THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-810-9

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

ACKNOWLEDGEMENTS

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

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 28

UNITED STATES

Alan Charles Raul and Snezhana Stadnik Tapia[1]

I OVERVIEW

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

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

---

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

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

3 Warren and Brandeis, supra note 2, at 213.

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

But there is now a growing perception that other jurisdictions have seized the privacy leadership mantle by adopting more comprehensive regulatory frameworks, exemplified by the European Union's General Data Protection Regulation (GDPR). A series of high-profile data breaches in both the public and private sectors and concerns about misinformation and the misuse of personal information have also created a 'crisis of new technologies' or 'techlash' that is shifting popular views about privacy in the United States. The privacy issues at the centre of the covid-19 pandemic, recent state privacy law developments and the rise in cybersecurity attacks on American companies have also led to serious public concern surrounding privacy and cybersecurity that have necessitated action by the new administration. Once again, it seems, the United States is starting to undergo a period of intense regulatory innovation in response to a new technological world.

In short, the US privacy zeitgeist is shifting – and this chapter, while not providing a comprehensive overview of the rich US privacy and cybersecurity landscape, will attempt to show how that is the case. The chapter will begin by describing, with a focus on the concrete developments over the past year, the significant shift in how the United States is thinking about privacy and cybersecurity regulation that appears to be underway:

a how the covid-19 pandemic continues to place issues concerning the collection and use of personal data front and centre, and coupled with the growing epidemic of cyberattacks in the current remote working environment, intense discussions over the need for privacy and cybersecurity regulation are paving the way for a concerted response by the federal US government;

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

c how the real action continues to be not in Washington, DC, but rather in the 50 US states – as California's far-reaching comprehensive privacy bill called 'California's GDPR' went into effect on 1 January 2020 and California voters approved an even more comprehensive law called the California Privacy Rights Act (CPRA), while numerous other states (such as Virginia and Colorado) either have enacted or are considering substantial new privacy legislation.

The chapter will then provide an overview of the existing US regulatory and enforcement framework – which exemplifies the balance between privacy protection and innovation described above. The chapter then concludes by detailing the significant changes in the international data transfer framework between the EU and US, considerations for foreign organisations that must engage with the US privacy regime, and some thoughts on how that regime may continue to evolve going forward.

II THE YEAR IN REVIEW

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

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

i Privacy issues and cybersecurity attacks during the covid-19 pandemic

From 20 January 2021 onward, the Biden administration has had to address unprecedented public health, economic and cybersecurity crises. Among other things, the collection of personal data and digital contact tracing during the pandemic, as well as the increasing prevalence of foreign cyberattacks, have led to serious public concern surrounding privacy and cybersecurity and necessitated action by the new administration. It is no understatement to say that the ongoing covid-19 pandemic has changed and is continuing to change our world in many ways. First, the need for employers to begin capturing significantly more health information about their employees as part of their back to work efforts, including now the vaccination status of employees, to the use of novel technologies to track the virus, it is no understatement to say that privacy and cybersecurity considerations have been central to the policy response to the pandemic. Second, the covid-19 teleworking environment has led to systemic cyber risks. As a large proportion of the US workforce was forced to begin teleworking almost overnight, companies saw a significant increase in the number of ransomware attacks. These cyber threats were designed to take advantage of remote working arrangements in place since the beginning of the pandemic lockdowns. Third, and somewhat relatedly, the past year has been highly eventful in terms of cybersecurity attacks (especially ransomware attacks), prompting responses from Congress and the Biden administration as calls for increased regulation intensify. This growing epidemic of cyberattacks has prompted a coordinated response from the federal government, as detailed below.

First, businesses have had to consider how to continue operating or reopen safely during the pandemic, which often involves or requires collecting sensitive health and related data (such as temperature and symptom checks, recent travel history and contact with infected persons) before employees return to work and establishing protocols for symptom and exposure reporting. During the height of the pandemic, new federal, state, and local laws and guidance on collecting and using covid-19-related information were issued on almost a daily basis. Various federal, state and local agencies issued mandatory or recommended guidance on nearly every aspect of these issues – from what screening must and may be done, what information can and should be captured, and how long such information must and can be maintained. Federal, state and local agencies also promulgated guidance or released statements noting that they may modify their enforcement posture or reporting requirements during the pandemic. For example, the Department of Health and Human Services (HHS)

waived penalties and refrained from enforcing certain provisions under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including the requirement to obtain patients' consent before speaking with family members or friends about patients' care, the requirement to distribute a privacy notice, and the patient's right to request privacy restrictions or request confidential communications.[4]

At the time of writing, with more than half of the US population fully vaccinated, the conversation has now shifted to the collection and use of vaccination status information. The pandemic has pushed many companies into new territory, requiring the gathering of personal information that they would not normally collect, such as temperature checks and travel histories. Now, asking for proof of a covid-19 vaccine in exchange for entry on a plane or into a concert venue presents the same type of privacy and data security concerns. Moreover, the concept of vaccine passports also prompts further interest in federal, omnibus privacy legislation.

Second, one of the most immediate consequences of the covid-19 pandemic was that a large proportion of the US workforce was forced to begin teleworking. This distributed environment raised the level of cybersecurity risk businesses faced, as did the fact that cybersecurity criminals and scammers increased their efforts to target vulnerable employers and workforces. Given this, several US federal agencies issued guidance on cybersecurity risks in relation to the pandemic; for example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Trade Commission (FTC) issued guidance on avoiding phishing and scam emails relating to covid-19.[5] And organisations increased their preventative efforts, undertaking such tasks as reviewing and updating their incident response plans to address an increased attack surface resulting from remote work, ensuring regular patching and remote wiping, clarifying business continuity plans and processes with vendors and clients, and raising employee awareness about covid-19 related phishing emails. Despite these efforts, ransomware cases have surged. Some estimate that cases increased 150 per cent in 2020 compared to the previous year. The Department of Justice noted that roughly US$350 million in ransom was paid to malicious cyber actors in 2020, an increase of more than 300 per cent from the previous year.[6]

Third, the past year has continued to be very eventful in terms of cybersecurity attacks, with the breaching of US government networks, ransomware hackers holding a major US pipeline hostage and attackers infiltrating software companies. On 13 December 2020, hackers compromised the update process of a widely used piece of SolarWinds software, the Orion platform. The update was downloaded onto thousands of organisations' information systems, essentially planting backdoors in the networks of up to 18,000 organisations, including the US Departments of Commerce, the Treasury, Homeland Security and Defense and the Energy Department's Nuclear Security Administration. This attack was the most visible, widespread and intrusive IT software supply chain attack to date. Around the same

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

5 Internal Revenue Service (IRS), *Avoid Scams Related to Economic Payments, COVID-19*, https://www.cisa.gov/sites/default/files/publications/Avoid_Scams_Related_to_Economic_Payments_COVID-19.pdf; FTC, *Coronavirus Advice for Consumers*, https://www.ftc.gov/coronavirus/scams-consumer-advice.

6 Dep't of Justice, U.S. *Government Launches First One-Stop Ransomware Resource at StopRansomware.gov* (July 15, 2021), https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov.

time, another cyberattack on California-based file-sharing software vendor, Accellion, made news headlines. As a result of the attack, one million Washington residents whose data was housed at the state auditor's office may have had their social security numbers and other personal information unlawfully accessed. And if that were not enough, the trend of targeting third-party software platforms continued in March, when Microsoft reported a cyberattack on its Exchange email servers. These attacks have emphasised the importance of software supply chain security, spurring companies to take a closer look at security risks from using third-party software providers. The attacks also showed that, by compromising just one vendor, attackers may get access to the vendor's customers. The attacks showed that even high-profile government agencies and security vendors, such as FireEye, can be targets.

Moreover, the pace of ransomware attacks had already been on the rise before 2021, but the issue made its way into the public domain after an attack temporary halted the Colonial pipeline in May, causing fuel shortages throughout the East Coast. The President and CEO of Colonial, Joseph Blount, defended the company's ransom payment worth US$4.4 million in cryptocurrency in order to get its systems operational faster. Although highly publicised, the Colonial Pipeline cyberattack is not unique. In fact, the event is just one in a growing pattern of ransomware attacks against major US companies and critical infrastructure. Weeks after the Colonial Pipeline event, meat processing company JBS also acknowledged a ransom payment of US$11 million in response to a ransomware attack. In addition, a ransomware cyberattack in July 2021 on software vendor Kaseya, a provider of remote software IT services, came with an aggregate demand of US$70 million in cryptocurrency and affected up to 1,500 organisations.

In light of these events, the growing epidemic of cyberattacks has become a key area of concern for federal lawmakers. The Senate Committee on Homeland Security and Governmental Affairs and the House Homeland Security Committee heard testimony from Colonial's CEO, where lawmakers expressed their expectation that companies should have plans in place to anticipate possible ransomware attacks; consult with the FBI on ransom payments; and participate in government cybersecurity initiatives that are applicable to their business. A key point of agreement between the legislators and the witnesses was the importance of communicating cybersecurity information between and among private entities and the federal government. The legislators also agreed that the federal government must take strong action against foreign nations that engage in cyberattacks or shelter cybercriminals.

The Biden administration has also responded, underscoring the broader shift to implementing certain security measures, greater reporting and coordination requirements and enhanced communication between the government and the private sector. On 12 May 2021, the Biden administration issued a lengthy Executive Order, 'Improving the Nation's Cybersecurity', which it described as the 'first of many ambitious steps' toward modernising US cybersecurity defences.[7] Although the Order details a host of new requirements that will apply to federal departments and agencies, the Order also focuses on private entities that do business with the federal government, particularly software suppliers. Pursuant to the Order, government agencies will be required to deploy multifactor authentication, encryption, endpoint detection response and logging, and operate under the principle of a 'zero trust' environment. The Order also requires federal contractors to share information regarding security incidents. The Order also tasked the Cybersecurity and Infrastructure Security Agency (CISA), a unit of the Department of Homeland Security, to produce a cloud service

7 Exec. Order No. 14028, 86 FR 26633 (2021).

governance framework and a standard incident response playbook for federal agencies. Under the Order, the National Institute of Standards and Technology (NIST) was tasked with identifying security measures for the use of critical software and recommending minimum standards for software vendors to test their products before offering them to the government. In response, NIST posted two new pieces of guidance in July 2021.[8] Now, the Office of Management and Budget must require federal agencies to implement the security measures NIST outlined for the using of critical software, including through their procurements. The new federal requirements and standards for development of secure software will undoubtedly also set expectations for software products sold and used exclusively in the private sector as well.

