IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

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

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 21

UNITED STATES

Alan Charles Raul and Sheri Porath Rockwell[1]

I OVERVIEW

Over 130 years ago, two US 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 (which many states have since codified into their statutory tort laws), and it is easy to consider Warren's and Brandeis' 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 enacting the Privacy Act of 1974 to grant certain data subject rights and 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 focused on digital governance in the face of technological and societal change.

---

1 Alan Charles Raul is a partner and Sheri Porath Rockwell is counsel at Sidley Austin LLP. The authors wish to thank Kathryn Allen, Casey Grant, Sasha Hondagneu-Messner, Lauren Kitces, Stephen McInerney, Alexandra Mushka, Mitchell Noordyke, Carly Owens, Cole Rianda, and Rimsha Syeda, associates at Sidley Austin who assisted in drafting this chapter, Joyce Yeager at Sidley, and former Sidley associates Vivek K Mohan, Tasha D Manoranjan, Frances E Faircloth and Snezhana Stadnik Tapia who contributed to prior versions . We also thank Christopher C Fonzone, who co-authored a prior version of this chapter, for his extensive contributions to this current version.

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.

3 Warren and Brandeis, see footnote 2, at p .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), China's Personal Information Protection Law (PIPL) and, more recently, India's Digital Personal Data Protection Act. In the United States, the rapid expansion of artificial intelligence capabilities, new research studies focused on social media and its impact on children and teens, a series of high-profile data breaches in both the public and private sectors and general 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 and cybersecurity.

This past year saw the passage of an unprecedented number of state data privacy laws and the emergence of sector-specific laws focused on children and teens and health data collected by entities not subject to federal health privacy laws (i.e., the Health Insurance Portability and Accountability Act (HIPAA)). Many of these laws, particularly the health privacy laws, have been motivated by concerns in the wake of the US Supreme Court's 2022 decision in *Dobbs vs. Jackson Women's Health Organization* and the proliferation of state and local laws focusing on issues of concern to the LGBTQ+ community. These concerns arise as prosecutors in some states have obtained and used sensitive information and private communications to investigate alleged violations of anti-abortion laws. Federal agencies, particularly the FTC and the Securities and Exchange Commission (SEC), have been active in both privacy and cybersecurity, through proposed rule-making and enforcement actions. Last year's progress on federal privacy legislation has stalled, and it seems unlikely that the US Congress will pass a comprehensive federal privacy law in the near future.

Overall, privacy and cybersecurity issues are increasingly front-of-mind for a larger swath of the US public, and regulators are responding in kind with new proposed laws, regulations and enforcement actions. This chapter, while not providing a comprehensive overview of the rich US privacy and cybersecurity landscape, will show how the US privacy and cybersecurity zeitgeist is shifting through the lens of the concrete developments taking place at the federal, state, and even local levels of government to address increasing concerns around privacy and cybersecurity. The chapter will begin by describing:

a how all three branches of the federal US government are actively taking steps to confront the privacy and cybersecurity questions of the day and the important role federal agency efforts are at the forefront of these changes; and

b how much of the action continues to be not in Washington, DC, but rather in the 50 US states – with 12 states having now passed comprehensive privacy laws. In addition, several states have also passed new laws around health privacy; and children and teen privacy), while others have addressed privacy concerns with laws governing social

media platforms. Enforcement efforts and private litigation under state laws such as the Illinois Biometric Privacy Act continue to address evolving technologies and methods of data collection. On the cybersecurity front, New York again leads the way with updates to its already strict cybersecurity laws for financial institutions regulated by the state's Department of Financial Services.

Note that this chapter provides a basic overview of the existing US regulatory and enforcement framework following an extensive discussion of significant recent developments – there has been very considerable privacy and data protection activity this year. The chapter will also briefly note certain relevant international developments that impact several entities in the US.

II THE YEAR IN REVIEW

As noted at the outset, the privacy and data security zeitgeist in the United States is shifting. 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.

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 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. And, of course, addressing governance of artificial intelligence is looming large over policymakers at all levels from the White House down.

