THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SIXTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Sixth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2019
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
Tommy Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Charlotte Stretch

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC2A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-062-2

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

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ALLENS

ANJIE LAW FIRM

ASTREA

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP. J.

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

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 26

UNITED STATES

Alan Charles Raul, Christopher C Fonzone 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 and Christopher C Fonzone are partners, and Snezhana Stadnik Tapia is an associate, at Sidley Austin LLP. The authors wish to thank Vivek K Mohan, Tasha D Manoranjan and Frances E Faircloth, who were previously associates at Sidley, for their contributions to this chapter and prior versions. 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. And 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 created a 'crisis of new technologies' or 'techlash' that is shifting popular views about privacy in the United States. Once again, it seems, the United States will be undergoing 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 US privacy regulation that appears to be underway.

How all three branches of the federal US government are actively taking steps to confront the privacy and cybersecurity questions of the day – for example, how the Congress, for the first time in a generation, is seriously considering comprehensive federal privacy legislation; how the Supreme Court is extending constitutional rights to digital data held by third parties; and how the executive branch is taking numerous steps to better secure our networks and ensure companies are respecting their users' privacy.

How the real action may not be in Washington DC, but rather in the 50 US states – as California has recently enacted a far-reaching comprehensive privacy bill called 'California's GDPR', and numerous other states either have enacted or are considering substantial new privacy legislation.

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 concludes by detailing some 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 it 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 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. 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.[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, 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 Section 5 authority, as laid out above, remains the closest thing to a general national-level cybersecurity regulator.

---

7 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.

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

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.

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

Financial information

The Financial Services Modernisation Act of 1999, more commonly known as 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

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).

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)).

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 for smaller banks, while the FTC (for non-bank financial institutions) and the Consumer Financial Protection Bureau (CFPB) (for larger 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 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

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)).

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.

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, to safeguard PHI, 'business associates' are required to enter into agreements, called business associate agreements. 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 entities covered by the statute (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.

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:

18 45 C.F.R. § 160.103.

19 45 C.F.R. § 164.504(f)(3)(iii).

20 45 C.F.R. § 164.103.

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

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.

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

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

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)).

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 new and highly significant California Consumer Privacy Act of 2018.)

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 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 (discussed below) contains security requirements, and New York has recently enacted a preliminary set of general safeguards, to say nothing of the section-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.

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.

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).

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 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

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.

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. 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 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

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.

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.

consumer class action litigation. Indeed, the wave of lawsuits that a company faces after being accused in the media of misusing consumer data, being victimised by a hacker, or suffering a data breach incident is well known across the country.

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 companies might face. 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 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.

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

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

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.

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. The United States is 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 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 $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'.[46] 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'.[47]

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

46 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.

47 Id.

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'.[48] In particular, governance aspects of the settlement order include 'greater accountability at the board of directors level,' including the establishment of an independent privacy committee of Facebook's board of directors, with an 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.[49]

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.[50] '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'.[51]

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'.[52]

Moreover, the Facebook settlement was not the only record-setting FTC action of the past year. On 27 February 2019, the FTC announced a US$5.7 million civil penalty against makers of the popular free video creation and sharing app, Musical.ly (also now known as TikTok), for violations of COPPA. To date, this is the largest civil penalty the FTC has issued concerning violations of COPPA.[53] The FTC based the penalty on a complaint that alleged that Musical.ly failed to provide appropriate notice and obtain parental consent before collecting information directly from children, despite the fact that Musical.ly not only operated a site that was 'directed to children' under COPPA but also had 'actual knowledge'

48 Id.

49 Id.

50 Id.

51 Id.

52 Id.

53 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).

of underage use, due to company practices such as collecting users' dates of birth and grades via their profiles and complaints received from parents who unsuccessfully sought to have their children's information deleted.

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,[54] 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.[55] The OCIE further issued two risk alerts in April and May 2019 to provide details regarding specific privacy and cybersecurity issues that regulated entities should focus on to prepare for examinations.[56]

The SEC was also active on the enforcement front. In April 2018, the SEC announced that Altaba Inc (formerly, Yahoo!) had settled cybersecurity allegations brought by the SEC (for US$35 million) in the Commission's first-ever enforcement action against a company for failing to disclose a breach.[57] (Altaba also settled claims with shareholders for US$80 million.) Not long after, the SEC brought an enforcement action against an investment adviser, Voya Financial Inc, for alleged failure to maintain cybersecurity policies and procedures. And, finally, 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 settle charges for 'making misleading disclosures regarding the risk of misuse' of 'user data'.[58]

The FTC's and SEC's increased enforcement emphasis in this area exemplifies the executive branch's broader focus on privacy and data protection issues. The White House has remained engaged, with the President issuing an executive order on 'America's Cybersecurity Workforce', which aimed to close America's cyber workforce gap.[59] The same month, another executive order declared a 'national emergency' related to certain threats against information

54 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.

55 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.

56 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.

57 Press Release, SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million, (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

58 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.

