The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 21

UNITED STATES

Alan Charles Raul, Tasha D Manoranjan and Vivek Mohan[1]

I OVERVIEW

Though not universally acknowledged, the United States' commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The United States' 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, '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 the 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

1 Alan Charles Raul is a partner and Tasha D Manoranjan and Vivek Mohan are associates at Sidley Austin LLP. 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.

professors astutely noted that '[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […] the right "to be let alone"'. In 1974, Congress enacted the federal Privacy Act, regulating government databases, and found that 'the right to privacy is a personal and fundamental right protected by the Constitution of the United States'. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices that have been incorporated in many other data protection regimes, including the European Union's 1995 Data Protection Directive.

The US has also led the way for the world not only on 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 notification by first requiring in 2003 that companies notify individuals whose personal information was compromised or improperly acquired. Since then, approximately 47 states, the District of Columbia and other US jurisdictions, and the federal banking, health-care and communications agencies have also required companies to provide mandatory data breach notification to affected individuals, and 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 US. Moreover, there is no designated central data protection authority in the US, though the Federal Trade Commission (FTC) has essentially assumed that role for consumer privacy. The FTC is independent of the President, and is not obliged (though it is encouraged) to respect the Administration's perspective on the proper balance between costs and benefits with respect to protecting data privacy.

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

The dynamic and robust system of privacy governance in the United States marshals the combined focus and enforcement muscle of the US Federal Trade Commission, state attorneys general, the Federal Communications Commission, the Securities and Exchange Commission, 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 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

As with nearly other area of recent legislative activity in Washington, Congress has not been able to act on privacy, consumer data security, data breach notification or cybersecurity legislation. While the Administration of President Obama has called upon Congress to enact a 'Consumer Privacy Bill of Rights' and legislation to help protect cybersecurity for 'critical infrastructure', partisan gridlock, as well as concern about over-regulating the private sector, has stalled action. The congressional stalemate was considerably shaken up, however, when former National Security Agency (NSA) contractor Edward Snowden leaked information regarding US government surveillance programmes to *The Guardian* and *The Washington Post* in the summer of 2013. This sparked a media frenzy around various NSA surveillance programmes. Some of the allegations concerned unauthorised surveillance of US citizens or foreign intelligence targets within the United States, while others suggested widespread surveillance outside the US.

As a result of these disclosures, foreign governments, including within the European Union, expressed concern regarding the breadth of NSA surveillance outside the United States. For example, the EU Article 29 Working Party sent a letter to EU Justice Commissioner Viviane Reding suggesting a possible investigation of violations by the US of the EU's data protection rules.[2]

The media and political firestorm surrounding the Snowden disclosures has led the executive branch to introduce proposals regarding NSA and commercial data collection processes. In addition to its proposals for reforms of the government's bulk metadata surveillance, the White House has also issued reports and recommendations for data collection in the private big data sector. Following closely on this, on 29 May the FTC issued a much anticipated report on big data that heavily criticised the lack of transparency in the data brokering industry, offered recommendations for consumer control of information and advocated for broad legislation that would not only create obligations for analytics companies, but also for retailers that may provide them with information. Significantly, however, the report does not suggest that any current data broker practices are illegal under existing law.

2 See Jacob Kohnstamm, Chairman of EU Article 29 Working Party, letter to Viviane Reding (13 August 2013), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf.

Cybersecurity remains a hot topic, although expectations for congressional action remain uncertain. Legislative action in the states continues, with Kentucky becoming the 47th state to have passed data breach notification legislation. Several states have also amended existing laws to expand breach obligations.

FTC actions

The FTC announced on 21January 2014 that it had entered into no-fault consent orders with 12 companies that allegedly claimed they were in compliance with the US–EU and US–Switzerland Safe Harbor programmes when in fact their certifications had lapsed. The agreement covers several large businesses, including three NFL football teams and Level 3 Communications LLC, one of the largest internet service providers in the world. The Safe Harbor programme requires companies to annually re-certify their compliance with the Safe Harbor framework. The FTC charged that by including statements in their privacy policies or posting certification notices that falsely indicated current compliance, these companies violated Section 5 of the FTC Act, which prohibits deceptive business practices. The settlements included no allegations of substantive violations of the Safe Harbor framework.

