The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

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 978-1-910813-32-4

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

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 28

UNITED STATES

Alan Charles Raul, Tasha D Manoranjan 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

1 Alan Charles Raul is a partner and Tasha D Manoranjan is an associate at Sidley Austin LLP. Vivek K Mohan was previously an associate at Sidley, and is now privacy counsel at Apple Inc. His contribution to this chapter predated his work at Apple. 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.

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.

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, approximately 47 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

2 Alabama passed data breach notification legislation in the Senate in April 2016, with companion legislation still progressing through the Alabama House. If enacted, Alabama will become the 48th state to adopt a breach notification law. New Mexico and South Dakota remain the only states without legislation specifically requiring data breach notification.

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 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 year has 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. Congress has finally passed long-awaited cybersecurity legislation: the Cybersecurity Act was passed in December 2015. The new overall law 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, a number of smaller cybersecurity provisions were included in a large transportation bill, the FAST Act, signed into law on 4 December 2015. 2015 also saw the end of US intelligence agency collection of bulk phone metadata pursuant to the USA Freedom Act. More specific, targeted court orders are now required for government collection of phone metadata stored by telecommunications companies.

The Defend Trade Secrets Act (DTSA) was enacted in May 2015. This law expands access to judicial redress for unauthorised access and use of trade secrets. Before the DTSA, trade secret disputes were normally litigated between companies in state court, landing in federal court only if the government prosecuted the thief under criminal law or if another federal civil statute was relevant. 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. In passing the bill, Congress recognised that the protections of state court are no longer sufficient, given the increasing sophistication of the criminal element or even state-sponsored corporate espionage groups. Significantly, plaintiffs will also be able to seek an *ex parte* order of seizure or injunctive relief. The DTSA authorises a federal court to grant an injunction to prevent actual or threatened misappropriation of trade secrets, but such 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 'otherwise conflict[s] with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business'.

The FTC obtained a $100 million no-fault settlement from LifeLock to resolve allegations that it violated a prior FTC settlement. 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. The FCC has remained interested in robocalls, imposing a fine against Travel Club for nearly $3 million in 2015 for violating the FCC's robocall rules by robocalling over 100 consumers without their consent. Many of the consumers had registered on the national 'do not call' registry. The case evidences the FCC's increased focus on preventing robocalls.

Very significantly, the FCC adopted a major new policy defining broadband internet access service (i.e., internet service providers (ISPs)) as subject to extensive new 'common carrier' regulation and enforcement by that agency. The new rule was announced by the FCC in the Open Internet Order concerning 'network neutrality'. On 14 June 2016, a divided panel of the Court of Appeals for the DC Circuit upheld the FCC's net neutrality rules. Multiple industry petitioners, including broadband ISPs and telecommunications companies, had challenged the FCC's reclassification of broadband internet as a common carrier under Title II of the Communications Act, which allowed the FCC to regulate the throttling of service and the prioritisation of certain content providers. Going forward, this ruling will potentially provide a legal basis for further regulation of the internet by the FCC, including its customer proprietary network information (CPNI) and set-top box rules.

The FCC also released proposed rules for broadband ISPs in March. The FCC's proposed rules are aimed at implementing the privacy requirements of Section 222 of the Communications Act. The proposed rules would greatly expand a strict opt-in privacy regime. Providers would be allowed to use consumer data to market their own communications-related services, although consumers could opt-out of advertisements for communications-related products and services that are unrelated to the consumers' services. Opt-in consent would be required to use customer data for any other purpose (i.e., advertisements for non-communications-related products and services) or to share data with third parties not related to the delivery of the service. The proposed regulations would also adopt a general data security standard that would require providers to adopt risk management and data security standards, and impose onerous and uniquely broad data breach notification requirements. The FCC has been increasingly active in enforcement, including through the imposition of a $25 million penalty against a major telecommunications provider in connection with a data breach affecting consumer phone records. Smaller carriers have also been subjected to significant penalties for alleged privacy and data security violations.

On 1 June 2015, Section 215 of the Patriot Act expired. This provision was used to justify the controversial National Security Agency (NSA) programme collecting bulk phone metadata. While the programme was fully disclosed in 2006 in the media, leaks of NSA documents by former NSA contractor Edward Snowden caused an international furore.

Congress subsequently reauthorised the lapsed provision, but in a modified form limiting the NSA to engage in automatic bulk collection of metadata. Broader efforts at surveillance reform have little momentum.

