Circuit also held that allegations that a defendant violated the Illinois Biometric Information Privacy Act by collecting biometric information without first obtaining informed consent constituted an 'injury in fact' sufficient to confer Article III standing.[83]

Another important decision was handed down on 9 September 2019, when the Court of Appeals for the Ninth Circuit cast into doubt whether the Computer Fraud and Abuse Act (CFAA) – a US law that criminalises accessing a computer 'without authorisation' – protects website owners against third-party web scrapers if such scrapers are accessing public data. For years, companies seeking to block web scrapers from collecting the information on their website would routinely invoke CFAA. But the Ninth Circuit ruled that merely instructing scrapers that they were not welcome on a public website was likely not enough to render their access 'unauthorised' under the CFAA.[84]

Finally, and potentially most importantly, on 26 May 2020, the District Court for the Eastern District of Virginia issued a decision with potentially significant ramifications for businesses' data breach response efforts.[85] The question before the court was whether the attorney work product doctrine allowed Capital One to withhold from discovery a forensic report developed by a third-party investigator at the direction of counsel. Believing a substantially similar report would have been prepared regardless of whether the litigation followed, the court relied on several key facts to find that the report must be produced, including that Capital One executed a non-privileged statement of work for services with the

80 138 S. Ct. 2206 (2018).

81 *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424 (9th Cir. Aug. 8, 2019).

82 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

83 *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617 (7th Cir. 2020).

84 *hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-16783, slip op. at 26 (9th Cir. Sept. 9, 2019).

85 *In Re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (May 26, 2020).

third party prior to the data breach, the post-breach agreement included the same scope of work as the prior statement of work, and the forensic report was widely distributed to different regulators and Capital One's accountant, suggesting that it was not specifically created in anticipation of litigation. This opinion underscores the importance for organisations to consider, in advance, how to engage with incident response service providers in order to protect privilege in the event of a data breach litigation.

iii Key state privacy and data protection actions

While, as the above demonstrates, the federal government has been very active on privacy and data security matters over the past year, there is a very good case that the real action may not be in Washington DC, but rather in the 50 US states.

The California Consumer Privacy Act (CCPA)

Outside of the issues surrounding the covid-19 pandemic, the biggest recent privacy development in the United States has been the entry into force of the CCPA, a comprehensive privacy bill that commentators have taken to calling 'California's GDPR'. Given California's size and the fact that it is the home of Silicon Valley, the CCPA is having a wide impact, and companies across the United States and around the world are considering what it might mean for them.

Much as with the GDPR, the early days of the CCPA have brought regulatory uncertainty. Since the CCPA went into effect on 1 January 2020, the California Attorney General has proposed regulations implementing the Act, which only recently were finalised on 14 August 2020 as this chapter was being drafted. The Attorney General was also only able to begin enforcing the Act on 1 July 2020, so his enforcement priorities are not yet certain.

Despite this uncertainty, one thing that is clear is that, upon enactment, the CCPA immediately became the most far-reaching privacy or data protection law in the country. In short, the bill's nickname reflects reality, as the CCPA shares many attributes with the EU's General Data Protection Regulation (GDPR). And while a full discussion of the lengthy law is beyond the scope of this chapter, the law's highlights include the following:

a The CCPA applies to for-profit entities that are doing business in California; that collect or determine the means of processing personal information; and that meet one of three size thresholds.[86]

b The CCPA mandates broad privacy policy disclosure requirements on companies that collect personal data about California residents.[87]

c The CCPA mandates that businesses provide California residents with the rights to access and delete their personal information, as well as the right to stop the sale of their information to third parties.[88]

d The CCPA prohibits businesses from selling personal information of individuals under the age of 16, absent affirmative authorisation.[89]

e The CCPA mandates that businesses not treat consumers differently based on the exercise of their CCPA rights, although businesses are allowed to offer incentives.[90]

86 The California Consumer Privacy Act, A.B. 375, 2017 Gen Assemb., Reg. Sess. (Cal. 2018).

87 id. § 1798.140 (g).

88 id. § 1798.105 (a), 120 (a).

89 id. § 1798.120 (d).

90 id. § 1798.125 (a).

f The CCPA provides a private cause of action for certain data breaches that result from a business's violation of the duty to implement and maintain reasonable security procedures and practices.[91]

g The CCPA authorises the California Attorney General to enforce its provisions with statutory fines of up to US$7,500 per violation.[92]

Seeking to temper the CCPA's broad demands, the California legislature has created a number of exemptions from all or a substantial part of the law – most notably, employee information and B2B information. These exemptions are slated to expire, however, at the end of 2020.

