THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
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 MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

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

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 26

UNITED STATES

Alan Charles Raul and Vivek K Mohan[1]

I OVERVIEW

Although not universally acknowledged, the US commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The US privacy system has a relatively flexible and non-prescriptive nature, relying more on *post hoc* government enforcement and private litigation, and on the corresponding deterrent value of such enforcement and litigation, than on detailed prohibitions and rules. With certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin a party from, 'unfair or deceptive' business practices. However, US federal law does impose affirmative prohibitions and restrictions in certain commercial sectors, such as those involving financial and medical data, and electronic communications, as well as with respect to children's privacy, background investigations and 'consumer reports' for credit or employment purposes, and certain other specific areas. State laws add numerous additional privacy requirements.

Legal protection of privacy in civil society has been recognised in US common law since 1890, when the article 'The Right to Privacy' was published in the *Harvard Law Review* by Professors Samuel D Warren and Louis D Brandeis. Moreover, from its conception by Warren and Brandeis, the US system for protecting privacy in the commercial realm has been focused on addressing technological innovation. The Harvard professors astutely noted that '[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual [. . .] the right "to be let alone"'. In 1974, Congress enacted the federal Privacy Act, regulating government databases, and found that 'the right to privacy is a personal and fundamental right protected by the Constitution of the United States'. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices that have been incorporated in many other data protection regimes, including the European Union's 1995 Data Protection Directive.

---

1 Alan Charles Raul is a partner at Sidley Austin LLP. Vivek K Mohan was previously an associate and is now senior privacy and cybersecurity counsel at Apple Inc. His work on the chapter predated his tenure at Apple. The authors wish to thank 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.

The United States has also led the way for the world not only in establishing model legal data protection standards in the 1974 Privacy Act, but also in terms of imposing affirmative data breach notification and information security requirements on private entities that collect or process personal data from consumers, employees and other individuals. The state of California was the path-breaker on data security and data breach notifications by first requiring in 2003 that companies notify individuals whose personal information was compromised or improperly acquired. Since then, all 50 states,[2] the District of Columbia and other US jurisdictions, and the federal banking, healthcare and communications agencies, have also required companies to provide mandatory data breach notifications to affected individuals, and have imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information. Dozens of other medical and financial privacy laws also exist in various states. There is, however, no single omnibus federal privacy law in the United States. Moreover, there is no designated central data protection authority in the United States, although the Federal Trade Commission (FTC) has primarily assumed that role for consumer privacy. The FTC is independent of the President, and is not obliged (although it is encouraged) to respect the Administration's perspective on the proper balance between costs and benefits with respect to protecting data privacy. The Chair of the FTC is designated by the President, however, and may be removed as Chair (although not as one of the FTC's five commissioners) at the discretion of the President.

As in the EU and elsewhere, privacy and data protection are balanced in the United States in accordance with other rights and interests that societies need to prosper and flourish, namely economic growth and efficiency, technological innovation, property and free speech rights and, of course, the values of promoting human dignity and personal autonomy. The most significant factor in counterbalancing privacy protections in the United States, perhaps, is the right to freedom of expression guaranteed by the First Amendment. Preserving free speech rights for everyone certainly entails complications for a 'right to be forgotten', since one person's desire for oblivion may run counter to another's sense of nostalgia (or some other desire to memorialise the past for good or ill).

The First Amendment has also been interpreted to protect people's right to know information of public concern or interest, even if it trenches to some extent on individual privacy. Companies have also been deemed to have a First Amendment right to communicate relatively freely with their customers by exchanging information in both directions (subject to the information being truthful, not misleading and otherwise not the subject of an unfair or deceptive business practice).

The dynamic and robust system of privacy governance in the United States marshals the combined focus and enforcement muscle of the FTC, state attorneys general, the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services, the Department of Education, the judicial system, and last – but certainly not least – the highly motivated and aggressive US private plaintiffs' bar. Taken together, this enforcement ecosystem has proven to be nimble, flexible and effective in adapting to rapidly changing technological developments and practices, responding to evolving consumer and citizen expectations, and serving as a meaningful agent

2 South Dakota and Alabama became the 49th and 50th states to enact data breach notification laws in 2018. South Dakota enacted data breach notification legislation on 21 March 2018, while Alabama enacted data breach notification legislation on 28 March 2018.

of deterrence and accountability. Indeed, the US enforcement and litigation-based approach appears to be particularly well suited to deal with 'recent inventions and business methods' – namely new technologies and modes of commerce – that pose ever-changing opportunities and unpredictable privacy challenges.

II THE YEAR IN REVIEW

Privacy and cybersecurity remain hot topics for regulators, and the past years have seen a number of agencies that previously exercised a limited mandate in this area issue guidance and pursue enforcement actions. The courts have also been active, and a number of recent cases promise to reshape the legal landscape for years to come.

As detailed below, the FTC has continued to play a leading role at the federal level on these issues. Other government agencies announced their focus on these issues, often issuing guidance for entities that fall within their regulatory sphere of influence. The SEC has exercised increasingly aggressive oversight regarding cybersecurity compliance and practices of broker-dealers and investment advisers. It announced exam priorities, and brought an enforcement action against an investment adviser that failed to maintain cybersecurity policies and procedures. The Department of Justice has also issued guidance for addressing data breach incidents, and for interacting with federal law enforcement.

At the end of 2017, the FCC adopted the Restoring Freedom Order, which reclassified broadband internet back to being an 'information service,' and thus not a common carrier service. This returned jurisdiction to the FTC to regulate ISPs under its Section 5 authority to protect consumers and promote competition, including ISP privacy practices. In January 2018, following adoption of the Restoring Internet Freedom Order, the FTC and FCC entered a memorandum of understanding, through which the agencies will coordinate online consumer protection as they did prior to the 2015 order.

States have continued to push privacy and cybersecurity initiatives forward. South Dakota and Alabama became the 49th and 50th states to enact data breach notification laws in 2018. The South Dakota law requires notice within 60 days of the discovery of a breach. Notice to individuals is not required where there is no significant risk of identity theft, but notice must still be given to the state's attorney general. The Alabama law requires companies to provide Alabama residents with notification of a breach within 45 days of discovery. Notification is triggered by a determination of a breach that poses a risk of harm to impacted individuals. Other states, including Arizona, Colorado, Louisiana, and Oregon, have updated their notification laws.

On 28 June 2018, the California Consumer Privacy Act of 2018 (CCPA) was signed into law by that state's governor. It is scheduled to go into effect on 1 January 2020, whereupon it may become the most far-reaching privacy or data protection law in the country. In many ways, the CCPA emulates the EU's General Data Protection Regulation (GDPR). It mandates greater transparency and user control over data by imposing highly detailed disclosure requirements on companies that collect personal data about California residents. Unlike GDPR, however, CCPA generally permits opt-out rather than opt-in consent and it does not prohibit specific practices. The California law does mandate data subject rights regarding disclosure, access, and deletion. While it is anticipated that the CCPA will be subject to both legislative amendment (to correct errors and excesses) and regulatory interpretation (by the State Attorney General) before it takes effect in 2020, it may nonetheless influence

the development of other federal and state privacy legislation around the US. For example, California was the first state to enact data breach notification legislation, which all other states then followed.