The FTC also brought an action against Jerk.com in April 2014 for allegedly deceptive practices. Jerk.com allegedly obtained the personal information of Facebook users and created profiles of people labelled 'Jerk' and 'not a Jerk.' Jerk.com then offered consumers the opportunity to pay US$30 to revise their profiles. The FTC alleged that such practices were misleading because the website stated that other Jerk.com users had created such profiles whereas most of the information had been pulled directly from Facebook by the operators of Jerk.com. In total, the FTC alleges that Jerk.com collected profiles on more than 73 million people, much of which had been designated as private by the users on Facebook. The FTC sought an order prohibiting such practices, including the use of personal information that is improperly obtained.

Interestingly, this case indicates that unauthorised scraping may be challenged not only by the website from which data is collected, but by regulators. The FTC's charges specifically alleged that the company 'harvested personal information from Facebook', and in the FTC's press release, they specifically noted that they were 'seeking an order barring the defendants' deceptive practices, prohibiting them from using the personal information they improperly obtained, and requiring them to delete the information'. The complaint also cited the restrictive authorisation terms of the social media site's platform agreement.

The FTC settled charges with Snapchat in May 2014 over the company's alleged deceptive privacy and confidentiality marketing promises. According to the complaint, the company, which currently transmits over 700 million messages back and forth each day, marketed its messaging services by telling users that the messages 'disappear forever', while in reality, the messages can be saved in several ways. In addition, the FTC alleged that Snapchat transmitted users' location data and transmitted sensitive information like address book contacts although the company told consumers it did not collect such information. The settlement prohibits Snapchat from misrepresenting how it maintains the privacy and confidentiality of user information and the company will also have to start a privacy programme that will be independently monitored for 20 years. If the company does not comply, it could face fines. The company has said it has resolved most

of these concerns over the last year and has improved the wording of its privacy policy, app description, and in-app just-in-time notifications.

In July 2012, following a significant data breach affecting hotel guest information, the FTC sued Wyndham Worldwide Corporation for failure to maintain reasonable and appropriate security measures. Wyndham, a hotel chain and licensing company that suffered at least three data breaches between 2008 and 2010, challenged the FTC's authority to bring an enforcement action under the unfairness prong of their Section 5 authority. In April 2014, a federal district judge in New Jersey rejected Wyndham's motion to dismiss, holding that the FTC could use its general, and flexible, 'unfairness' authority to enforce against companies that cause consumer and business harm because of weak data security systems. The court also ruled it was not necessary for Congress to provide express data security authority, or for the FTC to publish regulations specifying in detail what security practices would be deemed reasonable and appropriate. The case is currently on appeal.

The Puerto Rico Health Administration issued an unprecedented US$6.8 million fine in February 2014 against Triple-S Salud Inc, a Puerto Rican licensee of Blue Cross Blue Shield of Puerto Rico that handles managed care for Medicare enrollees. Triple-S admitted to accidentally sending out pamphlets with visible claim numbers to 70,000 Medicare Advantage customers.

II REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The US has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk: financial, insurance and medical information; information about children and students; telephone, internet and other electronic communications and records; credit and consumer reports and background investigations, at the federal level, and a further extensive array of specific privacy laws at the state level. Moreover, the US is the unquestioned world leader in mandating information security and data breach notification, 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, and each state's 'little FTC Act' analogue, comes in to 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 US. It should also be noted that 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 US. 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.