Executive branch – recent enforcement cases and proposed rules

The FTC had another active year with several health-privacy enforcement actions, proposed rule-making to update its Health Breach Notification Rule, biometric privacy guidance, September 2022 hearings on the far-reaching Advanced Notice of Proposed Rulemaking first published for public comment in August 2022 and litigation of its enforcement action against data broker Kochava. Many of the agency's actions highlight increasing concerns about the use of sensitive data and the intersection between data privacy and data protection, with settlements and consent orders that address these concerns.

For much of the year, the FTC was operating with only three Democratic-appointed commissioners: Chair Lina Khan and Commissioners Rebecca Slaughter and Alvaro Bedoya. Republican appointee Christine Wilson resigned from the Commission on 31 March 2023, following the October 2022 resignation of Republican appointee Noah Phillips. In July 2023, President Biden nominated two new Republicans to the Commission: Virginia Solicitor General Andrew Ferguson and Utah Solicitor General Melissa Holyoak. Their nominations are pending Senate approval.

The FTC was not the only agency active this year in the privacy and data protection space. Several agencies, including Health and Human Services, issued guidance and engaged in enforcement actions as described below.

A focus on health data and ad tech – notable developments

The FTC focused much of its privacy enforcement and rule-making efforts this year on online tracking technologies, particularly those used on websites or apps that collect information about physical or mental health. The Commission brought four significant health data privacy enforcement actions that broke new ground. Through these actions, the FTC has put forth an expansive definition of 'health data' to include non-sensitive data elements such as emails and IP addresses when used on health-related mobile applications or websites. The FTC has also used these enforcement actions to attempt to expand the meaning of 'unfair practices' under the FTC Act to include the act of disclosing personal identifiers and information to digital advertising companies without first obtaining consumers' affirmative express consent. In each of these enforcement actions, typically resolved by consent decrees that do not have general applicability but nevertheless inform regulated entities' compliance strategies, the FTC focused on the companies' digital advertising practices, including the types of data that were shared with third parties to effectuate such advertising and whether companies had access controls or internal training programmes concerning the use of health data for advertising purposes. Also at issue were claims that several of the companies engaged in deceptive practices because they disclosed in their privacy policies that they did not share health data with third parties but allegedly did engage in such sharing by virtue of sharing user data with digital advertising companies. Each of these enforcement actions resulted in settlements that included monetary damages and injunctive relief that, in several of the matters, included lifetime bans on engaging in digital advertising.

This year also marked the first time the FTC enforced its Health Breach Notification Rule. In an action against GoodRx Holdings, Inc, a digital health platform that offers prescription drug discounts, telehealth visits and other health services, the Commission alleged the presence of third-party tracking pixels on the company's website 'breached the security' of consumers' health information by transmitting such data to third parties without consumers' authorisation and without notifying consumers of the alleged breach.[4] The matter was settled, and the stipulated order includes monetary penalty of US$1.5 million in addition to injunctive relief that includes a permanent prohibition against sharing of health data for advertising, breach notification obligations, requirements that third party ad tech platforms delete health information GoodRx shared with them and limits on the disclosure of health information for non-advertising purposes without consent.[5] Several months later, the FTC brought its second enforcement action under the Health Breach Notification Rule against a fertility app that allegedly shared health information through the use of SDKs and shared health information for advertising without first obtaining users' consent.[6]

On the heels of these enforcement actions, the FTC announced proposed updates to the Health Breach Notification Rule, the first since the Rule was first issued in 2009. The proposed updates seek to clarify the Rule's application to mobile health applications

4 Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief, *United States of America v. GoodRx Holdings, Inc.*, Case No. 3:23-cv-460 (N.D. Cal. 1 February 2023).

5 Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, *United States of America v. GoodRx Holdings, Inc.*, Case No. 3:23-cv-460 (N.D. Cal. 1 February 2023).