On 16 May 2017, Washington became the third state to pass a law regulating biometric data, which governs the collection, use and retention of 'biometric identifiers', including fingerprints, voice prints, eye retinas, irises, or other patterns or characteristics that can be used to identify someone. The law specifically excludes 'physical or digital photograph, video or audio recording or data generated therefrom' (in addition to certain health-related data), suggesting the statute will have limited application in the context of facial-recognition technology. The law restricts the sale, lease and other disclosure of the data and requires its protection, but like a similar law in Texas, it does not provide for a private right of action. Illinois, the other state to pass a biometric data law, does, however, provide for a private cause of action, which has already spawned some litigation. Other states, including Connecticut, New Hampshire and Alaska, have considered the regulation of biometric data.

One case that saw continued development in early 2017 was *Spokeo, Inc v. Robins*. Thomas Robins had sued Spokeo for wilful violations of the Fair Credit Reporting Act (FCRA), alleging that inaccurate information disclosed about him on Spokeo's website harmed his employment opportunities. In May 2016, the Supreme Court remanded the case to the Ninth Circuit for consideration of whether Robins had suffered an injury that was sufficiently 'concrete' to find standing. On remand from the Supreme Court, on 15 August 2017, the Ninth Circuit held that an alleged injury was sufficiently 'concrete', citing the harms that may arise when persons' personal information is misused or improperly accessed. On 22 January 2018, the United States Supreme Court declined to review the Ninth Circuit Court of Appeals' decision.

In data breach litigation, courts continue to disagree about whether plaintiffs should prevail where they cannot allege that the criminal actually misused stolen data. In August 2017, the DC Circuit held that plaintiffs making allegations related to a 2015 breach had plausibly alleged a risk of harm, even without proving that their potentially stolen social security numbers had already been misused. Meanwhile, the Eighth Circuit held – on the one hand – that a plaintiff had standing to sue a company after a breach based on the theory that the plaintiff had paid for a certain level of security, and thus, the plaintiff arguably did not get the value of that bargain. On the other hand, however, the same court held that the case should be dismissed for failure to state a claim because of lack of evidence that anyone actually suffered fraud or identity theft resulting in financial loss. Moreover, the court stated that: '[t]he implied premise that because data was hacked [the company's] protections must have been inadequate is a "naked assertion devoid of further factual enhancement" that cannot survive a motion to dismiss' and 'massive class action litigation should be based on more than allegations of worry and inconvenience'.

Amid this uncertainty, large-scale breaches and attacks continue to occur. On 12 May 2017, the WannaCry attack disabled computers in organisations across the world, including the UK National Health Service. Hackers, believed to be in North Korea, demanded money to unfreeze the computers. WannaCry exploited weaknesses in unpatched Windows XP operating systems and wreaked havoc in the United States, the United Kingdom and around the world. On 7 September 2017, Equifax, one of the three major consumer credit reporting agencies, announced that it had suffered a hack that potentially compromised the

data of 143 million Americans. In 2018, a variety of websites including MyFitnessPal, a fitness app run by Under Armour; Ticketmaster; and numerous other companies publicly reported cybersecurity incidents.

i FTC actions

In October 2016, the FTC announced the release of a new guide for businesses dealing with data breaches. The guide covers the process businesses should follow and what officials they should contact when there is a data breach. It includes advice regarding secure systems, managing service providers, segmenting networks and notifying users whose information has been stolen. The FTC also released a video explaining much of the same material.

On 6 February 2017, the FTC announced that VIZIO had agreed to pay US$2.2 million to settle charges by the FTC and the New Jersey attorney general that it installed software on TVs to collect viewing data of its 11 million customers without their knowledge or consent. The order required VIZIO to prominently disclose and obtain affirmative express consent for data collection and sharing. The settlement also required VIZIO to delete all data it collected before 1 March 2016 and to implement a comprehensive data privacy programme that would be regularly assessed.

On 15 August 2017, the FTC reached a settlement with Uber regarding allegations that the company had misrepresented its cybersecurity protections and engaged in unreasonable cybersecurity practices. The settlement sheds greater light on what the FTC means by the 'reasonable data security' measures it expects companies to take. Uber suffered a breach of its drivers' location and other data and was the subject of 2014 news reports that alleged Uber employees could gain access to and use its customers' personal information, including precise geolocation data. The FTC settlement clarified the core elements of a 'reasonable' data security programme, including restricted employee access to sensitive data, multi-factor authentication for remote access and encryption of sensitive personal data both in transit and at rest.

The Court of Justice of the European Union (CJEU) has had an outsize impact on privacy and data protection issues that affect US companies. The CJEU decision invalidating the US–EU Safe Harbor in October 2015 led to lengthy negotiations between US and EU authorities on an appropriate replacement mechanism for data transfers across the Atlantic, resulting in the EU–US Privacy Shield Framework (Privacy Shield), which has been in place for more than a year. The FTC has brought three recent enforcement actions alleging that companies made false claims about Privacy Shield participation. In all three complaints, the FTC alleged the companies falsely stated in their privacy policies that they would comply with Privacy Shield, because the companies started the application for Privacy Shield compliance but did not complete the necessary steps to ensure full compliance before claiming they were Privacy Shield participants.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The United States has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk:

a financial, insurance and medical information;
b information about children and students;
c telephone, internet and other electronic communications and records;

d credit and consumer reports and background investigations at the federal level; and
e a further extensive array of specific privacy laws at the state level.

Moreover, the United States is the unquestioned world leader in mandating information security and data breach notifications, without which information privacy is not possible. If one of the sector-specific federal or state laws does not cover a particular category of data or information practice, then the Federal Trade Commission Act (FTCA), and each state's 'little FTCA' analogue, comes into play. Those general consumer protection statutes broadly, flexibly and comprehensively proscribe (and authorise tough enforcement against) unfair or deceptive acts or practices. The FTC is the *de facto* privacy regulator in the United States. State attorneys general and private plaintiffs can also enforce privacy standards under analogous 'unfair and deceptive acts and practices' standards in state law. Additionally, information privacy is further protected by a network of common law torts, including invasion of privacy, public disclosure of private facts, 'false light', appropriation or infringement of the right of publicity or personal likeness, and, of course, remedies against general misappropriation or negligence. In short, there are no substantial lacunae in the regulation of commercial data privacy in the United States. In taking both a general (unfair or deceptive) and sectoral approach to commercial privacy governance, the United States has empowered government agencies to oversee data privacy where the categories and uses of data could injure individuals.

FTCA

Section 5 of the FTCA prohibits 'unfair or deceptive acts or practices in or affecting commerce'. While the FTCA does not expressly address privacy or information security, the FTC applies Section 5 to information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities. The FTC has brought successful enforcement actions under Section 5 against companies that failed to 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.

Under Section 5, an act or practice is deceptive 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' – defined as an act or practice 'likely to affect the consumer's conduct or decision with regard to a product or service'. 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 takes the position that 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. The FTC brought an enforcement action in 2009 against Sears for allegedly failing to adequately disclose 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 behavior that occurs on [. . .] computers'. The FTC required Sears to prominently disclose any data practices that would have significant unexpected implications in a separate screen outside any user agreement, privacy policy or terms of use.

Section 5 is also generally understood to prohibit 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.

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.

The FTC's report does not, however, require opt-in consent for the use of non-sensitive information in behavioural advertising.