59 Exec. Order No. 13800, 82 F.R. 22391 (2017).

and communications technology and services in the United States. It authorised the Department of Commerce to block transactions that involve such services with a 'foreign adversary'.[60]

In September 2018, the Trump administration, through the US Department of Commerce's National Telecommunications and Information Administration, also initiated a process to modernise US privacy policy by requesting comments on a series of privacy principles. The approach laid out in this request signalled a desire to move away from notice-and-comment based approaches to 'refocus' on achieving desirable privacy 'outcomes', such as ensuring that users are 'reasonably informed' and can 'meaningfully express' their privacy preferences, while providing organisations with the flexibility to continue innovating with cutting-edge business models and technologies.[61]

Finally, numerous other federal agencies remain actively engaged, such that businesses operating in the United States should consider whether they would be affected by policies promulgated by a non-traditional privacy or data security regulator. For example, the Department of Homeland Security (DHS) released a 2018 Cybersecurity Strategy and opened a new cyberrisk centre where industry and government can cooperate to evaluate and combat cyberthreats, as well as defend critical US infrastructure.[62] Additionally, in May 2018, the DHS and DOE released a final joint assessment of US incident response capabilities with respect to electricity disruptions in response to President Trump's executive order 13800 on 'Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure'.[63] In March 2019, the DOE further announced funding of up to US$70 million for an institute for advancing cybersecurity in energy efficient manufacturing.[64]

Legislative branch

Unsurprisingly, the popular focus on 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 federal privacy legislation, and both industry and civil society are urging Congress to act. There is also widespread support in the Congress for action, 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 (mirroring industry) want to enact legislation that pre-empts state law such that US businesses are not subject to a patchwork quilt of

60 Exec. Order No. 13873, 84 F.R. 22689 (2019).

61 Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018).

62 Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts, U.S. Dep't of Homeland Security (May 15, 2018), https://www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts; U.S. Dep't of Homeland Security, U.S. Department Of Homeland Security Cybersecurity Strategy (2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

63 U.S. Dep't of Homeland Security, Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities (May 28, 2019), https://www.dhs.gov/publication/section-2e-assessment-electricity-disruption-incident-response-capabilities.

64 DOE Announces $70 Million for Cybersecurity Institute for Energy Efficient Manufacturing, Dept. of Energy (Mar. 26, 2019), https://www.energy.gov/articles/doe-announces-70-million-cybersecurity-institute-energy-efficient-manufacturing.

privacy regulation and those who 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.

Judicial branch, including key developments with discovery and disclosure

Finally, the federal courts have also recently decided a number of important cases relevant to privacy and data security, further demonstrating the relevance of the topic.

Of particular note, although it does not directly address commercial data practices, is the Supreme Court's decision in *Carpenter v. United States*.[65] *Carpenter* held that the Fourth Amendment protects an individual's historical cell-site locational information (CSLI), even when the information is in the hands of the phone company. This case could have dramatic implications, as, prior to *Carpenter*, the common understanding was that the Fourth Amendment did not protect information provided to another. By potentially limiting this 'third-party doctrine', the Court recognised that the information age has placed an extraordinary amount of potentially sensitive information in the hands of others, requiring a rethink of foundational doctrinal principles. Thus, while the *Carpenter* Court went out of its way to say that its decision was narrow, limited to CSLI, and did not call into question traditional applications of the third-party doctrine (e.g., to bank and telephone records), the decision nonetheless provides yet another example of how privacy regulation is starting to adapt in face of the recognition of the consequences wrought by new technologies.

The federal courts have also delivered this same message in cases more directly relevant to companies. For example, in January 2019, a federal court in Georgia allowed consumers, payment card issuers, and investors to proceed with class action claims against Equifax for its 2017 data breach. Importantly, the court ruled that the consumer plaintiffs had suffered sufficiently actual and concrete injuries to demonstrate standing, and that the investors had pleaded enough specific factual allegations beyond the mere existence of the data breach to demonstrate (if the allegations were proven true) that Equifax's cybersecurity was 'grossly deficient' and that Equifax's statements regarding its cybersecurity preparedness were thus at least misleading.[66] (Ultimately, Equifax reached a global settlement whereby it paid US$1.4 billion to resolve the outstanding class action and regulatory claims against it.)[67]

Similarly, on 8 August 2019, the Court of Appeals for the Ninth Circuit also 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 Privacy Act (discussed below) constituted a concrete and particularised harm sufficient to demonstrate standing.[68] 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.[69] 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 –

65 138 S. Ct. 2206 (2018).

66 *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019).

67 Equifax Reaches $1.4B Data Breach Settlement in Consumer Class Action, Law.Com (July 22, 2019), https://www.law.com/2019/07/22/equifax-reaches-1-4-billion-data-breach-settlement-in-consumer-class-action/.

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

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

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.