6 Federal Trade Commission, *Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order* (17 May 2023).

and health technologies.[7] Among the proposed revisions, the revised Rule would require in-scope entities to notify consumers if an unauthorised disclosure of health data occurs, authorises that such notice be provided electronically, and that the notice describe any potential for harm and the steps the vendor of personal health records is taking to protect affected individuals. As alleged in recent enforcement actions under the HBNR, a breach of unsecured health information, as defined in the HBNR, could arguably consist of the transmission or collection of personal data using common digital advertising technologies on a website or mobile application.

The FTC continued its focus on the use of digital advertising technologies with respect to health data when, in July 2023, it joined with the Department of Health and Human Services' Office of Civil Rights (which enforces HIPAA) to issue letters to 130 companies regarding the 'privacy and security risks related to the use of online tracking technologies' on websites and mobile applications.[8] The letter 'strongly encourage[d]' recipients to review applicable laws applicable to such technologies and take steps to ensure compliance.

The Department of Health and Human Services, through its Office of Inspector General, also published its final rule establishing penalties for 'information blocking', which the 21st Century Cures Act defines to mean a practice that is likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information, when conducted by entities offering health information technologies and others facilitating access to electronic health records.[9] The rule provides for penalties up to US$1 million per penalty per violation.

Litigation of Kochava enforcement action

In May 2023, a federal judge in Idaho dismissed, with leave to amend, the FTC's lawsuit against data broker Kochava. The lawsuit alleged the company's collection and sale of geolocation data violated the FTC Act's unfairness provisions.[10] The court found that the FTC had not sufficiently pleaded that the company's alleged sale of data created a 'significant risk' of concrete harm.

In July 2023, the FTC filed an amended complaint against Kochava and did so under seal, alleging the amended complaint might reveal Kochava's trade secrets.[11] Soon thereafter, Kochava filed a motion to dismiss the amended complaint, which is still being briefed by the

7 FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (18 May 2023) at https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

8 FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies (20 July 2023) at https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

9 U.S. Dept. of Health and Human Services – Office of Inspector General, Information Blocking (5 July 2023) at https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/#:~:text=The%20final%20rule%20establishes%20the,impose%20new%20information%20blocking%20requirements.

10 Memorandum Decision and Order, *Federal Trade Commission v. Kochava, Inc.*, No. 2:22-cv-00377-BLW (D. Idaho 4 May 2023).

11 First Amended Complaint, *Federal Trade Commission v. Kochava, Inc.*, No. 2:22-cv-00377-BLW (D. Idaho 5 June 2023).

parties.[12] This litigation represents one of the few instances in recent history where a business has pushed back against an FTC privacy enforcement action, rather than agree to settle and enter into a lengthy consent order.

Hearings and the close of comments regarding the 2022 Advanced Notice of Proposed Rulemaking

On 11 August 2022, the FTC released its Advanced Notice of Proposed Rulemaking (ANPR) seeking public input on nearly 100 separate questions on a range of topics related to 'surveillance and lax data security', including how and whether the Commission should regulate digital advertising and automated decision-making systems, alternative approaches to regulation of digital technologies, how to quantify damages and harm with tracking technologies and whether formal rule-making should be initiated on data security issues.[13] The Commission held a public forum to discuss the ANPR on 8 September 2022 and accepted comments until 14 October 2022.

New biometric privacy guidance

In mid-2023, the FTC also released a new Biometric Policy Statement that highlights potential risks in the use of biometric information technologies, including when used for purposes other than identification, and the factors the FTC will consider in determining whether these technologies constitute an 'unfair' practice in violation of the FTC Act.[14] The policy signalled an expansion of the FTC's unfairness doctrine, as it focused on actions businesses take before the collection of biometric information and obligations to continue to evaluate and monitor, with some regularity, the impact of technologies that collect such data and to do the monitoring in environments that 'mirror[] real world implementation and use', including the 'role of human operators'.[15]

Notable developments in children's privacy and ed tech

The Federal Trade Commission undertook several enforcement actions related to the privacy of minors this year. In its action against Microsoft based on its Xbox gaming system, the Commission asserted an expansive view of the Children's Online Privacy Protection Act (COPPA), the US federal privacy rule that applies to entities that collect personal information online from children under the age of 13. In the Xbox action, FTC applied COPPA to information collected on gaming platforms and treated avatars as personal information.[16] In

12 Motion to Dismiss for Failure to State a Claim, *Federal Trade Commission v. Kochava, Inc.*, No. 2:22-cv-00377-BLW (D. Idaho 5 July 2023).