Fair information practice principles

The innovative American privacy doctrine elaborated theories for tort and injunctive remedies for invasions of privacy (including compensation for mental suffering). The Warren–Brandeis right to privacy, along with the right to be let alone, was followed in 1973 by the first affirmative government undertaking to protect privacy in the computer age. The new philosophy was expressed in the Report of the Secretary's Advisory Committee on Automated Personal Data Systems, published by the US Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services). This report developed the principles for 'fair information practices' that were subsequently adopted by the United States in the 1974 Privacy Act, and ultimately by the European Union in 1995 in its Data Protection Directive. The fair information practice principles established in the United States in 1973–1974 remain largely operative around the world today in regimes and societies that respect information privacy rights of individuals. The fundamental US HEW/ Privacy Act principles were:

a there must be no personal data record-keeping systems whose very existence is secret;

b there must be a way for an individual to find out what information about him or her is in a record and how it is used;

c there must be a way for an individual to prevent information about him or her obtained for one purpose from being used or made available for other purposes without his or her consent;

d there must be a way for an individual to correct or amend a record of identifiable information about him or her; and

e any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use, and must take reasonable precautions to prevent misuse of the data.

Classification of data

The definitions of personal data and sensitive personal data vary by regulation. The FTC considers information that can reasonably be used to contact or distinguish an individual (including IP addresses) to constitute personal data (at least in the context of children's

privacy). Generally, sensitive data includes personal health data, credit reports, personal information collected online from children under 13, precise location data, and information that can be used for identity theft or fraud.

Federal laws

Congress has passed laws protecting personal information in the most sensitive areas of consumer life, including health and financial information, information about children and credit information. Various federal agencies are tasked with rule making, oversight and enforcement of these legislative directives.

The scope of these laws and the agencies that are tasked with enforcing them is formidable. Laws such as the Children's Online Privacy Protection Act of 1998 (COPPA), the Health Insurance Portability and Accountability Act of 1996, the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act or GLBA), the FCRA, the Electronic Communications Privacy Act, the Communications Act (regarding CPNI) and the Telephone Consumer Protection Act of 1991, to name just a few, prescribe specific statutory standards to protect the most sensitive consumer data.

The Cybersecurity Act, passed in 2015, includes a Cybersecurity Information Sharing Act (CISA). CISA is designed to foster cyberthreat information sharing and to provide certain liability shields related to such sharing and other cyber-preparedness. In addition, US intelligence agency collection of bulk phone metadata pursuant to the USA Freedom Act ended in 2015, which means that targeted court orders are required for government collection of phone metadata stored by telecommunications companies.

The Defend Trade Secrets Act (DTSA) also provides federal legislative protection for information by expanding access to judicial redress for unauthorised access and use of trade secrets. The DTSA amends the Economic Espionage Act of 1996 to provide plaintiffs with a private cause of action to sue for trade-secret theft and pursue damages in federal court. The DTSA authorises a federal court to grant an injunction to prevent actual or threatened misappropriation of trade secrets, but the injunction may not prevent a person from entering into an employment relationship; nor place conditions on employment based merely on information the person knows. Rather, any conditions placed on employment must be 'based on evidence of threatened misappropriation'. Moreover, the DTSA precludes the court from issuing an injunction that would 'otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business'.

State laws

In addition to the concurrent authority that state attorneys general share for enforcement of certain federal privacy laws, state legislatures have been especially active on privacy issues that states view worthy of targeted legislation. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues,[3]

3 See www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

cyberstalking,[4] data disposal,[5] privacy policies, security breach notification,[6] employer access to employee social media accounts,[7] unsolicited commercial communications[8] and electronic solicitation of children,[9] to name but a few.

California is viewed as a leading legislator in the privacy arena, and its large population and high-tech sector means that the requirements of California law receive particular attention and often have *de facto* application to businesses operating across the United States.[10]

The highly significant, new California Consumer Privacy Act of 2018 is discussed above in Section II.

Co-regulation and industry self-regulation

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 use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. This approach has had notable success, such as the development of the 'About Advertising' icon by the Digital Advertising Alliance and the opt-out for cookies set forth by the Network Advertising Initiative.[11] 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. 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. It should also be noted that various laws require publication or provision of privacy policies, including, *inter alia*, the GLBA (financial data), Health Insurance Portability and Accountability Act (HIPAA) (health data) and California law (websites collecting personal information). In addition, voluntary membership or certification in various self-regulatory initiatives also require posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on those policies.

ii General obligations for data handlers

There is no general requirement to register databases in the United States. Depending on the context, data handlers may be required to provide data subjects with a pre-collection notice, and the opportunity to opt out of the use and disclosure of regulated personal information.

4 See www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2016.aspx.

5 See www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

6 See www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

7 See www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

8 See www.ncsl.org/research/telecommunications-and-information-technology/state-spam-laws.aspx.

9 See www.ncsl.org/research/telecommunications-and-information-technology/electronic-solicitation-or-luring-of-children-sta.aspx.

10 See oag.ca.gov/privacy/privacy-laws.

11 See www.aboutads.info; www.networkadvertising.org/choices/?partnerId=1//.

Information that is considered sensitive personal information, such as health information, may involve opt-in rules. The FTC considers it a deceptive trade practice if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was obtained.

iii Technological innovation and privacy law

Electronic marketing is extensively regulated in the United States through a myriad of laws. The CAN-SPAM Act is a federal law governing commercial email messages. Generally, a company is permitted to send commercial emails to anyone under CAN-SPAM, provided these conditions are met: 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.

Generally, express written consent is required for companies to send marketing text messages. Marketing texts are a significant class action risk area.

There is no specific federal law that regulates the use of cookies and other similar online tracking tools. However, the use of tracking mechanisms should be carefully and fully disclosed in a company's website privacy policy. Additionally, it is best practice for websites that allow online behavioural advertising to participate in the Digital Advertising Alliance code of conduct, which enables users to easily opt out of being tracked for these purposes. California law imposes further requirements on online tracking. California requires companies that track personally identifiable information over time and multiple websites to disclose how the company responds to 'do-not-track' signals, and whether users can opt out of such tracking.

Location tracking is currently a subject of interest and debate. FCC regulations govern the collection and disclosure of certain location tracking by telecommunications providers (generally speaking, telephone carriers). Additionally, the FTC and California have issued best-practice recommendations for mobile apps and mobile app platforms.

iv Specific regulatory areas

The US system of privacy is composed of laws and regulations that focus on particular industries (financial services, healthcare, communications), particular activities (i.e., collecting information about children online) and particular types of data.

Federal

Financial privacy

For financial privacy, the federal banking agencies and the FTC were previously primarily responsible for enforcing consumer privacy under the GLBA, which applies to financial institutions. Following the 2010 Dodd-Frank legislation, such laws will be primarily (but not exclusively) enforced by the new Consumer Financial Protection Bureau, which has significant, independent regulatory and enforcement powers. The FTC, however, will remain primarily responsible for administering the FCRA, along with the general unfair and deceptive acts and practices standards under the FTCA and COPPA, which impose affirmative privacy and security duties on entities that collect personal information from children under 13 years of age.

The GLBA addresses financial data privacy and security by establishing standards for safeguarding customers' 'non-public personal information' – or personally identifiable financial information – stored by 'financial institutions', and by requiring financial institutions to provide notice of their information-sharing practices. In brief, the GLBA requires financial institutions to provide notices of policies and practices regarding disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties, unless consumers are provided the right to opt out of such disclosure or other exceptions apply; and to establish safeguards to protect the security of personal information.

The FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003, 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 FCRA 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.[12]

The Consumer Financial Protection Bureau (CFPB), which is the primary federal regulator of consumer financial products and services, brought its first data security enforcement action in 2016 under the authority granted by Dodd-Frank against Dwolla Inc, an online payments company, for allegedly deceptive representations with respect to its data security practices. Dodd-Frank authorises the CFPB to take action against institutions engaged in unfair, deceptive or abusive acts or practices or that otherwise violate federal consumer financial laws. Under the terms of the CFPB order against Dwolla, the company was required to stop misrepresenting its data security practices, train employees properly and fix security flaws. In addition, Dwolla was required to pay a US$100,000 civil money penalty.