On 28 May, the US Department of Homeland Security's Transportation Security Administration (TSA) also issued a Security Directive, 'Enhancing Pipeline Cybersecurity', laying out new cybersecurity requirements for operators of liquids and natural gas pipelines and LNG facilities designated as critical infrastructure.[9] Unlike the Executive Order, which covered government agencies and their suppliers, the Directive focuses directly on the activity of private sector entities.

Although the Executive Order and TSA's directive are noteworthy, they are limited in scope. To augment the nation's cybersecurity posture, lawmakers are contemplating national cyberincident reporting legislation. Federal officials note that the lack of information about breaches (that typically occur on private networks) hampers their ability to address digital threats and disruptions. This is due to the patchwork of federal and state data breach reporting laws, many of which are sector-specific (in the federal sphere) or require the exposure of consumers' personal information (in the state breach notification regime). Specifically, a bipartisan group of senators is considering legislation that would require a broad range of companies, including critical infrastructure operators, to report hacks (regardless of whether personal data is implicated) to the government. The House Homeland Security Committee is also drafting similar legislation.

The Biden administration continues to bolster its efforts to halt the growing ransomware threat via a national counter-ransomware campaign. In June 2021 the White House issued an open letter to corporate executives and business leaders, 'What We Urge You To Do To Protect Against The Threat of Ransomware', referring to the President's new Cybersecurity Executive Order and detailing practical steps companies should take to protect themselves.[10] The White House described the letter as setting forth the government's 'recommended best practices – we've selected a small number of highly impactful steps to help you focus and make rapid progress on driving down risk'.

8 National Institute of Standards and Technology, Security Measures for "EO-critical software" use under Executive Order (EO) 14028 (2021), https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2; Paul E Black, Barbara Guttman and Vadim Okun, Guidelines on Minimum Standards for Developer Verification of Software, National Institute of Standards and Technology (July 2021), https://www.nist.gov/system/files/documents/2021/07/13/Developer%20Verification%20of%20Software.pdf.

9 49 U.S.C. §§ 114(d), (f), (l) and (m).

10 Open Letter Available in *Readout of Deputy National Security Advisor for Cyber Anne Neuberger Meeting with the Bipartisan National Association of Attorneys General* (June 11, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/11/readout-of-deputy-national-security-advisor-for-cyber-anne-neuberger-meeting-with-the-bipartisan-national-association-of-attorneys-general/.

The administration also formed an inter-agency ransomware taskforce. The taskforce is overseeing and harmonising federal agencies' digital resilience activities, working to curtail ransom payments, working to disrupt ransomware operators' networks and their use of cryptocurrencies for transferring funds and urging international cooperation to combat the issue. The taskforce also provides the Biden administration with weekly updates on the agencies' efforts. Another option the administration is currently considering is hacking back. Recently, the State Department announced its Rewards for Justice programmes, offering rewards for helping identify the perpetrators of these attacks, especially of state-sanctioned breaches of critical infrastructure. The State Department announced that it would provide rewards of up to US$10 million 'or information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyberactivities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA)'. CISA has also been tasked with launching an interagency website, stopransomware.gov, to collect guidance from various agencies on the issue.

Meanwhile, lawmakers continue to question whether ransom payments should be permitted and if federal law should be passed to outright prohibit ransom payments in order to curtail and disincentivise such attacks. While there is no current federal or state law prohibiting ransom payments, on 1 October 2020, the US Treasury Department's Office of Foreign Assets Control (OFAC) published an advisory to highlight the risk of potential US sanctions law violations if US individuals and businesses comply with certain ransomware payment demands.[11] The US Treasury's Financial Crimes Enforcement Network (FinCEN) has issued a similar advisory.[12] Specifically, the advisory provides helpful guidance for financial institutions to better detect and report suspicious payments as required by FinCEN's anti-money laundering regulations. FinCEN also is continuing to address ransomware by setting up exchanges between government and private sector partners to determine next steps. Finally, the US Treasury Department is also focusing on efforts to track major cryptocurrency payments in order to stop ransoms before they reach hackers' crypto-wallets. Against this backdrop, the recent discussions of a federal law that broadly prohibits ransomware payments continue.

ii Key federal government privacy and data protection actions

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

Executive branch – recent enforcement cases and proposed rules

The FTC had an active year with several enforcement actions. In addition to the court's approval of the FTC's historic US$5 billion settlement with Facebook, the agency brought several notable actions regarding unfair practices, data security and the Children's Online Privacy Protection Act (COPPA).

11 U.S. Dep't. of the Treasury, *Advisory of Potential Risks for Facilitating Ransomware* (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

12 U.S. Dep't. of the Treasury, *FinCEN Guidance, FIN-2020-A00X, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

Along with the past year's significant increase and reliance on Zoom videoconferencing during the pandemic lockdowns came concerns about and allegations of inadequate data security. On 9 November 2020, the FTC announced a settlement with Zoom regarding the agency's allegations that the company made false and deceptive claims about its encryption since at least 2016, as well as engaged in unfair practices, which undermined the security of its users, specifically, the installation of software that bypassed a security feature in Apple's Safari browser.[13] The FTC also focused on allegedly deceptive claims and inadequate security for two healthcare companies (SkyMed and Flo Health) for failing to take reasonable steps to secure sensitive health records,[14] as well as sharing users' health information with undisclosed data analytics providers.[15] With respect to the use of facial technology, Everalbum settled FTC allegations that it deceived consumers about its retention of photos and videos of users who deactivated their accounts.[16]

Moreover, the FTC demonstrated its continued focus on children's privacy during the past year. In July 2020, the FTC finalised a settlement and consent agreement to resolve allegations that Miniclip misrepresented its status in a COPPA safe harbour programme.[17] Kuuhuub Inc, Kuu Hubb Oy and Recolor Oy (an online colouring book app) also settled FTC allegations that, in violation of COPPA, they collected and disclosed personal information about children who used the app without notifying their parents and obtaining their consent.[18]

The impact on the FTC's Section 5 enforcement activities of the recent appointment of a new FTC commissioner and chair, Lina Khan, remains to be seen. The former Columbia Law professor with the profile of a progressive reformer of antitrust is expected to focus on tech giants and their privacy practices. President Biden's recent Executive Order on Promoting Competition in the American Economy contains data-related provisions. The Order encourages the chair to focus on 'unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy'.[19] Many expect Chair Khan to scrutinise consumer data collection as part of her focus on the dominance of US tech giants, which may result in additional rule-making as well as high-profile enforcements by the FTC.

The FTC was not the only agency that had an active year. The Securities Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) have been exercising increasingly aggressive oversight regarding cybersecurity compliance in recent years, and the past year was no exception. Building on the SEC's 2018 issuance of new interpretive guidance to assist publicly traded companies in disclosing their material

13 *Zoom Video Communications, Inc.*, 192 F.T.C. 3167 (2021), https://www.ftc.gov/enforcement/cases-proceedings/192-3167/zoom-video-communications-inc-matter.

14 *SkyMed International, Inc.*, 192 F.T.C. 3140 (2020), https://www.ftc.gov/enforcement/cases-proceedings/1923140/skymed-international-inc-matter.

15 *Flo Health, Inc.*, 192 F.T.C. 3133 (2021), https://www.ftc.gov/enforcement/cases-proceedings/192-3133/flo-health-inc.

16 *Everalbum, Inc.*, 192 F.T.C. 3172 (2021), https://www.ftc.gov/enforcement/cases-proceedings/192-3172/everalbum-inc-matter.

17 *Miniclip S.A.*, 192 F.T.C. 3129 (2020), https://www.ftc.gov/enforcement/cases-proceedings/192-3129/miniclip-matter.

18 *USA v. KUUHUUB INC., et al.*, No. 1:21-cv-0178 ((D.D.C. 2021), https://www.ftc.gov/enforcement/cases-proceedings/1823184/kuuhuub-inc-et-al-us-v-recolor-oy.

19 Exec. Order No. 14036, 86 FR 36987 (2021).

cybersecurity risks and incidents to investors,[20] the SEC's Office of Compliance Inspections and Examinations (OCIE) (recently renamed the Division of Examinations)[21] issued guidance in 2019 identifying the multiple steps it is taking to heighten its enforcement presence for cybersecurity matters.[22] In April and May 2019, the OCIE further issued two risk alerts providing regulated entities with details on its privacy and cybersecurity focus areas during examinations.[23] More recently, the OCIE released its 2020 examination priorities, which, among other priorities, include cyber and information security risks, as well as a report on 'Cybersecurity and Resiliency Observations', providing an overview of best practices based on prior exams to help organisations when considering 'how to enhance cybersecurity preparedness and operational resiliency'.[24] Finally, earlier this year on 1 February 2021, FINRA updated its prior guidance by issuing a report on its examination and risk monitoring programme, which covers cybersecurity and technology governance – an area of emphasis for FINRA especially in this remote work environment.[25]

The SEC has also backed its guidance up with action on the enforcement front. For example, on 14 June 2021, the SEC settled an action against First American Insurance Company related to the same facts of New York DFS's Department of Financial Services investigation. The DFS alleged that First American experienced a vulnerability that resulted in the exposure of consumers' personal information and further alleged that the company failed to remediate the vulnerability and violated six provisions of the DFS Cyber Regulation. The SEC announced settled charges against First American for disclosure controls and procedures violations concerning cybersecurity vulnerability. The Exchange Act Rule 13a-15(a) requires 'every issuer of a security registered pursuant to Section 12 of the Exchange Act to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded,

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

21 SEC, *Statement on the Renaming of the Office of Compliance Inspections and Examinations to the Division of Examinations* (Dec. 17, 2020), https://www.sec.gov/news/public-statement/joint-statement-division-examinations.