13 FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (11 August 2023), at https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

14 FTC Warns About Misuses of Biometric Information and Harm to Consumers (18 May 2023) at https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

15 Federal Trade Commission, Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act (18 May 2023) at https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

16 FTC Business Blog, $20 million FTC settlement addresses Microsoft Xbox illegal collection of kids' data: A game changer for COPPA compliance (5 June 2023) at https://www.ftc.gov/business-guidance/blog/2023/06/20-million-ftc-settlement-addresses-microsoft-xbox-illegal-collection-kids-data-game-changer-coppa.

another COPPA enforcement action, the FTC filed suit against ed tech provider Edmodo and took the position that COPPA compliance is the responsibility of ed tech operators, not the schools that use their services.[17]

The FTC's actions this year reflect the growing concerns in society about the privacy of teenagers, not just children under 13 which have been the focus of children's privacy laws in the US since the passage of COPPA 25 years ago. In December 2022, the FTC filed suit against Epic Games under COPPA and the FTC Act based on features in the company's Fortnite application that allegedly allowed children and teens to connect with strangers.[18] The settlement requires Epic Games to implement certain privacy defaults for individuals under the age of 18, which may only be changed with the affirmative express consent of a child's parent or a teenager (or the teen's parent). The focus on teen privacy was also evident in the FTC's May 2023 proposal to modify its 2020 privacy order with Facebook by, among other things, restricting the company's use of data collected from users under the age of 18.[19] Facebook has until November 2023 to file a response to the FTC's Order to Show Cause as to why the FTC should not modify the 2020 privacy order.[20]

Cybersecurity

The Biden administration and federal agencies remain actively engaged in cybersecurity matters. In March 2023, the Biden administration announced its long-awaited National Cybersecurity Strategy, a policy document that signals a path to the future, but does not have the force of law.[21] It proposes two fundamental shifts in present cybersecurity policy: (1) rebalancing the risks of cybersecurity threats toward industry and the government rather than end users; and (2) realigning incentives to promote long-term investments in resilient, defensible systems. Administration officials noted that the Strategy 'reimagines the American cybersocial contract' and reflects a 'fundamental recognition' that the voluntary approach to securing critical infrastructure is inadequate.[22] In July 2023, the White House released the National Cybersecurity Implementation Plan, a roadmap to achieve the objectives of the

17 FTC Business Blog, Oh no, you don't, Edmodo: FTC sues ed tech company for violating school kids' privacy (22 May 2023) at https://www.ftc.gov/business-guidance/blog/2023/05/oh-no-you-don t-edmodo-ftc-sues-ed-tech-company-violating-school-kids-privacy.

18 FTC Business Blog, Record-setting FTC settlements with Fortnite owner Epic Games are the latest "Battle Royale" against violations of kids' privacy and use of digital dark patterns (19 December 2022) at https://www.ftc.gov/business-guidance/blog/2022/12/record-setting-ftc-settlements-fortnite-owner-epic-games-a re-latest-battle-royale-against-violations.

19 FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (3 May 2023) at https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventin g-facebook-monetizing-youth-data.

20 In the Matter of Facebook, Order Granting Respondent's Second Request for Extension of Time in Which to File its Answer to the Commission's Order to Show Cause, Docket No. C-4365 (Fed. Trade Comm. 13 July 20230).

21 FACT SHEET: Biden–Harris Administration Announces National Cybersecurity Strategy (2 March 2023) at https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harri s-administration-announces-national-cybersecurity-strategy/.