On 18 October 2017, the CFPB released a set of consumer protection principles principles designed to protect consumer interests in the market for services built around consumer-approved use of financial information. The Principles are targeted to so-called 'data aggregation' or 'screen scraping' services that collect customer information in order to provide financial planning or other services. Over the past few years, data aggregation services and banks have struggled to develop the right model for sharing customer account data. The Principles issued by the CFPB seek to provide a potential data-sharing model for banks and data aggregation services while protecting consumer interests. Although the Principles set forth by the CFPB are not binding requirements, they signal increased momentum for a workable model of data sharing between banks and fintech companies. They may also demonstrate the CFPB's expectations of market participants and its broader viewpoints about consumer privacy and consent. The nine Principles cover the areas of data access, data scope and usability, consumer control and informed consent, separate authorisation credentials, data security, access transparency, data accuracy, consumer ability to dispute and resolve unauthorised access, and efficient and effective accountability mechanisms for risks.

12 Available at www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act.

Healthcare privacy

For healthcare privacy, agencies within the Department of Health and Human Services administer and enforce HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). HIPAA was enacted to create national standards for electronic healthcare transactions, and the US Department of Health and Human Services has promulgated regulations to protect privacy and security of personal health information (PHI). Patients generally have to opt in before their information can be shared with other organisations.[13] HIPAA applies to '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.

'Protected health information' is defined broadly as 'individually identifiable health information [. . .] transmitted or maintained in electronic media' or in 'any other form or medium'. 'Individually identifiable health information' is defined as information that is 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. HIPAA also does not apply to 'de-identified' data.

A 'business associate' is 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). Business associates are required to enter into agreements, called business associate agreements, requiring business associates to use and disclose PHI only as permitted or required by the business associate 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, as well as numerous other provisions regarding confidentiality, integrity and availability of electronic PHI. HIPAA and HITECH not only restrict access to and use of medical information, but also impose stringent information security standards.

Communications privacy

For communications privacy, the FCC, the Department of Justice and, to a considerable extent, private plaintiffs can enforce the data protection standards in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and various sections of the Communications Act, which include specific protection for CPNI such as telephone call records. The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communications and related records. The Computer Fraud and Abuse Act prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders

13 Available at aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996.

or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks. The FCC, however, is the primary regulator for communications privacy issues, and has been active over the past year.

The FCC shares jurisdiction with the FTC on certain privacy and data security issues, including notably on the issue of robocalls as governed by the Telephone Consumer Protection Act. There has been significant regulatory activity in the past year, including guidance released by the FCC on auto-diallers in August 2015, not to mention substantial private litigation driven by the statutory penalties provided for by the Telephone Consumer Protection Act (TCPA). The FCC has stated that complaints regarding unwanted calls are the largest category of complaints received by the FCC – numbering over 215,000 complaints in 2014 alone.[14]

Children's privacy

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. COPPA requires 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.[15]

Other federal privacy laws

Even the array of privacy laws described above is hardly comprehensive. A number of other federal privacy laws protect personal information in the areas of cable television, education, telecommunications customer information, drivers' and motor vehicle records, and video rentals. Federal laws also protect marketing activities such as telemarketing, junk faxes and unsolicited commercial email. In addition, in October 2016, the Department of Transportation issued guidance on cybersecurity best practices for interconnected cars and self-driving technology.

State legislation

In the areas of online privacy and data security alone, state legislatures have passed a number of laws covering access to employee and student social media passwords, children's online privacy, e-Reader privacy, online privacy policies, false and misleading statements in website privacy policies, privacy of personal information held by ISPs, notice of monitoring of employee email communications and internet access, phishing, spyware, security breaches, spam and event data recorders. California is viewed as the leading legislator in the privacy arena, with many other states following its privacy laws. State attorneys general also have concurrent authority with the FTC or other federal regulators under various federal laws, such as COPPA, HIPAA and others.

The National Council of State Legislatures summarises the following state provisions regarding online privacy:

14 See www.fcc.gov/document/fcc-strengthens-consumer-protections-against-unwanted-calls-and-texts.

15 Available at www.law.cornell.edu/USCode/text/15/6501.

Privacy Policies for Websites or Online Services
California's Online Privacy Protection Act requires an operator [. . .] to post a conspicuous privacy policy on its Website or online service [. . .] and to comply with that policy. The law, among other things, requires that the privacy policy identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its Website [and] how the operator responds to a web browser 'Do Not Track' signal. Connecticut [r]equires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be 'publicly displayed' by posting on a web page and the policy must [. . .] protect the confidentiality of Social Security numbers.

Privacy of Personal Information Held by Internet Service Providers
Two states, Nevada and Minnesota, require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.

False and Misleading Statements in Website Privacy Policies
Nebraska prohibits knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public. Pennsylvania includes false and misleading statements in privacy policies published on Websites or otherwise distributed in its deceptive or fraudulent business practices statute.

Notice of Monitoring of Employee E-mail Communications and Internet Access
Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access.[16]

After Congress rescinded the FCC's privacy rules for internet providers, various states are considering legislation that would restrict how ISPs collect and use consumer data. Nevada and Montana now require ISPs to maintain the privacy of certain customer information absent consent, and California adopted the California Consumer Privacy Act as discussed under Year in Review above. 24 other states are considering their own legislative proposals.

Children's online privacy

California prohibits websites directed to minors from advertising products based on information specific to that minor. The law also 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.[17]

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

There are no significant or generally applicable data transfer restrictions in the United States; however, the United States has taken steps to provide compliance mechanisms for companies

16 National Conference of State Legislatures, www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

17 Calif Bus & Prof Code Sections 22580–22582.

that are subject to data transfer restrictions set forth by other countries. The ruling by the CJEU that the US–EU Safe Harbor Framework is 'invalid' has brought a considerable degree of uncertainty to the thousands of companies that rely on it as a bedrock of day-to-day global operations. This development had a significant impact on businesses that rely on Safe Harbor to legitimise transfers of personal data from the EU to the United States.

The EU–US Privacy Shield provides a new framework for transatlantic data transfers. The new agreement, which was announced in February and activated in August, replaces Safe Harbor, which was invalidated by the European Court of Justice in October 2015. The new agreement places more stringent duties on US companies to safeguard Europeans' personal data and on the US Department of Commerce and the FTC for increased scrutiny, enforcement and partnership with European data protection authorities. As part of the framework, the United States agrees that there will be no indiscriminate mass surveillance and access to data for law enforcement and national security purposes with respect to data transferred under the new framework, and must meet certain checks to ensure data are only accessed as necessary and proportionate. In addition, European citizens who believe their data have been compromised in violation of the new agreement will be able to bring complaints to a dedicated ombudsperson. However, some elements of the new agreement share qualities with the now-defunct Safe Harbor, including that companies will subscribe to data protection principles, and that there will be a structured redress process.

In 2012, the United States was approved as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC became the system's first privacy enforcement authority. The FTC's Office of International Affairs[18] works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[19] In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.[20]

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management[21] reveals the success of enforcement in pushing corporate privacy managers to look beyond the letter of the law to develop state-of-the-art privacy practices that anticipate FTC enforcement actions, best practices and other forms of FTC policy guidance. Many corporate privacy managers explain that the constant threat and unpredictability of future enforcement by the FTC and parallel state consumer protection officials, combined with the deterrent effect of enforcement actions against peer companies, motivate their companies to proactively develop privacy policies and practices that exceed industry standards. Other companies respond by hiring a privacy officer, or by creating or expanding a privacy leadership function. The risk of enforcement has also prompted companies to engage in ongoing dialogues with the FTC and state regulators.