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

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

24 See OCIE, *2020 Examination Priorities*, https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2020.pdf; SEC, *Office of Compliance Inspections and Examinations: Cybersecurity and Resiliency Observations*, https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

25 See FINRA, *2021 Report on FINRA's Examination and Risk Monitoring Program*, https://www.finra.org/sites/default/files/2021-02/2021-report-finras-examination-risk-monitoring-program.pdf.

processed, summarized, and reported within the time periods specified in the Commission's rules and forms.'[26] Without admitting or denying the SEC's findings, First American agreed to a cease-and-desist order and to pay a US$487,616 penalty.

Another regulator that has recently brought several enforcement actions was the US Department of Health and Human Services, Office for Civil Rights (OCR). In 2020 and 2021, OCR settled several cases related to the alleged violations of HIPAA. OCR mainly alleged non-compliance with the administrative and technical safeguards of the HIPAA Security Rule, with a focus on encryption practices, risk analyses and management plans, development of business associate agreements and proper employee training regarding protected health information (PHI).[27]

Several executive agencies have also proposed rules regarding privacy and data security. With respect to health information, on 10 December 2020 OCR released a proposed rule that would make a number of key changes to the Privacy Rule under HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).[28] The rule is intended to reduce burdens that may limit or discourage care coordination and case management communications among individuals and HIPAA-covered entities while continuing to protect the privacy of individuals' PHI. In the wake of the rise in cyberattacks, in December 2020 the US Federal Deposit Insurance Corporation approved and several federal banking agencies (including the Office of the Comptroller and the Board of Governors of the Federal Reserve System) jointly announced a notice of proposed rule-making, 'Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers'.[29] Generally, if finalised, the proposed rule would require certain banking organisations and bank service providers to provide accelerated notices of certain cybersecurity and related events 'as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred'.

Finally, in addition to promulgating policies regarding privacy or data security, federal regulators are also increasingly interested in studying and regulating digital innovation and

26 17 C.F.R. § 240.13a-15.

27 See, e.g., HHS, *Clinical Laboratory Pays $25,000 to Settle Potential HIPAA Security Rule Violations*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/peachstate/index.html; *Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lifespan/index.html; *Small Health Care Provider Fails to Implement Multiple HIPAA Security Rule Requirements*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/metro/index.html; *Orthopedic Clinic Pays $1.5 Million to Settle Systemic Noncompliance with HIPAA Rules*, https://www.hhs.gov/about/news/2020/09/21/orthopedic-clinic-pays-1.5-million-to-settle-systemic-noncompliance-with-hipaa-rules.html.

28 Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement (proposed Dec. 10, 2021) (to be codified at 45 C.F.R.. pts. 160, 164), https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf.

29 Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 7 (proposed Jan. 12, 2021) (to be codified at 12 C.F.R. pts. 53, 225, 304), https://www.fdic.gov/news/board/2020/2020-12-15-notice-sum-c-fr.pdf.

artificial intelligence. The examples of this trend are numerous, with some of the highlights being the following:

a In May 2020, the National Telecommunications and Information Administration (NTIA) published a notice seeking comments regarding the development of an implementation plan for the national strategy to secure 5G, a component of the 'Secure 5G and Beyond Act of 2020' that was signed into law on 23 March 2020.[30]

b In June 2020, FINRA issued its 2020 Artificial Intelligence Report for industry comment.[31] The report is a culmination of FINRA's Office of Financial Innovation review of emerging challenges and legal considerations confronted by the securities industry as broker-dealers introduce AI-based applications into their businesses.

c In March 2021, the five largest federal financial regulators in the US (the Board of Governors of the Federal Reserve System, the Bureau of Consumer Financial Protection, the Federal Deposit Insurance Corporation, the National Credit Union Administration and the Office of the Comptroller of the Currency) released a request for information on how banks use AI, signalling that new guidance for the financial sector may be issued soon.[32]

d In April 2021, the FTC released a set of guidelines aiming for 'truth, fairness, and equity' in companies usage of AI.[33] The previous year, in April 2020, the FTC's Bureau of Consumer Protection also issued a statement on 'Using Artificial Intelligence and Algorithms', which acknowledged the risks and benefits presented by AI technologies. The statement has served as helpful guidance for entities considering the use of AI and automated decision-making technologies.[34]

Legislative branch

The popular focus on privacy and cybersecurity matters in 2020 during the covid-19 pandemic has continued. Some privacy practitioners believe that 2021 has the best chance yet due to the election of President Joe Biden together with the President's party controlling both houses of Congress, and that the continued legislative action in the states may also result in federal momentum. Many of the world's governments have enacted data privacy legislation in the past year, and as more and more countries are expected to pass comprehensive legislation, including China and India, sufficient pressure may mount for the US to keep up with the largest international markets by enacting its own omnibus data privacy law.

Multiple congressional committees continue to hold high profile hearings on the possibility of enacting comprehensive federal privacy legislation, and both industry and civil society are urging Congress to act. Many see the value in having a federal law versus a

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

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

32 Meeting Notice, 86 Fed. Reg. 60 (March 30, 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf?utm_campaign=subscription+mailing+list&utm_source=federalregister.gov&utm_medium=email.

33 Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC: Business Blog (April 19, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

34 Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC: Business Blog (April 8, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

patchwork of state laws from both a consumer and business standpoint. One of the more recent proposals, the Information Transparency and Personal Data Control Act, was the first piece of comprehensive privacy legislation introduced in the 117th US Congress by Representative Susan DelBene (D-Washington) – about two weeks after Virginia passed its own comprehensive data privacy law.[35] (Congresswoman DelBene introduced a similar version of the bill in 2019, but it did not gain traction then.) On 29 April 2021, US Senator Jerry Moran (R-Kansas) also reintroduced a bill for the Consumer Data Privacy and Security Act. In particular, SB 1494 seeks to strengthen the laws that govern consumers' personal data and create clear standards and regulations for American businesses that collect, process and use consumers' personally identifiable data.[36] Senator Moran previously introduced a version of this bill in 2020 that stalled in committee. Both bills grant enforcement authority to both the FTC and state attorneys general, but notably do not include a private right of action. More recently, Senator Kirsten Gillibrand (D-New York) reintroduced the Data Protection Act.[37] The bill would establish a new federal agency, the Data Protection Agency, which, among other things, would regulate and enforce federal data privacy laws, create and develop model data privacy standards for the private sector, jointly review mergers with the FTC and DOJ involving the transfer of data for more than 50,000 individuals, and advise Congress on emerging privacy and technology issues.

Whether the bills noted above will garner enough support remains uncertain. Despite the current consensus that something needs to be done, however, support at the time of writing continues to cleave between those who want to enact legislation that pre-empts state law such that US businesses are not subject to a patchwork quilt of privacy regulation and those who (mirroring civil society) want to allow states to provide additional privacy rights above a federal floor. The enactment of federal privacy legislation rests on the resolution of this debate, as well as agreement on the particulars of the regulatory scheme.

In addition to comprehensive privacy legislation, in the past year Congress has also focused on several more targeted issues, such as artificial intelligence and US cybersecurity preparedness.[38] The 2021 National Defence Authorisation Act created the position of a National Cyber Director within the White House to strengthen the nation's cyber capability through national-level coordination of cyber strategy and policy, and President Biden nominated the first National Cyber Director on 12 July 2021. Congress has also continued

35 Press release, Suzan DelBene, U.S. Congresswoman, 1st Congressional District of Washington, DelBene Introduces National Consumer Data Privacy Legislation, *Bill would create national data privacy standard and give U.S. a seat at the international table* (March 10, 2021), https://delbene.house.gov/news/documentsingle.aspx?DocumentID=2740.

36 Press release, Sen. Jerry Moran, U.S. Senator for Kansas, Sen. Moran Introduces Bill Creating Clear Federal Standard for Consumer Data Privacy (April 29. 2021), https://www.moran.senate.gov/public/index.cfm/news-releases?ID=2AC2D48C-51D5-4D31-AE69-88C0C38C2D3F.

37 S. 3330, 160th Cong. (2021), https://www.gillibrand.senate.gov/download/dpatext.

38 See Tom Simonite, *As the Use of AI Spreads, Congress Looks to Rein It In*, Wired.com (July 16, 2021), https://www.wired.com/story/ai-spreads-congress-rein-in/; *Final Recommendations of the National Security Commission on Artificial Intelligence*, House Committee on Oversight and Reform (March 12, 2021), https://oversight.house.gov/legislation/hearings/final-recommendations-of-the-national-security-commission-on-artificial; *Hearing on U.S. Cybersecurity Preparedness and H.R. 7331, the National Cyber Director Act*, House Committee on Oversight and Reform (July 15, 2020), https://oversight.house.gov/legislation/hearings/hr-7331-the-national-cyber-director-act-1.

to focus on the issue of the government's use of facial recognition technology.[39] Indeed, the currency of this issue increased in the wake of civil unrest and protests regarding police reform in 2020, with some states and cities having banned the use of the technology and several companies calling on Congress to issue rules on the use of the technology and halting sales of facial recognition technology to US police.[40] Other recent issues that have attracted congressional attention include potential reforms to Section 230 of the Communications Decency Act, which shields tech companies that provide online platforms from civil liability stemming from third-party content.[41]

Judicial branch, including key developments with discovery and disclosure

Finally, as they do every year, the federal courts decided a number of important cases relevant to privacy and data security. Notably, on 25 June 2021, the Supreme Court issued its decision in *TransUnion LLC v. Ramirez*, which tightened the Court's requirements to establish the constitutionally required 'standing' necessary to sustain litigation – in other words, whether the plaintiff has suffered a sufficient 'injury in fact' to allow a federal court to adjudicate the claims in question.[42] In *TransUnion*, the named plaintiff, Sergio Ramirez, represented a class of 8,185 individuals who had been notified of their presence on the Treasury Department's OFAC list that identifies suspected terrorists and narcotics traffickers. The plaintiffs in the case alleged that TransUnion violated the Fair Credit Reporting Act (FCRA) by not ensuring the accuracy of certain information placed on credit reports; they alleged that TransUnion assigned an 'alert' to anyone whose name matched a name on the OFAC list without confirming that the name actually referred to the person in question. Ramirez alleged he suffered actual injury in the form of denied credit to finance a car, public embarrassment and a resulting vacation cancellation (out of fear that he would come under scrutiny when trying to travel). TransUnion has since changed its practices.