22 New York Times, *New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms* (2 March 2023) at https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

Strategy that describes various initiatives underway in various federal agencies, with timelines for completion.[23] Among other things, the Plan includes an initiative to explore shifting liability from users of software products to the companies that develop software.

In July 2023, the Security and Exchange Commission (SEC) finalised its rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (the Final Rule).[24] The Final Rule applies to all publicly traded companies subject to the reporting requirements of the Securities Exchange Act of 1934 and will require public disclosure of material cybersecurity incidents and periodic disclosure of cybersecurity risk management, strategy, and governance in annual reports filed with the SEC. Among the more notable features is that companies must disclose material cybersecurity incidents on a publicly filed form within four business days of a determination of materiality, absent a determination from the US Attorney General of a substantial risk to national security or public safety.

In 2023, the SEC also proposed amendments to its privacy and safeguards rules as applied to broker-dealers and investment advisers. The proposed amendments would strengthen cybersecurity requirements, impose data breach notification requirements for the first time, and make changes to provisions concerning the disposal of consumer report information by SEC-registered transfer agents.[25]

In June 2023, the FTC's updated Safeguards Rule, which was finalised in 2022, went into effect. The new rule requires certain 'catch-all' financial institutions (i.e., that are not banks, insurance companies, SEC-regulated entities, etc.) to strengthen cybersecurity practices by, among other things, assessing security risks, implementing access-controls, evaluating vendors' security practices and implementing multi-factor authentication for access to customer information.[26]

On 29 June 2023, the US Commodity Futures Trading Commission (CFTC) Division of Enforcement Director announced the establishment of a Cybersecurity and Emerging Technologies Task Force to be staffed with agency attorneys and investigators who will serve as subject matter experts and prosecuting cases. The goals of the task force include (1) ensuring entities subject to the jurisdiction of the CFTC have sufficient cybersecurity

23 FACT SHEET: Biden–Harris Administration Publishes the National Cybersecurity Strategy Implementation Plan (13 July 2023) at https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/13/fact-sheet-biden-harrisadministration-publishes-thenational-cybersecurity-strategyimplementation-plan/.

24 SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (26 July 2023) at https://www.sec.gov/news/press-release/2023-139; Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216, 88 FR 51896 (26 July 2023).

25 Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, 88 FR 20212 (5 April 2023) at https://www.federalregister.gov/documents/2023/04/05/2023-05767/cybersecurity-risk-management-rule-for-broker-dealers-clearing-agencies-major-security-based-swap.

26 Standards for Safeguarding Customer Information, 16 C.F.R. Part 314.

controls, including controls surrounding customer information and systems safeguards; and (2) exploring and overseeing those entities' use of technologies such as artificial intelligence and machine learning.

Artificial intelligence and algorithmic decision making

The White House and various federal agencies also continued to grapple with how to regulate the proliferation of artificial intelligence technologies (AI). On 26 January 2023, the National Institute of Standards and Technology (NIST) issued Version 1.0 of its Artificial Intelligence Risk Management Framework (the AI RMF).[27] The AI RMF outlines types of risks concerning AI, enumerating seven key principles to ensure trustworthy AI: safe, secure and resilient; explainable and interpretable; privacy-enhanced; fair; accountable and transparent, valid and reliable). It also offers a set of organisational processes and activities to assess and manage risk, mainly by breaking them down into core functions – to govern, map, measure and manage.

In October 2022, the White House issued its Blueprint for an AI Bill of Rights, a set of principles and associated practices to help guide the development of AI.[28] These principles focus on safety, preventing algorithmic discrimination, transparency and privacy, including implementing privacy by design, providing rights to access, delete and correct data used by AI systems and auditing of the efficacy of privacy protections.