Finally, the recent settlement of another case further demonstrates the new ways in which companies may face privacy and data security-related liability. On 31 July 2019, Cisco announced that it had paid US$8.6 million to settle a long-running False Claims Act suit in which the plaintiffs alleged that Cisco had knowingly sold vulnerable video surveillance systems to federal and state governmental entities in violation of contractual requirements to provide information protection.[70] This settlement, which has been termed the first time a company has faced cybersecurity-related liability under the False Claims Act, was reached despite the fact that Cisco claimed 'there is no evidence that any customer's security was ever breached'.[71]

ii 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)

The biggest recent privacy development in the United States – by far – has been California's enactment 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.

The CCPA will enter go into effect on 1 January 2020, and will immediately become the most far-reaching privacy or data protection law in the country. In short, the bill's nickname reflects reality, as CCPA shares many attributes with the EU's General Data Protection Regulation (GDPR). And while a full discussion of the lengthy bill is beyond the scope of this chapter, the bill'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.[72]

b The CCPA mandates broad privacy policy disclosure requirements on companies that collect personal data about California residents.[73]

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.[74]

70 Mike Lasusa, Cisco Inks $8.6M Deal To End Surveillance-Tech FCA Claims, Law360 (Jul 31, 2019, 10:31 PM), https://www.law360.com/articles/1184196/cisco-inks-8-6m-deal-to-end-surveillance-tech-fca-claims.

71 Mark Chandler, A Changed Environment Requires a Changed Approach, Cisco: Cisco Blogs (Jul. 31, 2019), https://blogs.cisco.com/news/a-changed-environment-requires-a-changed-approach.

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

73 Id. § 1798.140 (g).

74 Id. § 1798.105 (a), 120 (a).

d The CCPA prohibits businesses from selling personal information of individuals under the age of 16, absent affirmative authorisation.[75]

e The CCPA mandates that businesses not treat consumers differently based on the customers' exercise of their CCPA rights, although businesses are allowed to offer incentives.[76]

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.[77]

g The CCPA authorises the California Attorney General to enforce its provisions with statutory fines of up to US$7,500 per violation.[78]

h The CCPA was passed very quickly, and the California legislature has already amended it, with more amendments anticipated. The California Attorney General is also required to provide regulatory guidance on the meaning of many of the Act's provisions. The specific requirements of the CCPA are thus not set in stone, although, as of this writing, businesses are engaged in substantial efforts to prepare for its entry into force.

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 laws in the CCPA's wake.

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 will enter into force earlier – on 1 October 2019.[79]

Maine was the second state to follow in California's footsteps, with the Governor signing into law the Act to Protect the Privacy of Online Consumer Information on 6 June 2019.[80] 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.

Finally, on 25 July 2019, New York enacted the Stop Hacks and Improve Electronic Data Security Act (the SHIELD Act),[81] which updates 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. 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

75 Id. § 1798.120 (d).

76 Id. § 1798.125 (a).

77 Id. § 1798.140 (w)(2)(B).

78 Id. § 1798.155 (b).

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

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

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

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'.

Besides taking the lead on enacting broad, cross-sectoral privacy and data security legislation, 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,[82] 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).

States are also taking the lead in regulating emerging technologies, such as autonomous vehicles. A prime example of this is facial recognition technologies. 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.[83] A wide range of technology companies, including Facebook, Shutterfly, Snapchat and Google, thus 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.[84]

82 H.R. 4655, 122nd Reg. Sess. (S.C. 2018).

83 740 Ill. Comp. Stat. § 14/1 – 99 (2008); *Rosenbach v. Six Flags Ent. Corp.,* No. 123186, 2019 IL 123186 (Jan. 25, 2019).

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

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

iii 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.

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.[85]

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.[86]

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.[87]

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.

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

86 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/.

87 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.

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.

What has not changed is that 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 particular, the EU–US Privacy Shield continues to provide a framework for transatlantic data transfers, and the United States was approved in 2012 as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system. 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.[88]

The cross-border issue that has seen more 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 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 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).[89] 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 still not entered into any CLOUD Act agreements that would facilitate foreign government access to communication held within the United States. Moreover, the CLOUD Act's clarification of the extraterritorial reach of

88 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.

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

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.[90]

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.[91]

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.

90 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.

91 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.

CHRISTOPHER C FONZONE

Sidley Austin LLP

Christopher C Fonzone is a partner in Sidley Austin's privacy and cybersecurity group. His practice focuses on a wide range of issues related to information technology and cybersecurity, as well as the management of crisis situations. Before joining Sidley, Chris was deputy assistant and deputy counsel to President Obama and the legal adviser to the National Security Council. Before that, Chris worked at the Departments of Defense and Justice and as a law clerk to Justice Stephen Breyer of the US Supreme Court and Judge J Harvie Wilkinson III of the US Court of Appeals for the Fourth Circuit. Chris has lectured and taught classes at a variety of law schools, and his writing on national security and privacy and cybersecurity topics has been published in many forums, including the *Washington Post*, *The Hill*, *Newsweek*, *Lawfare* and *Just Security*.

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
cfonzone@sidley.com
sstadnik@sidley.comsnezhana
www.sidley.com

an LBR business

ISBN 978-1-83862-062-2