States have continued to push privacy and cybersecurity initiatives forward. Tennessee, California, Oregon and Rhode Island have updated their breach notification laws. Tennessee is the first state to remove the safe harbor for encrypted data: now notification to affected individuals may be required even if the data subject to the security incident was encrypted. However, a risk analysis is still permitted under the new law, such that encryption can be considered in evaluating whether notification is required. California expanded the definition of 'personal information' to include data obtained from an automated licence plate recognition system. This amendment will require entities using licence plate recognition systems to adopt reasonable safeguards to avoid unauthorised use or disclosure. Additionally, the California Governor formed a the California Cybersecurity Integration Center (Cal-CSIC) to 'reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state.' Cal-CSIC is housed within the California Office of Emergency Services, and will work with the existing California Threat Assessment System and the US Department of Homeland Security to improve information sharing and communication with local, state and federal agencies. Cal-CSIC will also establish a multi-agency Cyber Incident Response Team to lead efforts to detect, report and respond to cybersecurity threats. Oregon amended its breach notification law to require Attorney General notification and to cover breaches of health information. Rhode Island overhauled its breach notification law to strengthen notification requirements and add affirmative data security obligations.

State legislation related to social media privacy also continues to be popular. Delaware enacted a privacy bill protecting employee social media accounts, and Maine enacted an employee social media privacy law. Other significant state initiatives include New Hampshire's enactment of a bill to protect student data online. Delaware also enacted a Student Data Privacy Protection Act, as well as an Online Privacy and Protection Act. Wisconsin criminalised the unauthorised placement of GPS devices.

The EU–US Privacy Shield was announced in February to replace the Safe Harbor programme after it was invalidated by the European Court of Justice. It was adopted in July, and the Department of Commerce began accepting Privacy Shield certifications on 1 August.

The Supreme Court addressed privacy issues this year. In *Spokeo, Inc v. Robins*, the Supreme Court held that an injury suffered under the Fair Credit Reporting Act (FCRA) must be sufficiently 'concrete' to find standing. The Court held that a bare procedural violation was insufficient for standing, and a real, *de facto* injury was necessary for a successful lawsuit, even where Congress has authorised private litigation. A 'bare' statutory violation would not suffice. The Court found that a particularised injury without a concrete injury is insufficient for standing. However, the Court recognised that an intangible injury could potentially be real and sufficient, even in the absence of pecuniary or other tangible harm. The Court acknowledged that '[t]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury-in-fact'. However, it is the plaintiffs' burden to plead and establish a concrete injury. Thomas Robins had sued Spokeo for wilful violations of the FCRA, alleging that inaccurate information disclosed about him on Spokeo's website harmed his employment opportunities. The Court's decision came out in May 2016, and did not determine whether Robins had suffered a concrete injury, instead remanding the case to the Ninth Circuit for consideration.

In data breach litigation, cases have gone in different directions, but plaintiffs have had a difficult time prevailing where they cannot allege that the criminal actually misused stolen data. On one hand, Michaels won a dismissal of claims in December 2015 related to its 2014 breach based on the plaintiff's failure to allege actual injury. That same month, Target agreed to pay $39 million to card issuers for claims related to a 2013 breach. In another case, Genesco, which experienced a breach in 2010, is claiming that Visa improperly collected $13.3 million in Payment Card Industry Data Security Standard fines because Visa provided no evidence that specific card information was stolen as a result of the breach. In another closely watched breach case, a California federal judge consolidated 32 cases brought by T-Mobile customers against Experian for negligence in a data breach affecting 15 million people. Amid this uncertainty, large-scale breaches continue to occur, with an announcement the FBI that the Russian government hacked the Democratic National Committee (DNC).

i FTC actions

The FTC scored a major victory in 2015 with regard to the scope of cybersecurity authority in federal court. The Third Circuit Court of Appeals affirmed the Commission's authority to regulate data security in a much-anticipated ruling, *Federal Trade Commission v. Wyndham Worldwide Corp*.[3] The Third Circuit held that the FTC has the authority to bring data security actions based on the general mandate of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. The *Wyndham* decision confirmed that the FTC was authorised to sue companies for engaging in 'unfair' practices when they do not provide 'reasonable' cybersecurity for consumer data in their possession. The Third Circuit's decision in *Wyndham*, upholding the FTC's data security authority, is probably the most important consumer protection-related development for the Commission over the past few years. The FTC has remained active on these issues, both in issuing guidance as well as in bringing enforcement actions.