Faced with the question of what makes an injury concrete, the Court held that the vast majority of the class members whose allegedly inaccurate credit reports were not disseminated to any third party (outside of TransUnion) did not have standing to assert a claim under the FCRA. The Court held that for consumers whose information was not shared with third parties the risk of future harm was simply too speculative to support federal litigation. The *TransUnion* decision confirmed the Court's rule of 'no concrete harm, no standing' in its 2016 decision, *Spokeo, Inc v. Robbins*.[43] With *TransUnion*, the Court further restricted the circumstances where a statutory violation can form the basis for a claim; the Court expanded on *Spokeo* by instructing that 'an injury in law is not an injury in fact'. Perhaps most significantly, the *TransUnion* decision suggests it will be difficult to sue over internal information errors that are never disseminated externally and do not cause concrete harm. This case may also accelerate the trend for privacy litigation based on relatively more

39 *Facial Recognition Technology: Examining Its Use by Law Enforcement*, House Committee on the Judiciary (July 13, 2021), https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4635&utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202.

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

41 Mark MacCarthy, *Back to the future for Section 230 reform*, Brookings, https://www.brookings.edu/blog/techtank/2021/03/17/back-to-the-future-for-section-230-reform/.

42 *TransUnion LLC v. Ramirez*, No. 20-297, 2021 WL 2599472 (2021).

43 *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

abstract or speculative allegations of harm to be filed in state rather than federal court. The US Constitution only requires the doctrine of 'injury in fact' to be applied in federal courts, and many state courts apply less rigorous standing principles.

In another significant cyber-related decision, on 3 June 2021, the Supreme Court resolved a circuit split about the scope of the Computer Fraud and Abuse Act (CFAA), a statute that prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems.[44] The CFAA is sometimes invoked by website operators that restrict certain websites uses pursuant to contractual terms of use (or service) or by employers that pursue claims against former employees who misappropriated trade secrets or otherwise misused sensitive information stored on company computers. The Court significantly limited the scope of the statute in interpreting the meaning of 'exceed[ed] authorized access'. The Court essentially determined the CFAA only prohibits obtaining information from computer files that one does not have any legitimate access to; it does not cover those who 'have improper motives for obtaining information that is otherwise available to them'. (Of course, other statutory, contractual or tort remedies may be available to sanction individuals who access or use computer information for impermissible purposes, but the CFAA is a criminal statute that can also be used by private plaintiffs seeking civil damages.)

And, on 26 May 2020, the District Court for the Eastern District of Virginia issued a decision with potentially significant ramifications for the confidentiality of businesses' data breach response efforts.[45] The question before the Court was whether the attorney work product doctrine allowed Capital One to withhold from civil discovery a forensic report developed by a third-party investigator at the direction of counsel. Believing a substantially similar report would have been prepared regardless of whether the litigation followed, the Court relied on several key facts to find that the report must be produced, including that Capital One executed a non-privileged statement of work for services with the third party prior to the data breach, the post-breach agreement included the same scope of work as the prior statement of work, and the forensic report was widely distributed to different regulators and Capital One's accountant, suggesting that it was not specifically created in anticipation of litigation. This opinion underscores the importance for organisations to consider, in advance, how to engage with incident response service providers in order to protect privilege in the event of a data breach litigation.

iii Key state privacy and data protection actions

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

California's data privacy regime

One of the biggest privacy developments in the United States has been the recent entry into force of the CCPA,[46] a comprehensive privacy bill that commentators have called 'California's GDPR', which was recently amended by the newly enacted California Privacy Rights Act (CPRA). Alastair Mactaggart, the consumer rights advocate who was the driving

44 See *Van Buren v. United States*, No. 19-783 (June 3, 2021).

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

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

force behind the CCPA, secured enough signatures to place the CPRA, a proposed law that would significantly expand the CCPA (and sometimes referred to as 'CCPA 2.0') as an initiative on California's November 2020 ballot.[47] On 3 November 2020, Californians voted to approve Proposition 24. The CPRA amends various parts of the existing CCPA, with most of the substantive changes going into effect on 1 January 2023. The CPRA becomes fully enforceable on 1 July 2023 – with a lookback period from 1 January 2022. Given California's size and the fact that it is the home of Silicon Valley, the CCPA and CPRA are having a wide impact, and companies across the United States and around the world are considering what it might mean for them.

Upon enactment, the CCPA immediately became the most far-reaching privacy or data protection law in the country, and with the passage of the CPRA, California's privacy law regime will share many attributes with the EU's GDPR. The CPRA augments and expands the CCPA in many ways. While a full discussion of how the CPRA compares with the CCPA is beyond the scope of this chapter, notable changes by topic are highlighted below.

a Modification of the definition of a covered 'business': the CCPA applies to for-profit entities that are doing business in California; that collect or determine the means of processing personal information; and that meet one of three size thresholds.[48] The CPRA modifies the definition of a covered business that both increases and decreases the number of businesses currently subject to the CCPA.

b Expansion of disclosure requirements: the CCPA mandates broad privacy policy disclosure requirements on companies that collect personal data about California residents.[49] The CPRA introduces 'sensitive personal information' as a new regulated dataset in California. The category is subject to new disclosure and purpose limitation requirements, and consumers have new rights designed to limit businesses' use of their sensitive personal data. Businesses must also disclose the length of time the business intends to retain each category of personal information or the criteria that would be used to determine the retention period.

c Creation and expansion of consumer privacy rights: the CCPA mandates that businesses provide California residents with the rights to access and delete their personal information, as well as the right to stop the sale of their information to third parties.[50] The CPRA provides new rights and amends existing rights. Some of the new rights include the right to correction, the right to opt-out of automated decision making technology, the right to access information about automated decision making and the right to limit use and disclosure of sensitive personal information. Some of the modified rights include a modified right to delete, an expanded right to know, an expanded right to opt-out and an expanded right to data portability. Perhaps the most significant feature of the CPRA is the provision that gives consumers the right to stop a business from sharing their personal information with third parties for the purpose of engaging in 'cross-context behavioural advertising'.

d Strengthening of opt-in rights for minors: the CCPA prohibits businesses from selling personal information of individuals under the age of 16, absent affirmative

47 The California Privacy Rights Act of 2020, *Ballot initiative*, available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

48 California Consumer Privacy Act, A.B. 375, § 1798.140 (c).

49 id. § 1798.140 (g).

50 id. § 1798.105 (a), 120 (a).

authorisation.[51] As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her personal data after the minor has declined to provide it. The CPRA also increases fines for violations of the opt-in right for minors.

e Expansion of triggering data for a breach: the CCPA provides a private cause of action for certain data breaches that result from a business's violation of the duty to implement and maintain reasonable security procedures and practices.[52] The CPRA expands the CCPA's private right of action for breaches of certain login credentials that would permit access to an account if the business failed to maintain reasonable security.

f Creation of a new privacy enforcement authority: the CCPA authorises the California Attorney General to enforce its provisions with statutory fines of up to US$7,500 per violation.[53] The CPRA restructures this enforcement regime by establishing the California Privacy Protection Agency (CPPA), the first data protection agency in the United States, empowered to promulgate regulations supporting the CPRA and to enforce the CCPA and CPRA after it becomes effective. Moreover, the CPRA essentially removes the 30-day cure period that businesses currently have under the CCPA after being formally notified of an alleged violation. Instead, the CPPA has discretion to provide businesses with a time period to cure and may take into account 'voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of [a] complaint' made by any person. Businesses will still have the opportunity to cure violations of personal information security breaches within 30 days, but only to the extent the violations are curable.

g Extension of certain exemptions: seeking to temper the CCPA's broad demands, the California legislature has also created a number of exemptions from all or a substantial part of the CCPA – most notably, employee information and B2B information, which were slated to expire at the end of 2021. The CPRA has extended the employee data and business-to-business data exemptions through 2022.

h Expansion of contracting requirements: the CPRA requires businesses to enter into contracts with certain requirements with service providers, contractors and third parties.

i Creation of a new risk assessment and audit requirement: under the CPRA, annual cybersecurity audits are required for businesses whose processing presents a significant risk to consumer privacy or security. Businesses whose processing presents a significant risk to consumer privacy or security may also be required to submit a regular risk assessment to the CPPA.

In the meantime, businesses should focus on complying with the CCPA and the proposed regulations implementing the CCPA's obligations. The California Attorney General, exercising authority explicitly granted to him by the CCPA, has proposed regulations providing further guidance on a number of the CCPA's obligations. In particular, among other things, the regulations provide guidance on required content for privacy policies, requirements for responding to data subject requests and appropriate verification standards for requests. Since the CCPA went into effect on 1 January 2020, then Attorney General Xavier Becerra finalised

51 id. § 1798.120 (d).

52 id. § 1798.140 (w)(2)(B).

53 id. § 1798.155 (b).

the regulations implementing the Act on 14 August 2020 and subsequently proposed several sets of modifications to the regulations, with the most recent modifications being released on 12 October 2020 and 15 March 2021.

Much as with the GDPR, the early days of the CCPA have brought regulatory uncertainty. Even though the proposed regulations were only recently finalised, the office of the California Attorney General began actively enforcing the CCPA on 1 July 2020, sending violation notice letters to a 'swath' of online businesses.[54]

Moreover, since the CCPA went into effect on 1 January 2020, there have been many cases filed around the country that include alleged violations of the CCPA. The vast majority of those cases have been filed in federal courts in California. The rate at which the cases were filed was initially slow, but began to pick up throughout the year and did not appear to slow down during covid-related shutdowns.