18 See FTC, Office of International Affairs, www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs.

19 See FTC, International Consumer Protection, www.ftc.gov/policy/international/international-consumer-protection.

20 See 'APEC Overview', Chapter 2.

21 Kenneth A Bamberger and Deirdre K Mulligan, 'Privacy on the Books and on the Ground' (18 November 2011), Stanford Law Review, Volume 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Available at ssrn.com/abstract=1568385.

Corporate privacy managers have also emphasised that while compliance-oriented laws in other jurisdictions do not always keep pace with technological innovation, the FTC's Section 5 enforcement authority allows it to remain nimble in protecting consumer privacy as technology and consumer expectations evolve over time.

The United States does not require companies to appoint a data protection officer (although specific laws such as the GLBA and HIPAA require companies to designate employees to be responsible for the organisation's mandated information security and privacy programmes). However, it is best practice to appoint a chief privacy officer and an IT security officer. Most businesses in the United States are required to take reasonable physical, technical and organisational measures to protect the security of sensitive personal information, such as financial or health information. An incident response plan and vendor controls are not generally required under federal laws (other than under the GLBA and HIPAA), although they are best practice in the United States and may be required under some state laws. Regular employee training regarding data security is also recommended. Under the FCC's now judicially upheld Open Internet Order, broadband ISPs are now also likely to be expected to have incident response plans and vendor controls for data security.

Some states have enacted laws that impose additional security or privacy requirements. For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls, and California requires covered entities to have an online privacy policy with specific features, such as an effective date. And, on 22 May 2018, Vermont enacted the first state-level measure aimed at data brokers. The law requires data brokers to register as such with the Secretary of State, or be subject to civil and other penalties. It also requires data brokers to disclose information about their collection activities, adopt standard security measures, and notify authorities of security breaches.

VI DISCOVERY AND DISCLOSURE

Companies may be required under various federal and state laws to produce information to law enforcement and regulatory authorities, and to civil litigation demands. For example, companies may be ordered to produce information based on federal or state criminal authorities issuing a search warrant, a grand jury subpoena or a trial subpoena, or federal or state regulatory authorities issuing an administrative subpoena. Further, companies could be ordered to produce information upon receiving a civil subpoena in civil litigation.

Such US legal demands may create potential conflicts with data protection or privacy law outside the United States. Companies should consider these possible conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to European data, such that European data could be considered within the company's lawful control in the United States and thereby subject to production requests irrespective of European blocking statutes.

The United States does not have a blocking statute. Domestic authorities generally support compliance with requests for disclosure from outside the jurisdiction. The principle of comity is respected, but national law and the Federal Rules of Civil Procedure typically trump foreign law.[22]

22 *Société Nationale Industrielle Aérospatiale v. US District Court*, 482 US 522, 549 (1987) (requiring a detailed comity analysis balancing domestic and foreign sovereign interests, in particular US discovery interests and

In a highly significant recent case, the federal court in the Southern District of New York (Manhattan) ruled that Microsoft could be required to transfer customer communications (the contents of emails) stored in Ireland to law enforcement in the United States.[23] However, in July 2016, the Second Circuit overturned the District Court's decision, holding that the government cannot force Microsoft to turn over customer emails stored outside the United States.[24] The issue in the case concerns whether a search warrant served in the United States could authorise the extraterritorial transfer of customer communications notwithstanding the laws of Ireland and the availability of the mutual legal assistance treaty process. The Second Circuit held that Microsoft would not have to turn over customer emails stored in Ireland because the warrant provision of the Stored Communications Act (SCA) does not extend to data stored on foreign servers. The Court stated that 'Congress did not intend the SCA's warrant provisions to apply extraterritorially'. Microsoft's resistance to the US government's search warrant was supported by numerous other communications and tech companies. Microsoft hailed this decision as one that ensures people's privacy rights are protected by the laws of their own country, as well as one that prevents foreign governments from accessing consumer data stored within the United States. On 17 April 2018, the United States Supreme Court vacated and remanded the case, with instructions to dismiss it as moot in light of the 23 March 2018 enactment of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), and subsequent warrant from the government for the information pursuant to the new law.

In a significant January 2018 case, *Leibovic v. United Shore Fin. Servs., LLC*, the United States Court of Appeals for the Sixth Circuit issued a decision that concluded a company had implicitly waived privilege when it disclosed certain materials relating to a privileged forensic data breach investigation in response to a discovery request.[25] The Sixth Circuit's decision emphasises the need for caution by litigants wishing to raise a defence that relies on privileged investigations and reports, including third-party forensic reports, or otherwise disclosing the conclusions of such investigations and reports.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Every business in the United States is subject to privacy laws and regulations at the federal level, and frequently at the state level. These privacy laws and regulations are actively enforced by federal and state authorities, as well as in private litigation. The FTC, the Executive Branch and state attorneys general also issue policy guidance on a number of general and specific privacy topics.

Like many other jurisdictions, the United States does not have a central *de jure* privacy regulator. Instead, a number of authorities – including, principally, the FTC and state

foreign blocking statutes). These issues are currently being litigated in a case involving the execution of a criminal search warrant issued to Microsoft for data stored in its servers located in Ireland. The case is now on appeal following the District Court decision obliging Microsoft to produce the data in question.

23 *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp*, 15 F Supp 3d 466.

24 *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp*, No. 14-02985 (2nd Cir 14 July 2016).

25 See *In re United Shore Fin. Servs., LLC*, No. 17-2290, 2018 WL 2283893, at *1 (6th Cir 3 January 2018).

consumer protection regulators (usually the state attorney general) – exercise broad authority to protect privacy. In this sense, the United States has more than 50 *de facto* privacy regulators overseeing companies' information privacy practices. Compliance with the FTC's guidelines and mandates on privacy issues is not necessarily coterminous with the extent of an entity's privacy obligations under federal law – a number of other agencies, bureaus and commissions are endowed with substantive privacy enforcement authority.

Oversight of privacy is by no means exclusively the province of the federal government – state attorneys general have increasingly established themselves in this space, often drawing from authorities and mandates similar to those of the FTC. The plaintiff's bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of corporations doing business with consumers.

At the federal level, Congress has passed robust laws protecting consumers' sensitive personal information, including health and financial information, information about children and credit information. At the state level, nearly all 50 states have data breach notification laws on the books,[26] and many state legislatures – notably California[27] – have passed privacy laws that typically affect businesses operating throughout the United States.[28]

FTC

The FTC is the most influential government body that enforces privacy and data protection[29] in the United States.[30] It oversees essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[31] Through exercise of powers arising out of Section 5 of the FTCA, the FTC has taken a leading role in laying out general privacy principles for the modern economy. Section 5 charges the FTC with prohibiting 'unfair or deceptive acts or practices in or affecting commerce'.[32] 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.[33]

Former FTC Commissioner Julie Brill noted, 'the FTC has become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its

26 See www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

27 See www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

28 See, for example, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx and www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

29 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.

30 See Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 Columbia Law Review ('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.

31 See www.ftc.gov/about-ftc/what-we-do.

32 15 USC Section 45.