FTC Act

Section 5 of the Federal Trade Commission Act (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: (1) there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and (2) 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 of 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: (1) transparency and control, giving meaningful disclosure to consumers, and offering consumers choice about information collection; (2) maintaining data security, and limiting data retention; (3) express consent before using information in a manner that is materially different from the privacy policy in place when the data was collected; and (4) 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 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 US 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 US 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 Children's Online Privacy Protection Act of 1998, the Health Insurance Portability and Accountability Act of 1996, the Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act or GLBA), the Fair Credit Reporting Act, the Electronic Communications Privacy Act, the Communications Act (regarding consumer proprietary network information) 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,[3] cyberstalking,[4] data disposal,[5] privacy policies, security breach notification,[6] employer access to employee social media accounts,[7] unsolicited commercial communications[8] and electronic solicitation of children,[9] to name but a few.

California is viewed as a leading legislator in the privacy arena, and its large population and high-tech sector means that the requirements of California law receive particular attention and often have *de facto* application to businesses operating across the United States.[10] The combined legislative and enforcement authority of 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 government, academics, and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively-developed accountability programmes establish expected practices for use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. This approach has had notable success, such as the development of the 'About Advertising' icon by the Digital Advertising Alliance and the opt-out for cookies set forth by the Network Advertising Initiative.[11] Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. The same is true for companies that publish privacy policies – a company's failure to comply with its own privacy policy is a quintessentially deceptive practice. It should also be noted

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

4 See www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx.

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

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

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

8 See www.ncsl.org/research/telecommunications-and-information-technology/unsolicited-commercial-communication-laws.aspx.

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

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

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

that various laws require publication or provision of privacy policies, including for example, the GLBA (financial data), HIPAA (health data) and California law (websites collecting personal information). In addition, voluntary membership or certification in various self-regulatory initiatives also requires posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on such policies.

ii General obligations for data handlers

There is no requirement to register databases in the United States. Depending on the context, data handlers may be required to provide data subjects with pre-collection notice, and the opportunity to opt out for 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 US 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 emails 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 a 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. Federal Communications Commission regulations govern the collection and disclosure of certain location tracking by the telecommunications providers (generally speaking, telephone carriers). Additionally, the FTC and California have issued best-practice recommendations for mobile apps and mobile app platforms.

The Department of Commerce's National Telecommunications and Information Administration led a multi-stakeholder negotiation to develop a code of conduct for mobile app privacy. The draft code of conduct issued July 2013 is available online.[12]

iv Specific regulatory areas

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

Federal legislation

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 recent 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 Fair Credit Reporting Act, along with the general unfair and deceptive acts and practices standards under the FTC Act and the Children's Online Privacy Protection Act 1998 (COPPA), which imposes affirmative privacy and security duties on entities that collect personal information from children under 13 years of age.

The Financial Services Modernization Act of 1999 or 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 Fair Credit Reporting Act (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 credit worthiness, 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

12 Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices, available at www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf (last accessed 4 August 2014).

information, and limits the use of consumer reports to permissible purposes, such as employment and extension of credit or insurance.[13]

Health-care privacy

For health-care privacy, agencies within the Department of Health and Human Services administers and enforces the Health Insurance Portability and Accountability Act (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, health-care clearing houses, and health-care providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.

'Protected health information' is defined broadly as 'individually identifiable health information […] transmitted or maintained in electronic media' or in 'any other form or medium'. 'Individually identifiable health information' is defined as information that is a subset of health information including demographic information that 'is created or received by a health care provider, health plan, employer, or health care clearinghouse'; and '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 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 Federal Communications Commission, the Department of Justice and, to a considerable extent, private plaintiffs can enforce the data protection

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

14 Available at www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf.

standards in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and various Communications Acts, which include specific protection for 'customer proprietary network information' such as telephone call records.

The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communication 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 cyber-criminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks.

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, and obtain verifiable parental consent before collecting personal information from children, and other actions.[15]

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 email communications and internet access, phishing, spyware, security breaches, spam, and event data recorders. California is viewed as the leading legislator in the privacy arena, with many other states following its privacy laws. State attorneys general also have concurrent authority with the FTC or other federal regulators under various federal laws, such as COPPA, HIPAA and others.

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

> ***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*

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

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.