As noted above, the California Attorney General, exercising authority explicitly granted to him by the Act, has proposed regulations providing further guidance on a number of the Act's obligations. In particular, among other things, the draft regulations provide guidance on required content for privacy policies, requirements for responding to data subject requests, and appropriate verification standards for requests.

Even though the proposed regulations only recently were finalised, the office of the California Attorney General began actively enforcing the CCPA on 1 July 2020, sending violation notice letters to a 'swath' of online businesses.[93] The Attorney General took this action notwithstanding the request of several industry groups and entities for enforcement to be delayed until January 2021 in light of the covid-19 crisis, and, as at the time of writing, it remains to be seen how the Attorney General will follow up on its initial letters, including how it will expect businesses to take advantage of the 30-day 'cure' period provided by the Act.

Moreover, the massive changes to California privacy law we have seen over the past couple of years may not be complete. Alastair Mactaggart, the consumer rights advocate who was the driving force behind the CCPA, has recently secured enough signatures to place the California Privacy Rights Act (CPRA), a proposed law that would significantly amend the CCPA (and sometimes referred to as 'CCPA 2.0') as an initiative on California's November 2020 ballot. If passed, the CPRA will modify the CCPA by, among other things, adding the right to correct inaccurate information and limit first-party use of sensitive personal information, clarifying the right to opt out of the sale or sharing of data for purposes of online behavioural advertising, and extending the employee data and business-to-business data exemptions through 2022.

Other state laws

California has long been a privacy bellwether, as its legislative actions have often prompted other states to follow suit: for example, California was the first state to enact a data breach notification law, and all 50 states now have one. It is thus unsurprising that the passage of the CCPA has prompted numerous other states to consider comprehensive privacy legislation. And while these legislative initiatives fizzled out in some places, the past year has seen the enactment of a number of new data protection laws in the CCPA's wake:

91 id. § 1798.140 (w)(2)(B).

92 id. § 1798.155 (b).

93 Stacey Gray, *Off to the Races for Enforcement of California's Privacy Law*, Future of Privacy Forum (July 10, 2020), https://fpf.org/2020/07/10/off-to-the-races-for-enforcement-of-californias-privacy-law/.

a Nevada became the first state to follow the CCPA trend when, on 29 May 2019, it enacted a law that grants consumers the right to 'opt out' of the sale of personal information. While Nevada's law is not as comprehensive as the CCPA, it entered into force earlier on 1 October 2019.[94]

b Maine was the second state to follow California's footsteps, with the Governor signing into law the 'Act to Protect the Privacy of Online Consumer Information' on 6 June 2019, which officially went into effect on 1 July 2020 (although Maine's Attorney General agreed to delay enforcement until 1 August 2020 due to covid-19).[95] Again, this law is not as comprehensive as the CCPA, but it does obligate internet service providers in Maine to obtain permission from their customers before selling or sharing their data with a third party.

c On 25 July 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act),[96] updating New York's breach reporting law by, among other things, requiring entities that handle private information to implement a data security programme with 'reasonable' administrative, technical and physical safeguards. The Act's reasonable security requirement went into effect on 21 March 2020. While this law is again narrower than the CCPA, it is notable for detailing what constitutes 'reasonable security', laying out with some specificity examples of 'reasonable' safeguards. The SHIELD Act also makes clear that entities in compliance with data security frameworks under certain federal or state laws (such as GLBA and HIPAA) are in compliance with the SHIELD Act. In this regard, the Act mirrors a 2018 Ohio law, which did not establish minimum cybersecurity standards but which did provide companies with a safe harbour for tort liability in data breach actions when they put in place 'administrative, technical, and physical safeguards for the protection of personal information and that reasonably confor[m] to an industry recognised cybersecurity framework'.

d Finally, as happens most years, a number of states have also passed amendments to their data breach notification laws or had such amendments enter into force, offering another reminder of the fact that businesses must continually try to stay on top of the various state law requirements in this area.[97]

Besides taking the lead on enacting broad, cross-sectoral privacy and data security legislation and updating their data breach notification laws, states are also taking the lead in putting in place other, more focused regulatory regimes. We have discussed some examples of this, such as the New York Department of Financial Services' Cybersecurity Regulation, above, but there are many others. For instance, South Carolina passed a law putting in place prescriptive data security requirements for insurers that went into effect on 1 January 2019,[98] and other states have followed suit, enacting requirements that generally track the Insurance Data Security Model Law adopted by the National Association of Insurance Commissioners (NAIC).