In January 2016, the FTC published a 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.

In June 2015, the FTC published 'Start with Security: A Guide for Business' to guide companies on data security. This guide contains 10 best practices for addressing issues of data security based on lessons learned from the FTC's more than 50 data security actions to date. In particular, the guide identifies 'vulnerabilities' that could affect businesses – big or small – and provides 'practical guidance on how to reduce the risks [those vulnerabilities] pose'. The guide's suggestions include:

a start with security;
b control access to data sensibly;
c require secure passwords and authentication;
d store sensitive personal information securely and protect it during transmission;

3 *Federal Trade Commission v. Wyndham Worldwide Corp*, No. 14-3514 (3rd Cir 24 August 2015).

e segment your network and monitor who is trying to get in and out;
f secure remote access to your network;
g apply sound security practices when developing new products;
h make sure your service providers implement reasonable security measures;
i put procedures in place to keep your security current and address vulnerabilities that may arise; and
j secure paper, physical media and devices.

On 20 December 2015, Oracle Corporation agreed to settle deception allegations lodged by the FTC regarding Oracle's Java Platform. This platform is ubiquitous; more than 850 million personal computers have it installed. Oracle provides frequent updates to software as part of its customer service. The allegations detailed that Oracle represented to consumers that, by installing the updates, the user would keep his or her system 'safe and secure'. Allegedly, earlier versions of Java contained security flaws, and Oracle knew of these deficiencies. While the newest updates deleted other, more recent versions of Java, the allegations state that updates failed to remove older deficient versions that could compromise the security of a user's system. The FTC alleged that Oracle's statements regarding the safety of a user's system were thus allegedly misleading and a violation of Section 5 of the FTC Act. Oracle entered into a consent decree with the FTC, agreeing to provide notice to consumers and to submit to FTC oversight. Of note, Lesley Fair – the lead FTC attorney on the case – cited the FTC's business brochure, 'Start with Security', as relevant guidance for Oracle, emphasising the importance the agency places on its guidance publications.

LifeLock, a company specialising in identity theft protection services, entered into a no-fault settlement agreement with the FTC under which it will set aside $100 million to resolve allegations it violated a July 2010 FTC settlement related to deceptive claims about its identity-theft protection services. The 2015 settlement addresses the company's alleged failure to implement reasonable security practices for customer data and alleged failures to abide by promises to alert consumers 'as soon as' there were indications of potential identify theft. The $100 million represents the largest monetary award in an FTC data security enforcement action. In a press release, Chair Ramirez highlighted that '[t]he fact that consumers paid Lifelock for help in protecting their sensitive personal information makes the charges […] particularly troubling'. Of the $100 million, $68 million may be used for consumer redress unless a representative of the FTC determines that redress is impracticable.

The Court of Justice of the European Union (CJEU) has had an outsize impact on privacy and data protection issues that impact 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. The US fallout from the CJEU's 'right to be forgotten' ruling remains to be seen, but the FTC's involvement in both issues is notable.

Speaking at a US Council for International Business event, FTC Commissioner Julie Brill pointed to last year's decision by the CJEU regarding the right to be forgotten as something that could inform a 'right to obscurity' in the United States. The EU decision required search engines to delete links harmful to an individual's privacy interest when there is no other compelling public service. The broad EU implementation would face certain First Amendment challenges in the United States, but as Commissioner Brill pointed out, certain aspects of such a right are already US law. As an example, she pointed to the FCRA, which prohibits certain information from being used to inform credit reports after a certain

period, and that US law also allows expungement of criminal records in some circumstances. Commissioner Brill indicated that the right to obscurity could be well applied to information held by data brokers. The implementation of the right to obscurity in that case could require brokers to allow individuals to see information in their files and either correct or expunge it.

The CJEU opinion on the US–EU Safe Harbor came in October 2015 despite significant efforts by EU and US officials to negotiate on a set of agreed changes to the agreement; the final points of negotiation were on national security issues, which ultimately formed the crux of the CJEU decision. The FTC has a dual mandate – consumer protection and competition – and privacy issues have permeated across the internal walls. The Director of the FTC Bureau of Competition, Deborah L Feinstein, has indicated that privacy is growing as a part of the Commission's merger reviews, as the issue is becoming more important to consumers. Privacy could be considered as a form of actionable non-price competition. Although the FTC has yet to challenge a transaction because it would impede competition in privacy technology, such an action would not be entirely without precedent. The Commission recognised in 2007 that mergers may adversely affect consumer privacy. Additionally, the European Commission examined the issue in considering a merger between TomTom and TeleAtlas in 2008. This increased focus on privacy competition may incentivise companies to undertake due diligence of both their own and target acquisitions' privacy practices and policies, and consider how privacy protections may be strengthened as part of the merger process.