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.[16]

Children's online privacy

California prohibits websites directed to minors from advertising products based on information specific to that minor. The law also requires the website operator to permit a minor to request removal of content or information posted on the operator's site or service by the minor, with certain exceptions.[17]

IV INTERNATIONAL DATA TRANSFER

There are no significant or generally applicable data transfer restrictions in the United States.

The Federal Trade Commission is committed to international interoperability and cooperation. The US–EU Safe Harbor framework permits the FTC to complement the EU's effort to protect European consumers' privacy. The FTC has stated that Safe Harbor is a top enforcement priority.[18] The FTC has brought dozens of Safe Harbor

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

17 Calif. Bus. & Prof. Code Sections 22580–22582.

18 Available at www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-USeu-safe-harbor-

cases,[19] and the agency is committed to review on a priority basis all referrals from EU Member State authorities. The agency only began receiving referrals in the past three years, and on its own initiative sought to identify Safe Harbor violations in every privacy and data security investigation it conducts. The resulting orders protect over a billion consumers worldwide, including millions of European citizens.

The FTC has signed a memorandum of understanding[20] with Ireland's Office of the Data Protection Commissioner in June 2013 to promote communication and cooperation between the two agencies in an era when consumer information is increasingly moving across borders. The FTC also signed a memorandum of understanding with the UK Information Commissioner's Office in March 2014.[21] The memorandum of understanding is designed to promote increased cooperation and communication in both agencies' efforts to protect consumer privacy.

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[22] works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[23] In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.[24]

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management[25] 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

framework/131112europeancommissionsafeharbor.pdf.

19 See FTC Enforcement: Cases and Proceedings, available at www.ftc.gov/enforcement/cases-proceedings (last accessed 3 March 2014).

20 Press release, 'FTC Signs Memorandum of Understanding with Irish Privacy Enforcement Agency' (27 June 2013), available at www.ftc.gov/news-events/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement.

21 www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/140306ftc-uk-mou.pdf.

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

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

24 See 'APEC Overview', Chapter 2.

25 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 http://ssrn.com/abstract=1568385.

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 creating or expanding a privacy leadership function. The risk of enforcement also prompted companies to engage in ongoing dialogues with the FTC and state regulators.

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

The United States does not require companies to appoint a data protection officer (although specific laws such as the GLBA and HIPAA require companies to designate employees to be responsible for the organisation's mandated information security and privacy programs). However, it is a best practice to appoint a chief privacy officer and an IT security officer. Most businesses in the US 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 US and may be required under some state laws. Regular employee training regarding data security is also recommended.

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 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 US. 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 US and thereby subject to production requests irrespective of European blocking statutes.

The US 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.[26]

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

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

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

26 *Société Nationale Industrielle Aérospatiale v. US District Court*, 482 U.S. 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 execution of criminal search warrant issued to Microsoft for data stored in its servers located in Ireland. The case is now on appeal following a district court decision obliging Microsoft to produce the data in question.

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

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

passed privacy laws that typically affect businesses operating throughout the United States.[29]

Federal Trade Commission

The FTC is the most influential government body that enforces privacy and data protection[30] in the United States.[31] It oversees essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[32] Through exercise of powers arising out of Section 5 of the Federal Trade Commission Act, 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'.[33] 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 US.[34]

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 disposal to prosecute an impressive series of enforcement cases.'[35] 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.[36]

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 implement controls, audits, and other privacy enhancing processes during a period of time that can span decades. These enforcement actions have

29 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.

30 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 US.

31 See Daniel J Solove & Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 *Columbia L. Rev.* __ (forthcoming 2014) ('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 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

32 See http://export.gov/static/sh_en_FTCLETTERFINAL_Latest_eg_main_018455.pdf.

33 15 U.S.C. Section 45.

34 15 U.S.C. Section 45(a)(4).

35 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.