94 S.B. 220, 80th Leg., Reg. Sess. (Nev. 2019).

95 S.P. 275, 129th Leg., Reg. Sess. (Me. 2019).

96 S.B. 5775, Reg. Sess. 2019-2020 (N.Y. 2019).

97 H.B. 1071, 66th Leg., Reg. Sess. (Wash. 2019); H.B. 4390, 86th Leg., Reg. Sess. (Tex. 2019); S.B. 1624, 101st Leg., Reg. Sess. (Ill. 2019); S.B. 684, 80th Leg., Reg. Sess. (Or. 2019); S.B. 52, 208th Leg., Reg. Sess. (N.J. 2018); L.D. 696, 129th Leg., Reg. Sess. (Me. 2019); H.B. 1943, 92nd Leg., Reg. Sess. (Ark 2019); H.B. 1154, Leg. Reg. Sess. (Md. 2019).

98 S.B. 6280, Leg., Reg. Sess. (Wash. 2020).

States are also taking the lead in regulating emerging technologies, with a prime example of this being facial recognition technologies. On 31 March 2020, the Governor of Washington state signed into law S.B. 6280, a bill aimed at regulating state and local government agencies' use of facial recognition services.[99] The law contains safeguards that ensure testing, transparency, and accountability for the uses of facial recognition technology and includes various measures to uphold fundamental civil liberties. Several other states, including Arizona, Illinois, Massachusetts, New Hampshire, and Vermont, are also considering such legislation to curtail the use of facial recognition by government entities. Additionally, Texas, Washington, and Illinois have already enacted statutes governing biometric data directly, many other states indirectly regulate biometric data by including it in their statutory definitions of personal information, and several other states, including Connecticut, New Hampshire and Alaska, have considered or proposed legislation seeking to regulate biometric data. These laws – which generally require notice and opt-out, limitations on the commercial use of acquired biometric data, destruction of the data after a certain amount of time, and employment of industry standards of care to protect the data – will likely continue to be an area of focus going forward.

State courts

Just as the federal courts have decided a number of recent important privacy and data security cases, so too have state courts. While a complete canvas of all of these decisions is beyond the scope of this chapter, highlighting a couple of examples serves to demonstrate the general point.

First, the Illinois Biometric Information Privacy Act (BIPA) provides a private right of action for aggrieved individuals, and, much like the Ninth Circuit, the Illinois Supreme Court has held that bare procedural violations of the statute are sufficient to establish standing.[100] A wide range of technology companies, including Facebook, Shutterfly, Snapchat and Google, are finding themselves defending their implementation of facial recognition technology against BIPA claims in Illinois courts.

Second, on 31 May 2019, a trial court in the District of Columbia held that the District of Columbia's attorney general could challenge Facebook's privacy practices. In doing so, the court rejected Facebook's arguments that the court lacked jurisdiction over the California-based company and that the attorney general had failed to adequately plead his claims that the company ran afoul of the district's Consumer Protection Procedures Act.[101]

These cases, in short, demonstrate the risks companies face as courts also respond to the shifting privacy zeitgeist.

iv Companies expand oversight of privacy and data security issues

In light of the legal and regulatory trends at the federal and state level identified above – to say nothing of international trends discussed elsewhere in the book – companies are increasingly recognising the importance of showing that they have in place structures to ensure sufficient management and board oversight of privacy, data protection, and disruptive technologies.

99 S.B. 6280, Leg., Reg. Sess. (Wash. 2020).

100 740 Ill. Comp. Stat. § 14/1 – 99 (2008); *Rosenbach v. Six Flags Ent. Corp.*, No. 123186, 2019 IL 123186 (Jan. 25, 2019).

101 *District of Columbia v. Facebook Inc.*, 2018 CA 008715B (D.C. Super. Ct., Civ. Div. (Wash.)).

This is a trend that has been building over time. In recent years, it has become best practice to appoint a chief privacy officer and an IT security officer, to put in place an incident response plan and vendor controls (which may be required by some state laws and in some sectors by federal law), and to provide regular employee training regarding data security. However, as technology advances and companies increasingly view information as a significant strategic opportunity and risk, companies are increasingly sensing that these structures, policies, and procedures are insufficient.

Indeed, while not so long ago companies were comfortable with IT and legal departments running the show with respect to privacy issues, they are now increasingly elevating the level of attention these issues receive and involving senior management and the board in oversight and decision making. The examples of this are legion, and here are just a few:

a Microsoft has created a technology and corporate responsibility team that reports to the president and provides guidance to the board and management on ethical business practices, privacy and cybersecurity.[102]

b Microsoft and other companies have put in place internal boards to help oversee and navigate the challenging moral, ethical, and practical issues raised by artificial intelligence.[103]

c Numerous companies, including Walmart, BNY Mellon, and AIG, have put in place technology committees of their board, with responsibility to, among other things, review IT planning, strategy, and investment; monitor and provide guidance on technological trends; and review cybersecurity planning and investment.[104]

In short, companies have recognised the changing zeitgeist, and they are increasingly taking steps to create an effective organisational structure and practices to manage, guide, and oversee privacy, data protection, and disruptive technologies.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The changing privacy zeitgeist has altered not only the privacy and data protection regime within the United States, but it also threatens to change how the United States approaches certain transfers of information between the United States and other countries.