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 FTC Act' 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.

The FTC Act

Section 5 of the FTC Act prohibits 'unfair or deceptive acts or practices in or affecting commerce'. While the FTC Act 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, 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 1973–74 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.

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,[4] cyberstalking,[5] data disposal,[6] privacy policies, security breach notification,[7] employer access to employee social media accounts,[8] unsolicited commercial communications[9] and electronic solicitation of children,[10] 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.[11] The combined legislative and enforcement authority of the federal and state governments ensures that the policy leadership articulated at the federal level – like the White House's 2012 Privacy Report – can be implemented effectively in practice.

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.[12] 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

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

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

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

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

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

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

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

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

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

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 such 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. 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 e-mail messages. Generally, a company is permitted to send commercial e-mails to anyone under CAN-SPAM, provided these conditions are met: the recipient has not opted out of receiving such e-mails from the company, the e-mail identifies the sender and the sender's contact information, and the e-mail has instructions on how to easily and at no cost opt out of future commercial e-mails 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, until recently, 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 FTC Act 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.[13]

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.[14] 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

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

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

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 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.[15]

The FCC entered a $595,000 settlement with Cox Communications for Cox's failure to protect its customers' personal information during a breach. A hacker allegedly accessed the personal information of 61 Cox subscribers during a 2014 breach, and shared the information on social media sites and with other hackers. This settlement was the FCC's

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

first security enforcement action with a cable company, and includes significant compliance programme requirements. It is another reminder that the FCC is now an aggressive player in the cybersecurity arena, even for relatively minor incidents, and that the CPNI rules include breach notification requirements.

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.[16]

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 e-mail.

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 e-mail 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:

> ***Privacy Policies for Websites or Online Services***
>
> *California's Online Privacy Protection Act requires an operator […] to post a conspicuous privacy policy on its Web site 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 Web site [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.*

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

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 Web sites 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.[17]

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.[18]

IV INTERNATIONAL DATA TRANSFER

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 that are subject to data transfer restrictions set forth by other countries. Last year's 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.

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

18 Calif Bus & Prof Code Sections 22580–22582.

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 US 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[19] works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[20] In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.[21]

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management[22] 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.

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.

---

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

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

21 See 'APEC Overview', Chapter 2.

22 Bamberger, Kenneth A and Mulligan, Deirdre K, '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.

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.

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.[23]

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

23 *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 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.

(the contents of e-mails) stored in Ireland to law enforcement in the United States.[24] However, in July 2016, the Second Circuit overturned the District Court's decision, holding that the government cannot force Microsoft to turn over customer e-mails stored outside the US.[25] The issue in the case concerns whether a search warrant served in the United States could authorise the ex-territorial 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 e-mails 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 has 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 US. This decision may also help protect the interest of US companies to provide global cloud-computing services.

In another significant case, the Justice Department attempted to use the All Writs Act to force Apple to help it unlock the iPhone used by Syed Rizwan Farook, one of the shooters in the San Bernardino terrorist attack. However, the Department of Justice dropped the case after the FBI reportedly discovered an alternative means to access the phone by contracting with and paying $1 million to a private hacking company. It is unclear how investigators bypassed Apple's security measures, or what FBI agents learned about the plot from the content they were able to review. Reportedly, the government has decided not to disclose the vulnerability to Apple. The decision averts a judicial opinion on whether the All Writs Act permits a court to order a company to provide technical assistance – which includes compelling a company to write code – for use in unlocking encrypted devices. Many in the tech community had warned that a decision in favour of the FBI would set a dangerous precedent, violating companies' constitutional rights and weakening privacy and security for users around the world.

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 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

24 *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp*, 5 F Supp 3d 466.

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

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, bureaux 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]

As FTC Commissioner Julie Brill has 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, including states such as California, Connecticut and Maryland.

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 38).

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

The mini-FTC Acts 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.