33 15 USC Section 45(a)(4).

disposal to prosecute an impressive series of enforcement cases'.[34] Using this authority, the FTC has brought numerous privacy deception and unfairness cases and enforcement actions, including over 100 spam and spyware cases and approximately 60 data security cases.[35]

The FTC has sought and received various forms of relief for privacy related 'wrongs' or bad acts, including injunctive relief, damages and the increasingly popular practice of consent decrees. Such decrees require companies to unequivocally submit to the ongoing oversight of the FTC, and to implement controls, audit, and other privacy enhancing processes during a period that can span decades. These enforcement actions have been characterised as shaping a common law of privacy that guides companies' privacy practices.[36]

'Deception' and 'unfairness' effectively cover the gamut of possible privacy-related actions in the marketplace. Unfairness is understood to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context. The FTC has taken action against companies for deception when false promises, such as those relating to security procedures that are purportedly in place, have not been honoured or implemented in practice. As part of this new common law of privacy (which has developed quite aggressively in the absence of judicial review), the FTC's enforcement actions include both online and offline consumer privacy practices across a variety of industries, and often target emerging technologies such as the internet of things.

The agency's orders generally provide for ongoing monitoring by the FTC, prohibit further violations of the law and subject businesses to substantial financial penalties for order violations. The orders protect all consumers dealing with a business, not just the consumers who complained about the problem. The FTC also has jurisdiction to protect consumers worldwide from practices taking place in the United States – Congress has expressly confirmed the FTC's authority to redress harm abroad caused from within the United States.[37]

The states

Similarly to the FTC, state attorneys general retain powers to prohibit unfair or deceptive trade practices arising from powers granted by 'unfair or deceptive acts and practices' statutes. 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 the past two years, several state attorneys general have formally created units charged with the oversight of privacy, in states such as California, Connecticut and Maryland.

The mini 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. In 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

34 Commissioner Julie Brill, 'Privacy, Consumer Protection, and Competition', Loyola University Chicago School of Law (27 April 2012), available at www.ftc.gov/speeches/brill/120427loyolasymposium.pdf.

35 See Commissioner Maureen K Ohlhausen, 'Remarks at the Digital Advertising Alliance Summit' (5 June 2013), available at www.ftc.gov/speeches/ohlhausen/130605daasummit.pdf.

36 See, for example, Solove and Harzog, 2014 (see footnote 29).

37 15 USC Section 45(a)(4).

ii Recent enforcement cases

FTC data protection enforcement

The FTC's data protection enforcement has spanned both privacy and security cases, and has focused on both large and small companies across a variety of industries. Some illustrative cases are summarised below.

Internet of things

The FTC recently broke new ground by bringing an enforcement action in the emerging field of the 'internet of things'. In September 2013, the FTC announced that it settled a case with TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely. The FTC's complaint charged that the company falsely claimed in numerous product descriptions that its cameras were 'secure'; in reality, the cameras were equipped with faulty software that permitted anyone with the cameras' internet address to watch or listen online. As a result, hundreds of consumers' private camera feeds were made public on the internet. The FTC's order imposes numerous requirements on TRENDnet:

a a prohibition against misrepresenting the security of its cameras;
b the establishment of a comprehensive information security programme designed to address security risks;
c submitting to third-party assessments of its security programmes every two years for the next 20 years;
d notifying customers of security issues with the cameras and the availability of the software update to correct them; and
e providing customers with free technical support for the next two years.[38]

The FTC issued a report on the internet of things, 'Internet of Things: Privacy & Security in a Connected World', in 2015. Two years in the making, the report provides recommendations to companies about protecting consumer privacy and securing customer data created by the new world of sensors and wearables – mainly by building security into products and services, minimising data collection, and giving consumers notice and choice about how their data are used. The report considers new statutes to be premature, but does suggest that the agency intends to adapt existing authorities under the FTCA, the FCRA and COPPA. Republican Commissioner Wright dissented from the report, arguing that the FTC should not issue recommendations and best practices without engaging in a cost–benefit analysis to determine that such measures would, if adopted, improve consumer welfare. Commissioner Wright also suggested that the Commission departed from standard practice by issuing policy recommendations in a workshop report, as such reports typically serve only to 'synthesise the record developed during the proceedings'. Addressing attendees at the Better Business 2016 Conference in Washington, DC on 21 April 2016, Federal Trade Commissioner Maureen Ohlhausen remarked that the Commission should examine existing privacy regulations to determine how they apply to the potential new privacy risks created by the internet of things.

38 Press release, 'FTC Approves Final Order Settling Charges Against TRENDnet, Inc.' (7 February 2014), available at www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

Commissioner Ohlhausen expressed excitement about the potential benefits that smart devices can bring, but cautioned that these technologies carry with them new risks with respect to data collection and surveillance.

In 2016, the FTC published another report, entitled 'Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues'. The report focused on how Big Data are used after being collected and analysed, and presented questions for businesses to consider to avoid exclusionary or discriminatory outcomes for consumers. The report discussed innovative uses of Big Data that are benefiting underserved populations, such as through increased educational and healthcare opportunities, but also looked at risks that could arise from biases about certain groups. The report discusses numerous factors for companies to consider to enhance the relevance, quality, accuracy, objectivity and fairness of predictions and decision-making based on Big-Data analytics and embedded algorithms.

On 8 January 2018, the FTC announced a settlement with VTech (a maker of electronic children's toys) for violations of COPPA, adding to the regulatory activity mounting in the last few years around the internet of things, and more specifically, the internet of toys. The company agreed to pay US$650,000 to settle allegations that its app and platform collected personal information from almost 3,000,000 children without providing direct notice and obtaining their parent or guardian's consent. Specifically, the FTC alleged that the company failed to provide a link to its privacy policy in each area where personal information was collected from children. The FTC also alleged that the company failed to take reasonable steps to secure the data it collected in violation of both COPPA and the FTC Act, and that these poor data security practices contributed to a November 2015 data breach.

Financial and medical information

The SEC Office of Compliance Inspections and Examinations (OCIE) issued guidance on cybersecurity and announced examination priorities, taking multiple steps to heighten its enforcement presence for cybersecurity matters and identifying cybersecurity as an SEC OCIE exam priority for 2018. The SEC took several cybersecurity-related steps in September 2015 that related to its mandate to oversee investment advisers and broker-dealers, and to protect investors. OCIE issued a risk alert setting forth concrete guidance for broker-dealers and investment advisers, including notably a view that multifactor authentication was a 'basic control'. The alert served to announce cybersecurity as a renewed area of focus for examinations, and included a sample document request for upcoming exams. Further, the SEC announced that it reached a settlement with R T Jones, an investment adviser that did not have cybersecurity policies and procedures in place prior to a breach. Despite the company's immediate remedial steps, the SEC found that R T Jones's failure to maintain such policies was a violation of Regulation S-P. In connection with the settlement, the Office of Investor Education and Advocacy announced an investor alert to heighten individual awareness regarding response to identity theft or data breaches impacting their investment accounts. In August 2017, OCIE issued a summary of observations from recent sweep exams of broker-dealers, investment advisers and funds. OCIE reported an improvement in awareness of cyber risks and implementation of cybersecurity practices in the past few years. Nearly all entities examined maintained written cybersecurity policies and procedures. OCIE noted, however, that many policies were not sufficiently detailed and were overly vague, and recommended that policies should be 'reasonably tailored' to the company. There were also noted issues with companies failing to follow their written policies, follow up with remediation when issues were discovered or patch systems appropriately. In 2018, the SEC

issued new guidance on cybersecurity disclosures in SEC filings. In addition to information on cybersecurity disclosure controls and procedures, the guidance included components on policies to prevent insider trading based on non-public cyber information.

Mini FTCA privacy enforcement cases

In the past few years, state attorneys general have brought a number of enforcement actions pursuant to their authority under their respective states' mini FTCAs. Two illustrative examples are summarised below.