CCPA enforcement under the Attorney General continues, and California is preparing for enforcement of the CPRA: on 17 March 2021, California announced the appointment of the inaugural five-member board for the CPPA. The CPRA rulemaking process is scheduled to begin in the summer of 2021, and thus the CPPA staff is moving swiftly. The deadline for the CPPA to adopt final regulations implementing the CPRA is 1 July 2022.

Other state privacy laws

California has long been a privacy bellwether, as its legislative actions have often prompted other states to follow suit: for example, California was the first state to enact a data breach notification law, and all 50 states now have one. It is thus unsurprising that the passage of the CCPA has prompted numerous other states to consider privacy legislation. Nevada became the first state to follow the CCPA trend when, on 29 May 2019, it enacted a law that grants consumers the right to opt-out of the sale of personal information. While Nevada's law is not as comprehensive as the CCPA, it entered into force earlier on 1 October 2019.[55] Recent amendments to the law, signed by the Nevada Governor, include exemptions of certain persons and information collected about a consumer from the law's privacy requirements, expansion of the types of entities that must facilitate consumer privacy opt-out rights, provision of new and updated definitions, authorisation of the opportunity to remedy a failure to comply with certain requirements and updated provisions to reflect the addition of data broker entities.[56] Maine also followed California's footsteps, with the Governor signing into law the 'Act to Protect the Privacy of Online Consumer Information' on 6 June 2019, which officially went into effect on 1 July 2020 (although Maine's Attorney General agreed to delay enforcement until 1 August 2020 due to covid-19).[57] Again, this law is not as comprehensive as the CCPA, but it does obligate internet service providers in Maine to obtain permission from their customers before selling or sharing their data with a third party.

More recently, Virginia became the second state to pass comprehensive privacy legislation. On 2 March 2021, Governor Ralph Northam signed into law the Virginia Consumer Data Protection Act (VCDPA).[58] The VCDPA, which will not enter into effect

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

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

56 S.B. 260, 81st Leg., Reg. Sess. (Nev. 2021).

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

58 S.B. 1392, Special Sess. No. 1 (Va. 2021).

until 1 January 2023, borrows heavily from the CCPA and the EU'S GDPR – although there are subtle differences. The law contains several new rights and obligations, including the right to opt-out of targeted advertising and profiling, new limits on collection and required appeals process, restrictions on the use of 'sensitive data' and the requirement to conduct data protection assessments for certain processing activities.

Colorado also joined Virginia and California in passing a more comprehensive privacy law with the Governor of Colorado signing the Colorado Privacy Act (CPA) on 7 July 2021.[59] The CPA largely mirrors its predecessors in California and Virginia but includes greater fines (US$20,000 per violation). The CPA will go into effect 1 July 2023 – six months after Virginia's law and the CPRA go into effect. The CPA does not have a private right of action, and the Attorney General is required to promulgate regulations on certain aspects by 1 July 2023. Building on concepts from the CCPA, CPRA, VCDPA and GDPR, Colorado's law, once effective, will grant Colorado consumers the right to access, correct, delete, port and opt-out of certain processing of their personal data. Like the VCDPA, the CPA contains several new rights, including the right to opt-out of targeted advertising and profiling. The CPA will also require covered entities to provide privacy policy disclosures and create data protection assessments for certain types of processing activities.

While privacy legislative initiatives have fizzled out in some places, a number of states are considering comprehensive privacy bills, including Massachusetts, New York, North Carolina and Pennsylvania. Moreover, in July 2021, the Uniform Law Commission (ULC) voted to approve the Uniform Personal Data Protection Act (UPDPA). The UPDPA is a model data privacy bill designed to provide a template for uniform state privacy legislation.[60] After some additional amendments, the model law will be ready for introduction in state legislatures in January 2022 and, if adopted by states, will be binding law. Additionally, as happens most years, a number of states have also passed amendments to their data breach notification laws or had such amendments enter into force, offering another reminder of the fact that businesses must continually try to stay on top of the various state law requirements in this area.[61] Several states have also passed laws adopting prescriptive data security requirements for insurers that generally track the Insurance Data Security Model Law adopted by the National Association of Insurance Commissioners (NAIC).[62]

States are continuing to take the lead in regulating emerging technologies, with a prime example of this being facial recognition technologies. On 31 March 2020, the Governor of Washington state signed into law SB 6280, a bill aimed at regulating state and local government agencies' use of facial recognition services.[63] The law contains safeguards that ensure testing, transparency and accountability for the uses of facial recognition technology and includes various measures to uphold fundamental civil liberties. In June 2021, both chambers of Maine's legislature unanimously enacted a bill regulating the use of facial

59 S.B. 21-190, 73rd Leg., Reg. Sess. (Colo. 2021).

60 Uniform Law Commission, Uniform Personal Data Protection Act (July 11, 2021), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=009e3927-eafa-3851-1c02-3a05f5891947&forceDialog=0 .

61 See, e.g., H.B. 5310, Gen. Assemb. Reg. Sess. (Conn. 2021); H.B. 3746, 2021 Leg., 87th Sess. (Tex. 2021).

62 H.B. 6491, 2018 Leg., 99th Sess. (Mich. 2021); Maine Insurance Data Security Act, L.D. 51, 2021 Leg., 130th Sess. (Me. 2021); Iowa Insurance Data Security Act, H.F. 719, 89th Gen. Assemb. Reg. Sess. (Iowa 2021); S.B. 2075, 2021 Leg., 67th Sess. (N.D. 2021).

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

recognition technology, which goes into effect 1 October 2021. Maine's new facial recognition law strictly regulates how law enforcement agencies can employ the technology for their investigations in the state. The law also prohibits government use of facial recognition law in public schools and in many areas of government, including for surveillance purposes, and adds accountability measures.[64] Although Virginia, Massachusetts and Washington legislatures have also banned some police use of facial recognition technology, they fall short of regulating the technology in schools and other state agencies.

Additionally, while Texas, Washington and Illinois have already enacted statutes governing biometric data directly, many other states indirectly regulate biometric data by including it in their statutory definitions of personal information. At the time of writing, many states currently have BIPA-modelled legislation pending, including South Carolina. These laws, which generally require notice and opt-out, limitations on the commercial use of acquired biometric data, destruction of the data after a certain amount of time, and employment of industry standards of care to protect the data, are likely continue to be an area of focus.

State data protection actions

Besides taking the lead on enacting broad, cross-sectoral privacy and data security legislation and updating their data breach notification laws, states are also taking the lead in putting in place and enforcing cybersecurity regulatory regimes. One regulator that has been active in this space has been the New York Department of Financial Services (DFS). With its ground-breaking Cybersecurity Regulation, which took effect in March 2017, DFS is now actively enforcing its prescriptive cybersecurity requirements. DFS filed its first enforcement action on 21 July 2020 against First American Title Insurance Company, and First American has opted to litigate its action with DFS. A hearing before a DFS-appointed administrative judge was scheduled for August 2021.

At the time of writing, DFS has also brought actions and entered into settlements with three additional regulated entities. In March 2021, DFS announced a settlement with Residential Mortgage Services.[65] DFS alleged an unreported 2019 phishing attack in its 2020 examination of the company. Among other items, Residential Mortgage Services agreed to pay a US$1.5 million penalty. The following month, DFS announced a settlement with National Securities.[66] DFS alleged that National Securities failed to implement multifactor authentication as required under the Cybersecurity Regulation until well after the compliance deadline, failed to timely notify DFS of two cyber events, and, as a result of these failures, filed a false certification of compliance with the Cybersecurity Regulation for 2018. Among other items, National Securities agreed to pay a US$3 million penalty. Finally, in May 2021, DFS announced a settlement with First Unum and Paul Revere Life Insurance Companies.[67] The insurance companies provided notice to DFS of two phishing attacks in 2018 and 2019. In connection with the incidents, DFS alleged that the companies failed to implement

64 L.D. 1585, 2021 Leg., 130th Sess. (Me. 2021).

65 NYDFS, *In the Matter of Residential Mortgage Services, Inc.*, Consent Order Pursuant to §§ 44 and 44-a, https://www.dfs.ny.gov/system/files/documents/2021/03/ea20210303_residential_mortgage_0.pdf.

66 NYDFS, *In the Matter of National Securities Corporation*, Consent Order, https://www.dfs.ny.gov/system/files/documents/2021/04/ea20210412_national_securities_corp.pdf.

67 NYDFS, *In the Matter of First UNUM Life Insurance Company, et al.*, Consent Order, https://www.dfs.ny.gov/system/files/documents/2021/05/ea20210512_first_unum.pdf.

multifactor authentication (or reasonably equivalent or more secure access controls), and as a result of these failures, the companies' certification of compliance for 2018 was therefore false. Among other items, the companies agreed to pay a US$1.8 million penalty.

DFS was also the first US regulator to issue specific guidance concerning cyber insurance. On 4 February 2021, DFS issued Circular Letter No. 2, which announced a cyber insurance risk framework that describes industry best practices for New York-regulated property and casualty insurers.[68] As cybercrime becomes more common and more costly, this new cyber insurance framework seeks to 'foster the growth of a robust cyber insurance market' to help protect against the growing number of cyber threats faced by organisations in modern life.

Finally, DFS has positioned itself as an active regulator in both the cybersecurity preparedness and cyber risk management arena. On 27 April 2021, the Department issued a report on its investigation into the New York financial services industry's response to the SolarWinds supply chain attack.[69] Shortly after the attack, DFS alerted its regulated entities and made clear its expectation that any 'impacted' regulated entities should report if they used the infected versions of software and provide information to DFS. Upon investigating and receiving information from licensed entities, DFS prepared a report summarising the information gathered by the regulator from interviewing 88 regulated entities and compiling an analysis of effective response tactics and lessons learned, as well as highlighting the importance of vigorous third-party risk management to prevent such attacks.