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 its long-awaited report on the internet of things, 'Internet of Things: Privacy & Security in a Connected World', last year. 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 FTC Act, 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

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.

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. 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.

Settlement for misrepresenting Asia-Pacific Economic Cooperation (APEC) participation

The FTC brought an action against a company for claiming participation in APEC's Cross Border Privacy Rules (CBPR) system. The company, Very Incognito Technologies, Inc, is a hand-held vaporiser manufacturer doing business as Vipvape. On 4 May, Vipvape agreed to settle charges that it improperly represented itself as a participant in the APEC CBPR system, which requires businesses to develop internal rules on cross-border data protection. Vipvape is 'prohibited from misrepresenting its participation, membership or certification in any privacy or security program sponsored by a government or self-regulatory organization' according to the proposed consent order.

FTC finds LabMD's security practices unreasonable

On 29 July, the FTC issued a final order in a case that began with an FTC complaint filed three years ago against LabMD, alleging unreasonable data security practices that exposed sensitive medical and financial data. LabMD claimed the FTC 'lacked statutory authority to regulate or bring enforcement actions with respect to data security practices', and that LabMD's data security practices 'did not cause and are unlikely to cause substantial injury to consumers'. The FTC's Chief Administrative Law Judge (ALJ) ruled in favour of LabMD, and dismissed the complaint for failing to establish that LabMD's computer data security practices caused or were likely to cause substantial consumer injury. In a unanimous opinion, issued 29 July, the FTC reversed the ALJ ruling and concluded that LabMD data security practices were unreasonable. In brief, the FTC found that: 'LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system. Among other things, it failed to use an intrusion detection system or file integrity monitoring; neglected to monitor traffic coming across its firewalls; provided essentially no data security training to its employees' and never deleted any of the consumer data it had collected.'

Unless reversed on appeal, LabMD will be subject to an order governing its data security practices that requires LabMD to establish, implement and maintain a comprehensive information security programme, and to obtain biennial assessments of that programme for the next 20 years. Additionally, LabMD is required to notify consumers and health insurance companies about the data breach and to comply with certain recordkeeping provisions. The company has said that the FTC's decision suggests that anything that could theoretically be hacked would be 'vulnerable' and subject to data security enforcement action.

Financial and medical information

The SEC Office of Compliance Inspections and Examinations issued guidance on cybersecurity and announced examination priorities, taking multiple steps to heighten its enforcement presence for cybersecurity matters. 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. The Office of Compliance Inspections and Examinations 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.

Settlement with securities firm

A securities firm agreed to pay $1 million for failing to protect internal client information from improper employee access. According to the company's 8 June settlement with the SEC, Morgan Stanley had controls in place on its internal data portals, but for around 13 years, the company allegedly did not effectively secure two of those portals or monitor employee access to information. Those alleged failures enabled a 2014 data breach linked to former employee Galen Marsh, who ran reports on thousands of clients he never worked with, uploaded client information to private servers and did not protect the information from hackers. A separate SEC action barred Marsh from working in the industry for at least five years, at which point he may apply for reinstatement. Marsh was also sentenced to three years of probation and fined $600,000 after pleading guilty to unauthorised computer access in earlier proceedings. To the company's knowledge, no fraud has been connected with the data theft.

Mini-FTC Act 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-FTC Acts. Two illustrative examples are summarised below.

Google Street View settlement

Thirty-eight state attorneys general reached a $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 July 2013, the New Jersey Attorney General's Office announced a $1 million settlement with online advertising company PulsePoint concerning allegations that the company

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.

bypassed web browser privacy settings to collect information on consumers' online browsing habits to serve millions of online advertisements.[40] In November 2013, 37 states settled an investigation with Google involving essentially the same allegations for $17 million.[41]

Robocalls

The FCC remains interested in preventing robocalls. As previously mentioned, the FCC imposed a fine against Travel Club in 2015 for nearly $3 million for violating the FCC's robocall rules by making 185 unsolicited, prerecorded advertising messages (a form of robocalls) to the mobile and home phones of 142 consumers. These robocalls were made without their consent, and the consumers had never done business with Travel Club previously. Many of the consumers had registered on the national do not call registry.