There are no significant or generally applicable data transfer restrictions in the United States. That said, the United States has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by other countries. In

102 *We see the big picture*, Microsoft Corp. (August 23, 2019), https://www.microsoft.com/en-us/corporate-responsibility/governance.

103 *AI news and events*, Microsoft Corp. (August 23, 2019), https://www.microsoft.com/en-us/ai?activetab=pivot1%3aprimaryr5; *SAP Becomes First European Tech Company to Create Ethics Advisory Panel for Artificial Intelligence*, SAP News (Sept. 18, 2018), https://news.sap.com/2018/09/sap-first-european-tech-company-ai-ethics-advisory-panel/.

104 Walmart Inc., *Technology and Ecommerce Committee Charter* (adopted Jun. 2, 2011), https://s2.q4cdn.com/056532643/files/doc_downloads/Gov_Docs/TeCC-Charter[1].pdf; BNY Mellon, *Technology Committee: Charter of the Technology Committee of the Board of Directors, The Bank of New York Mellon Corporation* (approved Apr. 9, 2019), https://www.bnymellon.com/us/en/who-we-are/corporate-governance/technology-committee.jsp, American International Group, Inc., Technology Committee Charter (effective May 9, 2018), https://www.aig.com/content/dam/aig/america-canada/us/documents/corp-governance/technology-committee-charter-05.09.18.pdf.

particular, the United States was approved in 2012 as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC's Office of International Affairs further works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[105]

Significantly, however, as this chapter was being drafted, on 16 July 2020, the Court of Justice for the European Union (CJEU) decided *Data Protection Commissioner v. Facebook Ireland, Max Schrems (Schrems II)*, which held that the EU–US Privacy Shield – a transfer mechanism used by over 5,000 organisations as a mechanism enabling transfers of personal data from the EU to the US – was invalid because the privacy protections afforded to individuals under the Privacy Shield programme were not 'essentially equivalent' to privacy rights afforded to such individuals under EU law.[106] The court also potentially required additional protections to be implemented for another key transfer mechanism, called Standard Contractual Clauses (SCCs), requiring organisations to further evaluate and implement supplementary measures to provide additional privacy protections that afford an individual privacy protections that are 'essentially equivalent' to those under EU law.

At the time of writing, the long-term implications of *Schrems II* are unclear. Regulators on both sides of the Atlantic have preached calm, and guidance from European Data Protection Board is expected soon. The US government and the EU Commission have also committed to work cooperatively together to address the consequences of the *Schrems II* decision and announced their intention to develop a successor programme to the Privacy Shield. Nonetheless, while the Privacy Shield and SCCs are not the only approved legal transfer mechanisms under the GDPR, they are the most widely-used, and as result, a key facilitator of international trade and cross-border data flows. In light of the CJEU's ruling, at the very least, organisations relying on their Privacy Shield certification will be required to implement an appropriate alternate legal transfer mechanism (for example, enhanced SCCs, Binding Corporate Rules, or rely on informed consent or other exemptions under the GDPR) and organisations relying on SCCs will have to assess whether their use of such clauses is consistent with *Schrems II* and whether they need to put in place additional protections. In the meantime, the Commerce Department has stated that US companies with the Privacy Shield certification must continue to comply with the requirements even though they have been invalidated by the EU.[107] As such, the FTC can continue to enforce against certified companies that do not live up to their commitments.

Another cross-border issue that has experienced recent activity is law enforcement access to extraterritorial data. Historically, the mutual legal assistance treaty (MLAT) system has governed cross-border transfers of data for law enforcement purposes. In recent years, however, the rise of cloud computing has led to more and more data being stored somewhere other than the jurisdiction in which it was created, placing strain on the system as the

105 See FTC, *Office of International Affairs*, www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs. See also FTC, *International Consumer Protection*, www.ftc.gov/policy/international/international-consumer-protection.

106 Court of Justice of the European Union Press Release 91/20, *The Court of Justice invalidates Decisions 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield* (July 16, 2020), https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf; see also InfoCuria Case-law, http://curia.europa.eu/juris/documents.jsf?num=C-311/18.