State courts

Just as the federal courts have decided a number of recent important privacy and data security cases, so too have state courts. While a complete canvas of all of these decisions is beyond the scope of this chapter, highlighting a couple of examples serves to demonstrate the general point. The Illinois Biometric Information Privacy Act (BIPA) provides a private right of action for aggrieved individuals, and the Illinois Supreme Court has held that bare procedural violations of the statute are sufficient to establish standing.[70] A wide range of technology companies, including Facebook, Shutterfly, Snapchat and Google, are finding themselves defending their implementation of facial recognition technology against BIPA claims in Illinois courts.

It remains to be seen how state laws and state courts may be influenced by the Supreme Court's standing decision in *TransUnion v Ramirez*, discussed earlier. The Supreme Court precedent could substantially curtail federal court jurisdiction for CCPA and BIPA cases. Many state courts currently apply standing rules analogous to those of federal courts, so claims based on technical violations of privacy regulations could also be affected by the *TransUnion* precedent. Commentators emphasise that *TransUnion* will likely create procedural challenges for multi-state class actions where the complaint cannot allege that all members of the class

68 NYDFS, *Insurance Circular Letter No. 2 regarding Cyber Insurance Risk Framework* (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.

69 NYDFS, Report on the SolarWinds Cyber Espionage Attack and Institutions' Response (2021), https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf.

70 740 Ill. Comp. Stat. § 14/1 – 99 (2008); *Rosenbach v. Six Flags Ent Corp*, No. 123186, 2019 IL 123186 (Jan. 25, 2019).

suffered the same concrete harm. Notably, however, state courts in California do not follow the federal standing rules, so cases filed under the CCPA or CPRA in state court would not likely be affected by *TransUnion*.

III REGULATORY FRAMEWORK INCLUDING PUBLIC AND PRIVATE ENFORCEMENT

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

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

General consumer privacy enforcement agency – the FTC

Although there is no single omnibus federal privacy or cybersecurity law or designated central data protection authority, the FTC comes closest to assuming that role for consumer privacy in the US.[71] The statute establishing the FTC, the FTC Act, grants the Commission jurisdiction over essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[72] And while the Act does not expressly address privacy or information security, the FTC has interpreted the Act as giving it authority to regulate information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities – and accordingly to play a leading role in laying out general privacy principles for the modern economy.

The FTC has rooted its privacy and information security authority in Section 5 of the FTC Act, which charges the Commission with prohibiting 'unfair or deceptive acts or

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

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

practices in or affecting commerce'.[73] An act or practice is deceptive under Section 5 if there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and the representation or omission is 'material'. The FTC has taken action against companies for deception when companies have made promises, such as those relating to the security procedures purportedly in place, and then not honoured or implemented them in practice. An act or practice is 'unfair' under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition. (This statutory framework for determining when the FTC can penalise a practice as unfair is widely acknowledged to be a cost-benefit analysis test.) The FTC understands unfairness to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context.

A few examples of what the FTC believes constitutes unfair or deceptive behaviour follow. First, the FTC takes the position that, among other things, companies must disclose their privacy practices adequately and that, in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses.[74]

Second, the FTC also takes the position that Section 5 generally prohibits a company from using previously collected personal data in ways that are materially different from, and less protective than, what it initially disclosed to the data subject, without first obtaining the individual's additional consent.[75]

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

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

b maintaining data security and limiting data retention;

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

d express consent before using sensitive data for behavioural advertising.[76]

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

In terms of enforcement, the FTC has frequently brought successful actions under Section 5 against companies that did not adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments, or failed to provide a 'fair' level of security for consumer information.

73 id. at § 5.

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

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

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

Although various forms of relief (such as injunctions and damages) for privacy-related wrongs are available, the FTC has frequently resorted to settling cases by issuing consent decrees. Such decrees generally provide for ongoing monitoring by the FTC, prohibit further violations of the law and subject businesses to substantial financial penalties for consent decree violations. These enforcement actions have been characterised as shaping a common law of privacy that guides companies' privacy practices.[77]

Cybersecurity and data breaches – federal law

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

That said, recent years have brought a flurry of federal action related to cybersecurity. In 2015, Congress enacted the Cybersecurity Information Sharing Act (CISA),[78] which seeks to encourage cyberthreat information sharing within the private sector and between the private and public sectors by providing certain liability shields related to such sharing. CISA also authorises network monitoring and certain other defensive measures, notwithstanding any other provision of law. In addition to CISA, Presidents Obama, Trump and Biden have issued a series of executive orders concerning cybersecurity, which have, among other things, directed the Department of Homeland Security and a number of other agencies to take steps to address cybersecurity and protect critical infrastructure and directed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework.[79] The latter, in particular, has been a noteworthy development: while the NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, there is a general expectation that use of the framework (which is laudably accessible and adaptable) is a best practice consideration for companies holding sensitive consumer or proprietary business data. (The federal government's response to the recent wave of cyberattacks is further detailed in Section II above.)

Specific regulatory areas – federal law

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

a financial information;

b healthcare information;

77 See, for example, Solove and Harzog, supra note 4.

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

79 Exec. Order No. 13636, 78 F.R. 11737 (2013); Exec. Order No. 13718, 81 F.R. 7441 (2016); Exec. Order No. 13800, 82 F.R. 22391 (2017); Exec. Order No. 13873, 84 F.R. 22689 (2019); Exec. Order No. 14028, 86 FR 26633 (2021).

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

We briefly examine each of these categories,[80] and the agencies with primary enforcement responsibility for them, below.

Financial information

The Gramm-Leach-Bliley Act (GLBA)[81] addresses financial data privacy and security by establishing standards pursuant to which financial institutions must safeguard and store their customers' 'non-public personal information' (or 'personally identifiable financial information'). In brief, the GLBA requires financial institutions to notify consumers of their policies and practices regarding the disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties, unless consumers have the right to opt-out or other exceptions apply; and to establish safeguards to protect the security of personal information. The GLBA and its implementing regulations further require certain financial institutions (i.e., banks) to notify regulators and data subjects after breaches implicating non-public personal financial information, often referred to as NPI.

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

The SEC has also increasingly used its broad investigative and enforcement powers over public companies that have suffered cybersecurity incidents. In doing so, the SEC has relied on multiple theories, including that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to do so and that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. Of particular note, in 2018, the SEC published interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors.[82] The SEC has suggested that all public companies adopt cyber disclosure controls and procedures that enable companies to:

a identify cybersecurity risks and incidents;
b assess and analyse their impact on a company's business;
c evaluate the significance associated with such risks and incidents;

80 There are several additional sectoral privacy laws that protect additional types of information – for example, student records, video viewing data and personal information obtained from state departments of motor vehicles – which are not discussed in this chapter. For further information, see, e.g., the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99; the Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. § 2710; and the Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. §§ 2721–2725.

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

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

d provide for open communications between technical experts and disclosure advisers;
e make timely disclosures regarding such risks and incidents; and
f adopt internal policies to prevent insider trading while the company is investigating a suspected data breach.

Healthcare information

For healthcare privacy, entities within the Department of Health and Human Services (HHS) administer and enforce the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[83] as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).[84] Congress enacted HIPAA to create national standards for electronic healthcare transactions, and HHS has promulgated regulations to protect the privacy and security of personal health information. In general, HIPAA and its implementing regulations state that patients generally have to opt-in before covered organisations can share the patients' information with other organisations.

HIPAA's healthcare coverage is quite broad. It defines PHI as 'individually identifiable health information [. . .] transmitted or maintained in electronic media' or in 'any other form or medium'.[85] Individually identifiable health information is in turn defined as a subset of health information, including demographic information, that 'is created or received by a health care provider, health plan, employer, or health care clearinghouse'; that 'relates to the past, present, or future physical or mental health or condition of an individual', 'the provision of health care to an individual', or 'the past, present, or future payment for the provision of health care to an individual'; and that either identifies the individual or provides a reasonable means by which to identify the individual.[86] Notably, HIPAA does not apply to 'de-identified' data.

With respect to organisations, HIPAA places obligations on 'covered entities', which include health plans, healthcare clearing houses and healthcare providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.[87]

Moreover, HIPAA also places obligations on 'business associates,' which are required to enter into agreements, called business associate agreements, to safeguard PHI. A business associate is defined as an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities).[88] Such agreements require business associates to use and disclose PHI only as permitted or required by the agreement or as required by law and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement. The agreements also include numerous other provisions regarding the confidentiality, integrity and availability of electronic PHI.

83 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified and amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).
84 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, 467 (codified in scattered sections of 42 U.S.C. (2009)).
85 45 C.F.R. § 160.103.
86 45 C.F.R. § 160.103.
87 45 C.F.R. § 164.504(f)(3)(iii).
88 45 C.F.R. § 164.103.

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

Information about children

The Children's Online Privacy Protection Act of 1998 (COPPA) applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. The FTC is generally responsible for enforcing COPPA's requirements, which include, among other things, that these website operators post a privacy policy, provide notice about collection to parents, obtain verifiable parental consent before collecting personal information from children and other actions.[89]

Telephone, internet, and other electronic communications and records

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

a the Electronic Communications Privacy Act of 1986 (ECPA) protects the privacy and security of the content of certain electronic communications and related records;[90]

b the Computer Fraud and Abuse Act (CFAA) prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks;[91]

c various sections of the Communications Act protect telecommunications information, including what is known as customer proprietary network information, or CPNI;[92]

d the Telephone Consumer Protection Act (TCPA) governs robocalls and texts;[93] and

e the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act governs commercial email messages, generally permitting companies to send commercial emails to anyone provided that the recipient has not opted out of receiving

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

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

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

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

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

such emails from the company, the email identifies the sender and the sender's contact information, and the email has instructions on how to easily and at no cost opt-out of future commercial emails from the company.[94]

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

Credit and consumer reports

The Fair Credit Reporting Act (FCRA),[95] as amended by the Fair and Accurate Credit Transactions Act of 2003,[96] imposes requirements on entities that possess or maintain consumer credit reporting information or information generated from consumer credit reports. Consumer reports are 'any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility' for credit, insurance, employment or other similar purposes.