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

been characterised as shaping a common law of privacy that guides companies' privacy practices.[37]

'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 the businesses to substantial financial penalties for order violations. The orders protect all consumers dealing with the 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 US – Congress has expressly confirmed the FTC's authority to redress harm abroad caused from within the US.[38]

The states

State attorneys general retain powers to prohibit unfair or deceptive trade practices similar to the FTC arising from powers granted by 'unfair or deceptive acts and practices' statutes. Recent privacy events have seen increased cooperation and coordination in enforcement amongst 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.

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. Three illustrative cases are summarised below.

37 See, for example, Solove and Harzog, 2014 (footnote 31, *supra*).

38 15 U.S.C. Section 45(a)(4).

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 prohibition against misrepresenting the security of its cameras; the establishment of a comprehensive information security programme designed to address security risks; submitting to third-party assessments of its security programmes every two years for the next 20 years; notifying customers of security issues with the cameras and the availability of the software update to correct them; and providing customers with free technical support for the next two years.[39]

Online advertising

In December 2012, the FTC announced a settlement with a large online advertising company, Epic Marketplace Inc, that was using 'history sniffing' to secretly and illegally gather data from millions of consumers about their interest in sensitive medical and financial issues, from fertility and incontinence to debt relief and personal bankruptcy. The company would then use this information to send consumers targeted ads. The FTC's order barred the company from continuing to use the history sniffing technology and required it to destroy information that it had gathered unlawfully.[40]

Financial and medical information

In 2009 the FTC settled a case against CVS Caremark (CVS) the largest pharmacy chain in the United States, which had been charged with failing to take reasonable and appropriate security measures to protect the sensitive financial and medical information of its customers and employees, in violation of federal law. Based on its failure to take these measures, CVS was also charged with engaging in unfair and deceptive practices by failing to act in accordance with its claim that 'nothing is more central to our operations than maintaining the privacy of your health information'. The FTC order requires CVS to maintain a comprehensive information security programme; to obtain a biannual audit from an independent professional for the next 20 years; and remain subject to FTC monitoring. In a related settlement with the Department of Health and Human Services,

39 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.

40 Press Release, 'FTC Approves Final Order Settling Charges Against Epic Marketplace, Inc.' (19 March 2013), available at www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-order-settling-charges-against-epic.

CVS had to develop new policies and practices related to information handling; undergo outside auditing; and pay US$2.25 million to the agency.[41]

Safe Harbor enforcement cases

The FTC has pursued a number of enforcement actions against companies under its Safe Harbor authority.[42] The FTC's Safe Harbor cases allege both specific violations of the Safe Harbor's privacy principles and false claims of Safe Harbor participation, in which companies continue to represent themselves as Safe Harbor members even when their annual certifications have lapsed. US entities that persistently fail to comply with the Safe Harbor principles will lose the benefits of Safe Harbor participation.[43]

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 US$7 million settlement with Google over allegations that the company violated people's privacy by collecting Wi-Fi data as part of its Street View activities. Google agreed to train its employees about privacy and confidentiality for at least the next 10 years and to destroy or secure any improperly collected information.[44]

Safari cookie settlements

In July 2013, the New Jersey Attorney General's Office announced a US$1 million settlement with online advertising company PulsePoint concerning allegations that the company bypassed web browser privacy settings to collect information on consumers'

41 Press Release, 'FTC Approves Final Consent Order in Matter of CVS Caremark Corporation' (23 June 2009), available at www.ftc.gov/news-events/press-releases/2009/06/ftc-approves-final-consent-order-matter-cvs-caremark-corporation.

42 See *In the Matter of Myspace LLC*, FTC File No. 102 3058 (2012); *In the Matter of Facebook, Inc*, FTC File No. 092 3184 (2011); *In the Matter of Google Inc*, FTC File No. 102 3136 (2011); *In the Matter of Collectify LLC*, FTC File No. 092 3142 (2009); *In the Matter of Progressive Gaitways LLC*, FTC File No. 092 3141 (2009); *In the Matter of Directors Desk LLC*, FTC File No. 092 3140 (2009); *In the Matter of Onyx Graphics, Inc*, FTC File No. 092 3139 (2009); *In the Matter of ExpatEdge Partners, LLC*, FTC File No. 092 3138 (2009); *In the Matter of World Innovators, Inc*, FTC File No. 092 3137 (2009); and *FTC v. Javian Karnani, and Balls of Kryptonite, LLC*, Civil Action No. 09-CV-5276, FTC File No. 092 3081 (2009).