Google Street View settlement

In 2013, 38 state attorneys general reached a US$7 million settlement with Google over allegations that the company violated people's privacy by collecting Wi-Fi data as part of its Street View activities. Google agreed to train its employees about privacy and confidentiality for at least the next 10 years, and to destroy or secure any improperly collected information.[39]

Safari cookie settlements

In 2013, 37 states settled, for US$17 million, an investigation with Google involving allegations that the company bypassed web browser privacy settings to collect consumers' browsing information. Another settlement related to this incident, which was already approved by a judge and requires Google to donate more than US$3 million to schools and non-profits, is now being criticised by attorneys general from 11 states, who argue that the settlement should provide for the money to go to the people who were allegedly affected.

Robocalls

The FCC remains interested in preventing robocalls. The FCC issued its biannual warning to political campaigns about robocalls and text abuse in March 2016. The FCC's warning said the FCC 'is committed to protecting consumers from harassing, intrusive, and unwanted robocalls and texts, including to cell phones and other mobile devices'. The warning pledged that the FCC's Enforcement Bureau will 'rigorously enforce' the TCPA. On 16 March 2018, the US Court of Appeals for the DC Circuit issued a ruling on a challenge to the FCC's 2015 order that expanded the scope of the Telephone Consumer Protection Act (TCPA). In *ACA International v. FCC*, the court invalidated a rule that had broadly defined automatic telephone dialing systems, or 'auto-dialers'; it also struck down the FCC's approach to situations where a caller obtains a party's consent to be called but then, unbeknownst to the caller, the consenting party's wireless number is reassigned.[40] In the same ruling, the court upheld the FCC's decision to allow parties who have consented to be called to revoke their consent in 'any reasonable way,' as well as the FCC's decision to limit the scope of an exemption to the TCPA's consent requirement for certain healthcare-related calls. Following the ruling, the FCC issued a public notice seeking input about how it should interpret the TCPA.

39 See, for example, press release, 'Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data' (12 March 2013), available at www.ct.gov/ag/cwp/view.asp?Q=520518.

40 *ACA Int'l v. Fed. Commc'ns Comm'n*, 885 F.3d 687, 692 (DC Cir 2018).

Unsolicited faxes

The FCC imposed a US$1.84 million penalty against Scott Malcolm, DSM Supply and Somaticare for sending 115 unsolicited fax advertisements to the fax machines of 26 consumers. The faxes were primarily sent to healthcare practitioners. The FCC issued this forfeiture order in February 2016.

iii Private litigation

Privacy rights have long been recognised and protected by common law. The legal scholar William Prosser created a taxonomy of four privacy torts in his 1960 article 'Privacy' and later codified the same in the American Law Institute's Restatement (Second) of Torts. The four actions for which an aggrieved party can bring a civil suit are:

a intrusion upon seclusion or solitude, or into private affairs;
b public disclosure of embarrassing private facts;
c publicity that places a person in a false light in the public eye; and
d appropriation of one's name or likeness.

These rights protect not only the potential abuse of information, but generally govern its collection and use.

The plaintiff's bar

The plaintiff's bar is highly incentivised to vindicate commercial privacy rights through consumer class action litigation. 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 plaintiff's litigation around the Video Privacy Protection Act (VPPA) may attempt to take advantage of a narrow opening in the First Circuit, which broadens the statute's definition of personally identifiable information to find liability against companies that disclose information about consumers' video viewing. In *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit held that 'personally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior'.[41] This narrow definition of personally identifiable information is upheld across numerous jurisdictions. However, this creates a circuit split with the First Circuit, which held in *Yershov v. Gannett Satellite Information Network Inc* that the VPPA was violated when a company disclosed a unique anonymous Adobe ID, GPS coordinates and video title information without consent to a third party.[42]

Role of courts

Courts remain central to defining and reshaping the contours of privacy rights and remedies. This role goes beyond the role of trial courts in adjudicating claims brought by regulators and private parties that seek to protect and define privacy rights and remedies; interest in these issues has been expressed at the highest levels. The Supreme Court has demonstrated recent interest on commercial privacy matters. Although it refused to take up *Spokeo, Inc v. Robins* again in 2018, in 2016, the Supreme Court held that an injury suffered under the

41 827 F.3d 262, 290 (3d Cir 27 June 2016).
42 820 F3d 482, 489-90 (1st Cir 29 April 2016).

FCRA must be sufficiently 'concrete' to find standing (discussed above). The Court held that a bare procedural violation was insufficient for proper standing. Additionally, in a November 2013 dismissal of a petition for *certiorari*, Chief Justice Roberts noted *in dicta* what issues the Court might consider when evaluating the fairness of class action remedies brought by plaintiffs challenging a privacy settlement.[43] Consumer protection regulators like the FTC and state attorneys general are becoming increasingly aggressive, both in terms of the scope of enforcement jurisdiction and the stringency of regulator expectations.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign organisations can face a federal or state regulatory action or private action if the organisation satisfies normal jurisdictional requirements under US law. Jurisdiction typically requires 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. If a foreign organisation is a publicly traded company, the SEC has jurisdiction. If an organisation is a healthcare provider, the Department of Health and Human Services has jurisdiction.

Additionally, foreign organisations must consider the residency of their data subjects. Massachusetts information security regulations apply whenever an organisation processes data of Massachusetts residents. Since Massachusetts was among the first states to enact highly detailed information security requirements, its rules have become a *de facto* consideration for national best practices.

The United States does not have a general data localisation requirement, although certain requirements do exist for government contractors. Although the United States does generally require data localisation, it requires vendor oversight to ensure reasonable standards of data care. Foreign organisations operating in the United States should know that they are the responsible party under US law even if data processing is handled by a vendor outside the United States.

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. The United States respects comity, but a foreign country's blocking statute does not trump a US legal requirement to produce information.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity has been the focus of intense attention in the United States in recent years, and the legal landscape is dynamic and rapidly evolving. Public discourse has tended to conflate distinct legal issues into a single conversation that falls under the blanket term 'cybersecurity'. Cybersecurity law and policy are more accurately described and characterised

43 Statement of Chief Justice Roberts, *Marek v. Lane*, 571 US ___ (2013).

in distinct buckets: primarily consumer or personal information on the one hand, and critical infrastructure or sensitive corporate data on the other. Of course, the same or similar safeguards provide protection in both contexts.

While the United States does not have an omnibus law that governs data security, an overlapping and comprehensive set of laws enforced by federal and state agencies provides for the security of this information. These information security safeguards for personal and consumer information, as well as data breach notification provisions, are prescribed in the federal GLBA (financial data), HIPAA (healthcare data) and 50 state laws, plus the laws of numerous US territories and districts such as the District of Columbia (for broad categories of sensitive personal information). The GLBA, HIPAA and Massachusetts state law[44] provide the most detailed and rigorous information security safeguards. The emergence of the National Institute for Standards and Technology (NIST) cybersecurity framework, as detailed below, is likely to emerge as the predominant framework under which companies undertake to ensure information security.

Fifty states and various US jurisdictions have enacted data breach notification laws, which have varying notification thresholds and requirements. These laws generally require that individuals be notified, usually by mail (although alternate notice provisions exist), of incidents in which their personal information has been compromised. These laws usually include a notification trigger involving the compromise of the name of an individual and a second, sensitive data element such as date of birth or credit card account number.