The CFPB, FTC and federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency) share authority for enforcing FCRA, which mandates accurate and relevant data collection to give consumers the ability to access and correct their credit information and limits the use of consumer reports to permissible purposes such as employment, and extension of credit or insurance.[97]

ii Privacy and data protection legislation and standards – state law

Oversight of privacy is by no means exclusively the province of the federal government. All 50 US states also engage in some form of privacy and data protection regulation, with particular emphasis on data security and breach notifications. Moreover, state attorneys general have become increasingly active with respect to privacy and data protection matters, often drawing on authorities and mandates similar to those of the FTC. Of particular note, as the largest of the US states, the home to Silicon Valley, and a frequent regulatory innovator, California continues to be a bellwether for US privacy and data protection legislation, with businesses across the United States often applying its regulatory approaches, whether or not they are jurisdictionally required to do so.[98] (To this end, Section II above discusses the highly significant California Consumer Privacy Act of 2018, which went into effect on 1 January 2020, and the recently enacted California Privacy Rights Act, which goes into effect on 1 January 2023.)

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

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

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

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

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

Cybersecurity and data breaches – state law

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

In addition to the data breach notification laws, states have also imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information.[99] For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls.[100] Likewise, as discussed in Section II above, the California Consumer Privacy Act contains security requirements, and a preliminary set of general safeguards went into effect in 2020 in New York, to say nothing of the sector-specific cybersecurity rule issued by New York's Department of Financial Services (DFS). In short, absent pre-emptive federal legislation, we should expect to see states continuing to pass new legislation in this area, creating an increasingly complicated patchwork quilt of state laws for companies to navigate.

General consumer privacy enforcement – 'Little FTCA' analogues

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

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

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

100 201 Mass. Code Regs. 17.00 (West 2009).

Specific regulatory areas – state laws

While, as described above, the federal government has enacted a number of privacy and data protection laws that target particular industries, activities and information types, the diversity of data laws is even greater at the state level. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues, such as biometric information,[101] cyberstalking,[102] data disposal,[103] privacy policies, employer access to employee social media accounts,[104] unsolicited commercial communications[105] and electronic solicitation of children,[106] to name just a few. State attorneys general also frequently issue policy guidance on specific privacy topics. For instance, like the FTC, California has also issued best-practice recommendations for mobile apps and platforms.

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

First, consider cybersecurity standards. New York's Department of Financial Services (DFS) is a key regulator here, recently promulgating safeguards that require banks, insurance companies and other financial service institutions it regulates to create and maintain a cybersecurity programme designed to protect consumers and New York's financial industry.[107] Thus, as of 28 August 2017, all financial institutions regulated by DFS -- which is a wide-range of US financial institutions with a presence in many states -- must create a cybersecurity programme that, among other things, is approved by the board or a senior corporate official, appoint a chief information security officer, limit access to non-public data, and implement guidelines to notify state regulators of cybersecurity or data security incidents within 72 hours. Notably, the New York DFS filed its first enforcement action on 21 July 2020 against First American Title Insurance Company, as well as recently brought actions and entered into settlements with several regulated entities in 2021.

Moreover, a number of states are promulgating similar or even broader cybersecurity requirements. For instance, New York has built upon the DFS standards by enacting the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) on 25 July 2019, which, among other things, requires entities that handle private information to implement a data security programme with 'reasonable' administrative, technical and physical safeguards. The Act's reasonable security requirement went into effect on 21 March 2020. The law is notable for detailing what constitutes reasonable security, providing specific examples of reasonable

101 *National Law Review*, 'The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020', https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

102 National Conference of State Legislatures, *Cybersecurity Legislation 2021*, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx.

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

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

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

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

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

safeguards. The SHIELD Act also makes clear that entities in compliance with data security frameworks under certain federal or state laws (such as GLBA and HIPAA) are in compliance with the SHIELD Act.

Second, consider privacy policies. As is typical, California plays an outsized role here, with its California Online Privacy Protection Act (CalOPPA) almost serving – as many of its laws do – as a de facto national standard and thus affecting businesses operating throughout the United States.[108] In short, CalOPPA requires operators to post a conspicuous privacy policy online that identifies the categories of personally identifiable information that the operator collects about individual consumers. The privacy policy must also detail how the operator responds to a web browser 'do not track' signal. California law also prohibits websites directed to minors from advertising products based on information specific to that minor, and the law further requires the website operator to permit a minor to request removal of content or information posted on the operator's site or service by the minor, with certain exceptions.[109]

While California's privacy policy laws are likely the most prominent, they do not stand alone. For instance, Connecticut law requires any person who collects social security numbers in the course of business to create a publicly displayed privacy protection policy that protects the confidentiality of the sensitive number. Nebraska and Pennsylvania have laws that prohibit the use of false and misleading statements in website privacy policies.[110] And there are many other state laws concerning privacy policies, making this an excellent example of the many and diverse regulations that may be relevant to businesses operating across multiple US states.

iii Private litigation

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

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

A full discussion of the many potential causes of action granted by US law is beyond the scope of this chapter, but a few examples will suffice to show the range of possible lawsuits. For example, plaintiffs often sue under state 'unfair and deceptive acts and practices' standards, and state law also allows plaintiffs to bring common law tort claims under general misappropriation or negligence theories. Moreover, as mentioned at the outset, US courts have long recognised privacy torts, with the legal scholar William Prosser building on the famed work of Brandeis and Warren to create a taxonomy of four privacy torts in his 1960

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

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

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

article, 'Privacy'[111] – a taxonomy that was later codified in the American Law Institute's famous and influential Restatement (Second) of Torts.[112] Thus, aggrieved parties can generally bring a civil suit for invasion of privacy (or intrusion upon seclusion), public disclosure of private facts, being cast in a 'false light', and appropriation or infringement of the right of publicity or personal likeness. Importantly, these rights protect not only the potential abuse of information, but generally govern its collection and use. However, not all states recognise all the common law torts. For example, New York does not recognise a legal claim for publication of private facts.

iv Industry self-regulation: company policies and practices

To address concerns about privacy practices in various industries, industry stakeholders have worked with the government, academics and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively developed accountability programmes establish expected practices for the use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. While there are obviously limits to industry self-regulation, these initiatives have led to such salutary developments as the Digital Advertising Alliance's 'About Advertising' icon and a policy on the opt-out for cookies set forth by the Network Advertising Initiative.[113]

Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. It should be noted that the same is true for companies that publish privacy policies – a company's failure to comply with its own privacy policy is, quintessentially, a deceptive practice. To this end, as noted above, California law requires publication or provision of a privacy policy in certain instances, and numerous other state and federal laws do as well, including, inter alia, the GLBA (financial data) and HIPAA (health data).[114] 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 deception or detrimental reliance on those policies.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The changing privacy zeitgeist has altered not only the privacy and data protection regime within the United States, but it also threatens to change how the United States approaches certain transfers of information between the United States and other countries. There are no significant or generally applicable international data transfer restrictions in the United States. That said, the United States has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by other countries. In particular,

111 William L Prosser, 'Privacy,' 48 *Calif. L. Rev.* 383 (1960).

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

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

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

the United States was approved in 2012 as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC's Office of International Affairs further works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[115]

Significantly, however, on 16 July 2020, the Court of Justice for the European Union (CJEU) decided *Data Protection Commissioner v. Facebook Ireland, Max Schrems* (*Schrems II*), which held that the EU–US Privacy Shield (a transfer mechanism used by over 5,000 organisations as a mechanism enabling transfers of personal data from the EU to the US) was invalid because the privacy protections guaranteed in principle to individuals under the Privacy Shield programme were not 'essentially equivalent' to privacy rights afforded to such individuals under EU law.[116] The Court also required additional protections to be implemented for another key transfer mechanism, called standard contractual clauses (SCCs), requiring organisations to further evaluate and implement supplementary measures to provide additional privacy protections that afford an individual privacy protections that are essentially equivalent to those guaranteed in principle under EU law. Essentially, the CJEU required companies exporting data to the US to conduct legal self-assessments of whether US national security surveillance law interferes with private companies' ability to comply with their SCC obligations for data transfers to the US.

On 4 June 2021, the European Commission adopted a long-awaited set of updated SCCs meant to govern the transfer of personal data between companies in the EU and US. The new SCCs, which are binding EU privacy law, are intended to, among other things, more closely align with the requirements of the GDPR, better reflect the reality of complex processing operations and address the concerns of the CJEU identified in *Schrems II*. Specifically, the new SCCs impose an obligation on data importers to take into account the nature of the data, the company's technical and organisational safeguard measures and its own past experience (if any) with national security data requests. A few weeks after the European Commission issued the updated SCCs, the European Data Protection Board (EDPB) released a set of recommendations on how to perform a *Schrems II* legal self-assessment and what supplementary measures may consist of. The EDPB's recommendations serve as non-binding, harmonised guidance from Member State privacy regulators responsible for enforcing EU privacy law. The EDPB's recommendations guide companies through a six-step process they should undertake before transferring data to the US, including how to assess the risk that third-country national security access to the transferred data might not be protected in an equivalent manner to rights guaranteed in principle by the EU.

Some of the long-term implications of *Schrems II* remain unclear. Regulators on both sides of the Atlantic have preached calm, and the US government and the EU leadership have also committed to work cooperatively together to address the consequences of the Schrems II decision and develop a successor programme to the Privacy Shield. At a recent summit in Brussels between President Biden and the EU leadership, the parties issued a joint statement

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

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

committing to ensure cross-border data flows and enhance privacy protections, and 'to continue to work together to strengthen legal certainty in Transatlantic flows of personal data'.[117] The US Commerce Department Secretary, who is responsible for the negotiations to replace the Privacy Shield, also travelled to Brussels and met with her EU counterpart. The resulting joint statement also emphasised the 'shared commitment to find a comprehensive successor to Privacy Shield that is fully in line with the *Schrems II* requirements and with US law'. Commentators state that a political agreement could be reached before the end of the year, but warn of a possible '*Schrems III*' debacle.