43 US–EU Safe Harbor Framework: Guide to Self-Certification at 32.

44 See, for example the 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.

online browsing habits to serve millions of online advertisements.[45] In November 2013, 37 states settled an investigation with Google involving essentially the same allegations for US$17 million.[46]

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 intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and 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, or being victimised by a hacker or suffering a data breach incident, is well known across the country.

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 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.[47] Consumer protection regulators like the FTC and state attorneys general are becoming increasingly aggressive – both in terms of the scope of enforcement jurisdiction and the stringency of regulator expectations.

---

45 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 http://nj.gov/oag/newsreleases13/pr20130725a.html.

46 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-schnetiderman-announces-17-million-multistate-settlement-google-over-tracking.

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

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 US, the FTC has jurisdiction. If a foreign organisation is a publicly traded company, the SEC has jurisdiction. If an organisation is a health-care 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 US does not have any forced localisation requirements for data servers, and national requirements have even been struck down in the government procurement context. Though the US does not force localisation, it requires vendor oversight to ensure reasonable standards of data care. A foreign organisation operating in the US should know they are the responsible party under US law, even if data processing is handled by a vendor outside the US.

The US 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 US 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 (health-care data), and 47 state laws plus the laws of numerous US territories and districts like the District of Columbia (for broad categories of sensitive personal information). The GLBA, HIPAA and Massachusetts

state law[48] 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.[49]

The Securities and Exchange Commission (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 is currently investigating companies for alleged cybersecurity failures under two theories: (1) 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 (2) 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

48 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.

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

implements the privacy and security provisions of the GLBA for entities subject to its direct regulatory jurisdiction (such as 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.

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.[50] 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, health-care providers, banks subject to detailed examinations by the Federal Financial Institutions Examination Council, or investment firms that are regulated by the Securities and Exchange Commission are subject to detailed cybersecurity standards.

Also, as detailed above, the FTC increasingly plays the role of *de facto* cybersecurity enforcement agency where consumer or personal information is 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.

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 US, and unlike many other regulatory issues, privacy has not become mired in

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

Democrat–Republican partisan battles. And though the EU often disparages the US approach, in some ways the recent EU privacy proposal cuts some red tape and promotes streamlined EU-wide regulatory approvals. It also focuses more heavily on what has been a priority in the US, namely information security and data breach notification requirements. The EU's new proposal also seeks to encourage more enforcement and collective redress, like that seen from the FTC and state attorneys general and in private class actions.

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 FTC's broad mandate proves a stronger incentive to invest in privacy than the European regulators' more siloed mandate.[51]

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'.[52] 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.[53] The FTC has noted that issues likely to capture their 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 Senator Rockefeller, 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 has been 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 clamour begins to fade, it is possible that legislation will come to pass to enable further

51 Bamberger and Mulligan, 2011 (see footnote 25).

52 Id.

53 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).

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

Investment in 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 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 chairman 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 Privacy, Intellectual Property, Technology and Antitrust Litigation Advisory Committee of the National Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President. He is a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government, and Yale Law School.

TASHA 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 MOHAN

Sidley Austin LLP

Vivek Mohan is an associate with Sidley Austin LLP's privacy, data security and information law group in Washington, DC. Vivek is affiliated with and serves as visiting faculty for 'The Cyber Project' at the Harvard Kennedy School, where he spent two years as resident fellow. Vivek has also held a special appointment with the Internet Bureau of the Office of the New York State Attorney General and worked as in-house counsel at Microsoft's Innovation & Policy Center. Vivek holds a JD from Columbia University School of Law 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
vivek.mohan@sidley.com

www.sidley.com