The GLBA Safeguards Rule requires financial institutions to protect the security and confidentiality of their customers' personal information, such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers. The Safeguards Rule requires companies to develop a written information security plan that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

a designate an employee to coordinate its information security programme;

b conduct a risk assessment for risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks;

c design and implement a safeguards programme, and regularly monitor and test it;

d select service providers that can maintain appropriate safeguards, contractually require them to maintain such safeguards and oversee their handling of customer information; and

e evaluate and adjust the programme in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[45]

The SEC has broad investigative and enforcement powers over public companies that have issued securities that are subject to the Securities Acts, and enforce this authority through the use of a number of statutes, including Sarbanes-Oxley. The SEC has investigated companies that are public issuers that have suffered cybersecurity incidents, including Target, and has

44 See Standards for the Protection of Personal Information of Residents of the Commonwealth (of Massachusetts), 201 CMR 17.00, available at www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

45 www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

considered theories, including that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to disclose material cybersecurity risk; 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. The SEC also enforces Regulation S-P, which implements the privacy and security provisions of the GLBA for entities subject to its direct regulatory jurisdiction (such as broker-dealers and investment advisers). In 2015, the SEC and its 'self-regulatory' counterpart, the Financial Industry Regulatory Authority, issued guidance and 'sweep' reports regarding the state of data security among broker-dealers and investment advisers.

On 21 February 2018, the SEC published new interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors. 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.

The Department of Health and Human Services 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.

In April 2015, the Department of Justice issued its own guide, Best Practices for Victim Response and Reporting of Cyber Incidents.[46] The Department noted concerns about working with law enforcement after suffering a data breach: 'Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harbouring such concerns should not hesitate to contact law enforcement.'

Several states also require companies operating within that state to adhere to information security standards. The most detailed and strict of these laws is the Massachusetts Data Security Regulation, which requires that companies maintain a written information security policy (commonly known as a WISP) that covers technical, administrative and physical controls for the collection of personal information.

In February 2013, President Obama issued Executive Order 13,636, 'Improving Critical Infrastructure Cybersecurity'. This Executive Order directs the Department of Homeland Security to address cybersecurity and minimise risk in the 16 critical infrastructure sectors identified pursuant to Presidential Policy Directive 21.[47] The Order directed the NIST to develop a cybersecurity framework, the first draft of which was released in February 2014.

46 Available at www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

47 Available at www.dhs.gov/critical-infrastructure-sectors.

The NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, and 'provides a means of expressing cybersecurity requirements to business partners and customers and help identify gaps in an organisation's cybersecurity practices'. While the framework is voluntary and aimed at critical infrastructure, 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 business proprietary data. Companies operating in highly regulated industries such as the defence industrial base, energy sector, healthcare providers, banks subject to detailed examinations by the Federal Financial Institutions Examination Council and investment firms that are regulated by the SEC are subject to detailed cybersecurity standards.

Congress cybersecurity legislation in December 2015, known as the Cybersecurity Act. This law includes CISA, which is designed to foster cyberthreat information sharing and provided certain liability shields related to such sharing and other cyber-preparedness. Specifically, CISA provides liability protection for sharing cyberthreat information with government and private parties. CISA also authorises network monitoring and other defensive measures, notwithstanding any other provision of law.

On 11 May 2017, the White House followed up on the 2016 PPD-41 with a cybersecurity executive order that requires further studies and outlines priorities for the current administration's cybersecurity efforts. The executive order calls for an assessment of critical infrastructure and seeks to build the government's cybersecurity capacities by updating old technologies and hiring more skilled technologists. It also strongly endorsed the NIST Cybersecurity Framework, requiring all agencies to use the NIST Cybersecurity Framework to manage cyberrisks. On 16 August 2017, NIST issued an updated draft of its security and privacy guidance for federal information systems, providing specific guidance on internet-of-things (IOT) devices and on how to apply this guidance outside the government sector. NIST finalised the guidance and released an updated version of its Cybersecurity Framework on 17 April 2018.

As detailed above, the FTC also increasingly plays the role of *de facto* cybersecurity enforcement agency where consumers or personal information are involved. Based on Section 5 of the FTCA, the Commission has stated that providing reasonable and appropriate information security is required as a 'fair' trade practice. State attorneys general, empowered pursuant to state-level mini FTCAs (see Sections VII.i and ii), have taken a similar approach. Essentially, every major data breach is investigated by the FTC and state attorneys general, and may also draw the attention of other regulators such as the SEC. New York's Department of Financial Services (DFS) issued a proposed rule in September, which would require banks, insurance companies and other financial service institutions regulated by New York's DFS to create and maintain a cybersecurity programme designed to protect consumers and New York's financial industry. The New York DFS rule went into full effect on 28 August 2017, requiring that all financial institutions regulated by DFS 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.

Cybersecurity remains a headline issue. In September and December 2016, Yahoo! announced that data associated with at least 500 million user accounts were stolen by what was later confirmed to be a state-sponsored actor. In December 2016, Yahoo! announced a second breach affecting 1 billion users that dated back to 2013. These two incidents are considered as possibly the largest cybersecurity breaches ever reported. The FBI announced

on 11 August 2016 that it is nearly certain that the hacking of the Democratic Party in late July was the work of the Russian government. The federal investigation of the hack revealed that, in addition to the DNC and to the Democratic Congressional Campaign Committee, other party-affiliated groups were targeted in the hack, which probably included the breach of personal email accounts of the groups and group leaders. On 20 March 2017, after the 2016 election and inauguration of President Donald Trump, the FBI confirmed that it was investigating the Russian government's interference in the 2016 election. In September 2017, the consumer reporting agency Equifax announced that the sensitive financial information of 143 million Americans had been exposed to hackers that exploited an unpatched website vulnerability. Given the pivotal role of credit bureaux such as Equifax, the ramifications of this breach may impact decision-making in the consumer financial sector.

In 2018, Yahoo! settled cybersecurity allegations brought by the SEC (for US$35 million) and by shareholders for (US$80 million).

X OUTLOOK

With regard to privacy regulation of internet, telecom and tech companies, it is still not certain in which direction new regulators appointed by the Trump administration will head. Privacy has not been an especially partisan issue in the United States to date.

Under new FTC Chairman Joseph Simons, the agency 'will hold a series of public hearings during the fall and winter 2018 examining whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy.' These hearings will include coverage of privacy and cybersecurity enforcement. Public comments have been solicited on the FTC's authority to deter unfair and deceptive conduct in privacy and data security matters, including the identification of any additional tools or authorities necessary to adequately deter unfair and deceptive conduct related to privacy and data security.

There are also indications that the White House is considering the development of a new privacy framework that may be published by a component of the Department of Commerce in the fall of 2018.

Appendix 1

ABOUT THE AUTHORS

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator 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. 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 Data Security, Privacy & Intellectual Property 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.

VIVEK K MOHAN

Sidley Austin LLP

Vivek K Mohan is senior privacy and cybersecurity counsel at Apple Inc, where he is responsible for privacy and security issues associated with Apple's products, services and corporate infrastructure. He joined Apple from the privacy, data security and information law group at Sidley Austin LLP, where he counselled clients in the technology, telecommunications, healthcare and financial services sectors. Mr Mohan is the co-editor and author of the PLI treatise 'Cybersecurity: A Practical Guide to the Law of Cyber Risk', published in September 2015. He has worked as an attorney at Microsoft, at the Internet Bureau of the New York State Attorney General (under a special appointment) and at General Electric's corporate headquarters (on secondment). For five years, Mr Mohan was a resident fellow and later a non-resident associate with the Cybersecurity Project at the Harvard Kennedy School. He holds a JD from Columbia Law School and a BA from the University of California, Berkeley.

SIDLEY AUSTIN LLP

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com
www.sidley.com

ISBN 978-1-912228-62-1