Another cross-border issue that has experienced recent activity is law enforcement access to extraterritorial data. Historically, the mutual legal assistance treaty (MLAT) system has governed cross-border transfers of data for law enforcement purposes. In recent years, however, the rise of cloud computing has led to more and more data being stored somewhere other than the jurisdiction in which it was created, placing strain on the system as the antiquated MLAT process was insufficiently nimble to keep up with the increased demand. Other countries therefore became increasingly concerned about their inability to obtain timely evidence, as US technology companies frequently held the relevant information but were barred by US law from turning it over to foreign governments without going through the MLAT process.

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

Given the prospect of US industry facing this twin dilemma, as well as the desire of foreign governments to address the concerns caused by the current operation of the MLAT process, Congress enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[118] The CLOUD Act was designed to serve two purposes. First, it clarified that a US search warrant could compel companies to disclose certain communications and records stored overseas, thereby mooting the case before the Supreme Court. Second, the CLOUD Act addressed the converse issue – foreign government access to information held in the United States – by authorising the executive branch to enter into international agreements that would allow for certain, approved foreign nations to obtain content directly from US companies without going through the MLAT process.

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

117 White House Briefing Room, U.S.-EU Summit Statement, (June 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

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

providers' in the jurisdiction of the other government.[119] In addition, on 24 June 2021, the Australian parliament passed legislation establishing a framework for its enforcement agencies to access certain electronic data held by companies outside of Australia for law enforcement and national security purposes. Commentators note that this law paves the way for the establishment of a bilateral agreement with the US under the CLOUD Act. The Australian government has been negotiating this agreement with the US since 2019.

Beyond the one agreement with the UK, the CLOUD Act's clarification of the extraterritorial reach of US law enforcement process has caused consternation, as companies that store data outside the United States have been pressed by non-US customers and counterparts to explain whether the CLOUD Act creates new risk that their data may now be within reach of the US government. The US Department of Justice has thus recently taken steps to explain that, in its view, the CLOUD Act broke no new ground and only clarified, rather than expanded, the reach of US law enforcement; and that, in any event, the requirements in the United States for obtaining a warrant for the content of electronic communications are perhaps the toughest in the world and are highly protective of individual privacy.[120]

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

V COMPANY POLICIES AND PRACTICES

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

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

While not so long ago companies were comfortable with IT and legal departments running the show with respect to privacy issues, they are now increasingly elevating the level

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

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

of attention these issues receive and involving senior management and the board in oversight and decision making. The examples of this are legion, and the below are just a few examples.

a Microsoft has created a technology and corporate responsibility team that reports to the president and provides guidance to the board and management on ethical business practices, privacy and cybersecurity.[121]

b Microsoft and other companies have put in place internal boards to help oversee and navigate the challenging moral, ethical and practical issues raised by artificial intelligence.[122]

c Numerous companies, including Walmart, BNY Mellon and AIG, have put in place technology committees of their board, with responsibility for, among other things, reviewing IT planning, strategy and investment; monitoring and providing guidance on technological trends; and reviewing cybersecurity planning and investment.[123]

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

VI DISCOVERY AND DISCLOSURE

US civil discovery and government access rights are discussed in connection with relevant, recent developments above. In brief, companies may be required under various federal and state laws to produce information to law enforcement and regulatory authorities and in response to civil litigation demands.

Litigants in both federal and state courts are entitled to expansive discovery rights to access nearly all data relevant to the proceeding held by opposing parties, except that privileged information usually only needs to be broadly identified rather than disclosed. Courts routinely enter protective orders to restrict access to and use of highly confidential or personal information. Courts may also quash discovery requests that are deemed unduly burdensome or otherwise unwarranted. Electronically stored information (ESI), including metadata, is subject to discovery. In federal courts, discovery is governed by the Federal Rules of Civil Procedure, in particular, by Rule 26. State courts operate under analogous rules.

Government access to information in private hands is governed by numerous statutes, including the following selection of legal authorities: Fourth Amendment of the

121 We see the big picture, Microsoft Corp (accessed 14 July 2021), https://www.microsoft.com/en-us/corporate-responsibility/governance.

122 AI news and events, Microsoft Corp (accessed 14 July 2021), https://www.microsoft.com/en-us/ai?activetab=pivot1%3aprimaryr5; SAP Becomes First European Tech Company to Create Ethics Advisory Panel for Artificial Intelligence, SAP News (Sept. 18, 2018); https://news.sap.com/2018/09/sap-first-european-tec h-company-ai-ethics-advisory-panel/; Taking an ethical approach to artificial intelligence, Adobe (accessed 14 July 2021), https://www.adobe.com/about-adobe/aiethics.html.

123 Walmart Inc, Technology and Ecommerce Committee Charter (adopted June 2, 2011), https://s2.q4cdn.com/056532643/files/doc_downloads/Gov_Docs/TeCC-Charter[1].pdf; BNY Mellon, Technology Committee: Charter of the Technology Committee of the Board of Directors, The Bank of New York Mellon Corporation (approved Feb. 20, 2020), https://www.bnymellon.com/us/en/who-we-are/corporate-governance/technology-committee.jsp, American International Group, Inc., Technology Committee Charter (effective Sept. 16, 2020), https://www.aig.com/content/dam/aig/america-canada/us/documents/corp-governance/technology-committee-charter-effective-09.16.20.pdf.

US Constitution (searches and seizures of persons, houses, papers and effects), ECPA (wiretapping, collection of stored electronic communications and call records),[124] the Right to Financial Privacy Act of 1978 (banking records),[125] Rule 41 of the Federal Rules of Civil Procedure (search warrants), the Foreign Intelligence Surveillance Act of 1978 (national security communications surveillance),[126] the USA PATRIOT Act (national security business records)[127] and so forth. The Presidential Policy Directive (PPD) 28, regarding Signals Intelligence Activities, extended certain legal protections against excessive government surveillance to foreign citizens.[128]

As discussed in greater detail below in the Considerations for Foreign Organisations section, companies should also consider potential conflicts with data protection or privacy law outside the US when responding to US legal demands and crafting their global privacy and data protection compliance programmes.

Finally, 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.

VII PUBLIC AND PRIVATE ENFORCEMENT

As discussed in greater detail above in the Year In Review and Regulatory Framework sections, the US does not have a central *de jure* privacy regulator; the US system for privacy and cybersecurity litigation and enforcement is carried out by an army of disciplinarians. The FTC and state attorneys general are perhaps the most prominent general-purpose enforcers to protect against abuses of personal information and unfair data practices, although the new CPPA will likely become a force to be reckoned with soon.

Moreover, 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. Specifically, agencies like the FCC, CFPB, SEC, HHS/OCR play a strong role in investigating and enforcing under their respective statutory authorities over personal data and cybersecurity.

Of course, in the US, private litigation may be the ultimate deterrent. The plaintiff's bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of

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

125 The Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641, 3697 (codified at 12 U.S.C. §§ 3401-422 (1978)).

126 The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. ch. 36 § 1801 et seq (1978)).

127 The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107–56, 115 Stat. 272 (codified in scattered titles and sections of the U.S.C.).

128 The White House Office of the Press Secretary, Presidential Policy Directive -- Signals Intelligence Activities (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

corporations doing business with consumers. Class action lawsuits alleging violations of data security obligations, or biometric and telephone consumer protection laws, among many other theories, have produced settlements in the amount of hundreds of millions of dollars.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign organisations can face federal or state regulatory or private action if they satisfy normal jurisdictional requirements under US law, which typically require minimum contacts with or presence in the United States. Additionally, a foreign organisation could be subject to sector-specific laws if the organisation satisfies that law's trigger. For example, if a foreign organisation engages in interstate commerce in the United States, the FTC has jurisdiction, and if a foreign organisation is a publicly traded company, the SEC has jurisdiction. Moreover, US law enforcement and other enforcement agencies have broad ideas about their jurisdiction.[129]

IX CYBERSECURITY AND DATA BREACHES

As discussed in greater detail above in the Year in Review and Regulatory Framework sections, cybersecurity has been the focus of intense attention in the United States in recent years, and the legal landscape is dynamic and rapidly evolving.

In brief, 50 states and various US jurisdictions have enacted data breach notification laws, which have varying notification thresholds and requirements. These laws generally require that individuals be notified, usually by mail (although alternate notice provisions exist), of incidents in which their personal information has been compromised. These laws usually include a notification trigger involving the compromise of the name of an individual and a second, sensitive data element such as date of birth or credit card account number. Several states also require companies operating within that state to adhere to information security standards.

X OUTLOOK

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

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

Appendix 1

ABOUT THE AUTHORS

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and leader of Sidley Austin LLP's highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. He also advises companies on their digital governance strategies and cyber crisis management. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate White House counsel to the President. He currently serves as a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul has also served as a member of the American Bar Association's Cybersecurity Legal Task Force by appointment of the ABA president. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School. Mr Raul is a lecturer on law at Harvard Law School where he teaches a course on digital governance: privacy and technology trade-offs.

SNEZHANA STADNIK TAPIA

Sidley Austin LLP

Snezhana Stadnik Tapia is an associate in Sidley's New York office. Snezhana maintains a hybrid practice that includes privacy and cybersecurity matters, commercial litigation and arbitration, and government enforcement actions and investigations. As a member of Sidley's privacy and cybersecurity group, Snezhana focuses on privacy, cybersecurity and emerging technology matters, including regulatory investigations and compliance counselling regarding evolving laws and regulations, such as the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA) and the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation. Snezhana received her law degree from New York University School of Law.

SIDLEY AUSTIN LLP

787 Seventh Avenue
New York, NY 10019
United States
Tel: +1 212 839 5300
Fax: +1 212 839 5599
sstadnik@sidley.com

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

www.sidley.com

an LBR business

ISBN 978-1-83862-810-9