In another recent significant post on its business blog, the FTC warned businesses that placing robocalls without first obtaining signed, written consent directly from consumers could subject them to increased scrutiny under the Telemarketing Sales Rule (TSR). In answers to frequently asked questions included in the post, the FTC emphasised that robocalls cannot go to any number, whether on the do not call registry or not, without first obtaining written consent from the consumer – in what some might consider an expansive reading. This consent needs to include the consumer's phone number as well as a clear and conspicuous statement that the consumer gives the specific company, and not a third-party affiliate, permission to make robocalls. The blog entry also reminds entities that if a call list is obtained from a lead generator, that list should still be scrubbed against the do not call registry. The post also cautioned that the TSR's 'business relationship exception' can only be used when the telemarketing calls are live.

The FCC also 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.

Unsolicited faxes

The FCC imposed a $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.

40 Press release, 'New Jersey Division of Consumer Affairs Obtains Million-Dollar Settlement With Online Advertising Company Accused of Overriding Consumers' Privacy Settings Without Consent' (25 July 2013), available at nj.gov/oag/newsreleases13/pr20130725a.html.

41 Press release, 'A.G. Schneiderman Announces $17 Million Multistate Settlement With Google Over Tracking Of Consumers' (18 November 2013), available at www.ag.ny.gov/press-release/ag-schneiderman-announces-17-million-multistate-settlement-google-over-tracking.

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'.[42] 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.[43]

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; in *Spokeo, Inc. v. Robins,* the Supreme Court held that an injury suffered under the FCRA must be sufficiently 'concrete' in order 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.[44] Consumer

42 -- F3d --, 2016 WL 3513782, at *21 (3d Cir 27 June 2016).

43 820 F3d 482, 489-90 (1st Cir 29 April 2016).

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

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 information security requirements, it has become a *de facto* national standard.

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 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 47 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[45] 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.

Forty-seven states 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.[46]

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 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

45 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.

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

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.

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.[47] 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.[48] The Order directed the NIST to develop a cybersecurity framework, the first draft of which was released in February 2014. 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 *de facto* requirement 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 finally passed long-awaited cybersecurity legislation in December 2015, known as the Cybersecurity Act. As previously mentioned, the new 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, not withstanding any other provision of law. In April, President Obama created the Commission on Enhancing National Security to make recommendations

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

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

for the public and private sectors to improve cybersecurity. President Obama announced 12 appointees to this Commission, who have experience in both the public and private sectors. The appointees are drawn from backgrounds in, *inter alia*, academia, national defence, financial services, telecommunications and payment processing.

The White House released the Presidential Policy Directive on Cyber Incident Coordination (PPD-41) in July. In the wake of the hacking of the DNC, the President announced PPD-41, which codifies lines of responsibility for cyber incidents. The Directive defines cyber incidents to include vulnerabilities that could potentially be exploited, but limits significant cyber incidents to those 'likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people'. Regardless of whether the cyber incident occurs in the private or public sector, for significant incidents, the Directive provides that the Department of Justice will take the investigatory lead, with the Department of Homeland Security leading on asset protection, the Office of the Director of National Intelligence taking the lead on intelligence support activities. The National Security Council's Cyber Response Group will lead national policy coordination, and a 'Unified Coordination Group' including 'Federal lead agencies for threat response, asset response, and intelligence support' will coordinate national operations with private sector entities. The relevant agency will coordinate the government's efforts to understand potential business or operational effects for private sector critical infrastructure. Field-level federal representatives may be placed within affected private entities to coordinate efforts.

The Directive notes guiding principles of enhanced coordination and cooperation between government sectors and private entities to better safeguard national interests and improve the US response to such incidents. The Directive also emphasises a guiding principle of 'respecting affected entities', explaining that the government will defer to private entities to notify other affected private entities and the public, and will coordinate with the affected entities if a public statement is necessary to serve the government interest. The Department of Homeland Security and the Department of Justice will maintain and update an information sheet detailing how private entities may contact the government about an incident.

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 FTC Act, 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-FTC Acts (see Sections VII.i and ii, *supra*), 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.

Cybersecurity remains a headline issue. In September, Yahoo announced that data associated with at least 500 million user accounts were stolen by what it believes to be a state-sponsored actor. This is being reported as possibly the largest cybersecurity breach ever. The FBI announced on 11 August 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 likely included the breach of personal e-mail accounts of the groups and group leaders. The FBI has not publicly released the findings.

X OUTLOOK

There may be more and increasing convergence between US and EU privacy regimes than is commonly believed. Focus on data protection is unquestionably growing throughout the United States, and unlike many other regulatory issues, privacy has not become mired in Democrat–Republican partisan battles.