107 Press Release, U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

antiquated MLAT process was insufficiently nimble to keep up with the increased demand. Other countries therefore became increasingly concerned about their inability to obtain timely evidence, as US technology companies frequently held the relevant information but were barred by US law from turning it over to foreign governments without going through the MLAT process.

These issues came to a head in 2018 when the Supreme Court heard a case concerning whether a search warrant served in the United States could authorise the extraterritorial transfer of customer communications notwithstanding the laws of Ireland. US companies were thus faced with being placed in the middle of a second conflict of law – not only would they be forbidden from turning over information to foreign governments without a formal MLAT request, but they would also have to turn over information to the US government even absent an MLAT request.

Given the prospect of US industry facing this twin dilemma, as well as the desire of foreign governments to address the concerns caused by the current operation of the MLAT process, Congress enacted the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act).[108] The CLOUD Act was designed to serve two purposes. First, it clarified that a US search warrant could compel companies to disclose certain communications and records stored overseas, thereby mooting the case before the Supreme Court. Second, the CLOUD Act addressed the converse issue – foreign government access to information held in the United States – by authorising the executive branch to enter into international agreements that would allow for certain foreign nations to obtain content directly from US companies without going through the MLAT process.

At the time of writing, the United States has entered into only one CLOUD Act agreement that would facilitate foreign government access to communication held within the United States. On 3 October 2019, the United States and United Kingdom signed the CLOUD Act agreement, which entered into force on 8 July 2020. The Agreement obligates each government to ensure their domestic laws permit US and UK national security and law enforcement agencies to directly obtain certain electronic information from 'Covered Providers' in the jurisdiction of the other government.[109]

Beyond this one agreement, the CLOUD Act's clarification of the extraterritorial reach of US law enforcement process has caused consternation, as companies that store data outside the United States have been pressed by non-US customers and counterparts to explain whether the CLOUD Act creates new risk that their data may now be within reach of the US government. The US Department of Justice has thus recently taken steps to explain that, in its view, the CLOUD Act broke no new ground and only clarified, rather than expanded, the reach of US law enforcement; and that, in any event, the requirements in the United States for obtaining a warrant for the content of electronic communications are perhaps the toughest in the world and are highly protective of individual privacy.[110]

108 Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. §§ 2523, 2713 (2018).

109 See Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (Oct. 2019), *available at*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

110 Press Release, U.S. Dep't of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (April 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

Thus, it is safe to say that it is still too soon to tell what the impact of the CLOUD Act will be. That said, the CLOUD Act is clearly yet another example of how US lawmakers and regulators are trying to redesign the regulatory structures governing the data economy.

V CONSIDERATIONS FOR FOREIGN ORGANISATIONS AND OUTLOOK

Foreign organisations can face federal or state regulatory or private action if they satisfy normal jurisdictional requirements under US law, which typically require minimum contacts with or presence in the United States. Additionally, a foreign organisation could be subject to sector-specific laws if the organisation satisfies that law's trigger. For example, if a foreign organisation engages in interstate commerce in the United States, the FTC has jurisdiction, and if a foreign organisation is a publicly traded company, the SEC has jurisdiction. Moreover, US law enforcement and other enforcement agencies have broad ideas about their jurisdiction.[111]

For all these reasons, US law can have a dramatic impact on foreign organisations. And, as a result, we live in interesting times. As detailed above, the US law concerning privacy and data security is quite dynamic, with both federal and state lawmakers and regulators actively considering potentially dramatic new laws and regulations. Foreign organisations are thus recommended to keep careful tabs on US developments, as the requirements may change at any moment.

111 The United States does not have any jurisdictional issues for multinational organisations related to cloud computing, human resources and internal investigations. However, foreign organisations subject to US law should carefully consider how their data network is structured, and ensure they can efficiently respond to international data transfer needs, including for legal process. Companies should also consider possible international data transfer conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to non-US data, such that non-US data could be considered within the company's lawful control in the United States and thereby subject to production requests irrespective of foreign blocking statutes. The United States respects comity, but a foreign country's blocking statute does not trump a US legal requirement to produce information.

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.

SNEZHANA STADNIK TAPIA

Sidley Austin LLP

Snezhana Stadnik Tapia is an associate in Sidley Austin's privacy and cybersecurity practice, where she assists clients with privacy and cybersecurity issues. Snezhana received her law degree from New York University School of Law, where she was an online editor for the *Journal of International Law and Politics*. During law school, Snezhana explored transnational legal and regulatory issues with respect to global digital technologies as a research assistant and worked on data governance and privacy issues at an urban innovation tech company.

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
sstadnik@sidley.com
www.sidley.com

an LBR business

ISBN 978-1-83862-485-9