No system of data protection anywhere in the world has produced more legal settlements, judgments, consent decrees and, perhaps most importantly, corporate compliance programmes that seek to protect and ensure privacy than the United States. Even though every Member State of the European Union has a data protection authority, they vary greatly in terms of aggressiveness and resources. Indeed, a recent study found that the very 'unpredictability' of the FTC's broad mandate proves a stronger incentive to invest in privacy than the European regulators' more siloed mandate.[49]

The FTC noted in recent testimony to Congress that enforcement actions have focused on 'protecting financially distressed consumers from fraud, stopping harmful uses of technology, protecting consumer privacy and data security, prosecuting false or deceptive health claims, and safeguarding children in the marketplace'.[50] The FTC's approach to emerging issues can be informal and inclusive, allowing for productive working relationships that have helped shape the development of products and services in a way that protects consumers while allowing the government to better understand the technology. The use of public meetings and workshops, such as a November 2013 event on the internet of things, to help identify cutting-edge issues raised by technology, is an example of such an approach.[51] The FTC has noted that issues likely to capture its privacy-related attention in the years ahead include big data, mobile technologies and connected devices, and protection of sensitive data, particularly health information and information that relates to children. Entities known as 'data brokers' have captured the attention of the FTC, and are likely to be targets for future enforcement and oversight. If nothing else, the robust public debate surrounding these issues is indicative of engaged, capable policymakers. Companies have responded to regulation and oversight by expanding privacy leadership functions, redoubling compliance and training efforts, and engaging in proactive and ongoing dialogues with federal and state regulators.

At the same time, cybersecurity continues to be an issue of intense focus for the government and private sector alike. This trend is likely to intensify in the coming years, as technology develops and changes and puts further strain on existing laws. Congressional gridlock has stymied reform on otherwise non-partisan issues, but as the post-Snowden

49 Bamberger and Mulligan, 2011 (see footnote 30).

50 Id.

51 Prepared Statement of the Federal Trade Commission on 'The FTC at 100: Where Do We Go From here?' before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade (December 2013).

clamour fades, it is possible that legislation will come to pass to enable further collaboration between the private and public sector, and provide clearer reporting and notification requirements, eclipsing the messy state model that exists and is in use today.

Issues related to intellectual property theft are likely to continue to rise to the top of the international diplomacy agenda for the United States as its competitive position risks erosion from China and other such alleged cyber-intruders. Nation–state level interactions on these issue are increasingly likely to include privacy, as the FBI identified Russia as the party responsible for hacking the DNC.

Surveillance issues are likely to continue to be a sticking point between US and European counterparts as the explosion of cloud data centres is likely to continue to prove to be a point of tension with regard to requests for information by the United States government.

Investment in the protection of computer and communications systems is likely to be a continued regulatory focus, as agencies – and companies – seek to determine and understand how to balance the costs and benefits of imposing information security requirements and reporting. Moreover, implementation of the NIST cybersecurity framework may emerge as a *de facto* requirement for companies. While the broader cybersecurity outlook is unclear, it is certain that intervening factual and technological developments will continue to propel this field to the front of the national consciousness for reasons related to surveillance, competitiveness and intellectual property theft, or to personal security when information is compromised (such as through retail breaches).

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, data security and information law 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 has also served on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President, and currently remains an *ex officio* member. 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.

TASHA D MANORANJAN

Sidley Austin LLP

Tasha Manoranjan is an associate in Sidley Austin's Litigation practice in the Washington, DC office, frequently supporting the privacy, data security and information law practice group. Ms Manoranjan earned her law degree at Yale Law School, where she served as the features editor and book reviewer for the *Yale Journal of International Law*, chair of the South Asian Law Students Association and community enrichment chair of the Women of Color Collective. While at Yale, Ms Manoranjan wrote a paper entitled 'Beaten but not Broken: Tamil Women in Sri Lanka', which was subsequently published at 11 *Georgetown Journal*

of International Affairs 139 (2010). Ms Manoranjan received her BA, *magna cum laude*, in justice and peace studies from Georgetown University's School of Foreign Service. Before joining Sidley, Ms Manoranjan worked at the Department of Justice Human Rights and Special Prosecutions Section, and at an advocacy group working on human rights in Sri Lanka.

VIVEK K MOHAN

Sidley Austin LLP

Vivek K Mohan is privacy 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
tmanoranjan@sidley.com