In July 2023, the White House announced it had secured voluntary commitments from seven of the leading US AI companies to develop their AI systems in line with the goals of the Blueprint, including by ensuring safety and transparency in the AI systems they develop, working to avoid risks of bias and discrimination, and implementing privacy protections.[29]

In May 2023 the US Department of Commerce National Telecommunication and Information Administration (NTIA) issued an AI Accountability Policy Request for Comment, seeking feedback on policies that can help the development of AI audits, assessments, certifications, and other mechanisms to create trust in AI systems. The request seeks to understand which measures, regulatory and self-regulatory, can be used to ensure AI systems are 'legal, effective, ethical, safe, and otherwise trustworthy'.[30]

The SEC has also joined efforts to regulate AI technologies. In August 2023, the agency issued proposed rules for broker-dealers and investment advisers regarding the use of predictive data analytics and similar technologies in interactions with investors.[31] The proposed rules focus on the potential for these technologies to create conflicts of interest

27 Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023) at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

28 Blueprint for an AI Bill of Rights (October 2022) at https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

29 FACT SHEET: Biden–Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (21 July 2023) at https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

30 AI Accountability Policy Request for Comment (11 April 2023) at https://www.ntia.gov/issues/artificial-intelligence/request-for-comments.

31 SEC Proposes New Requirements to Address Risks to Investors From Conflicts of Interest Associated With the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers (26 July 2023) at https://www.sec.gov/news/press-release/2023-140.

as between the broker-dealer and investment adviser, on the one hand, and natural person investors, on the other. They require broker-dealers and investment advisers to 'eliminate or neutralize' any identified conflicts, among other things.

Employee privacy and algorithmic decision-making

The use of emerging technologies in the employment context is a concern for the US top employment regulator, the Equal Employment Opportunity Commission (EEOC). In January 2023, the EEOC held a three-hour commission meeting focused on the use of automated decision tools in the employment context, in which it described this area as the 'new civil rights frontier' and heard testimony from academics, civil society groups and business representatives regarding the use these technologies in the employment context and the role the EEOC might play in regulating them.[32] The agency continued to provide guidance regarding how to identify and manage bias in software tools that incorporate algorithmic decision-making at various stages in the employment process, consistent with its goals as articulated in its 2021 Artificial Intelligence and Algorithmic Fairness Initiative.[33] In early 2023, the EEOC also announced it would focus its enforcement efforts in the coming years on the use of automated systems, including artificial intelligence or machine learning, in the employment context.[34] Additionally, the EEOC settled its first enforcement action based on the use of automated tools. The agency alleged that a group of employers had programmed job applicant screening software to automatically reject applicants over the ages of 55 (women) and 60 (men).[35] We expect more movement from the EEOC and other agencies relating to the use of AI and machine learning tools in the employment context in the years to come.

Legislative actions

There has not been any meaningful progress on comprehensive federal privacy legislation after the failure to pass such legislation last year. Sectoral privacy bills have largely replaced efforts at broad federal legislation, with several bills focusing on the privacy of minors, both online and in the classroom. These proposals mirror legislative trends in the states.

With respect to children's privacy, bills advanced in Congress sought to expand protections to teens under 18 years of age and focused on provisions that would limit advertising to minors and require more stringent age verification provisions.[36]

Bills focused on artificial intelligence also surfaced, several with bipartisan sponsorship, reflecting generalised concerns about the rapid acceleration of these technologies. The bills include provisions that would require agencies to disclose when they are using AI technologies

32 Navigating Employment Discrimination in AI and Automated Systems: A New Civil Rights Frontier (31 January 2023) at https://www.youtube.com/watch?v=rfMRLestj6s and https://www.eeoc.gov/newsroom/eeoc-hearing-explores-potential-benefits-and-harms-artificial-intelligence-and-other.

33 Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964 (2023) at https://www.eeoc.gov/select-issues-assessing-adverse-impact-software-algorithms-and-artificial-intelligence-used;.

34 EEOC Draft Strategic Enforcement Plan, 88 Fed. Reg. 1379 (1 January 2023) at https://www.federalregister.gov/documents/2023/01/10/2023-00283/draft-strategic-enforcement-plan.

35 Joint Notice of Settlement and Request for Approval and Execution of Consent Decree, *EEOC v. iTutor*, *et al.*, Case No. 1:22-cv-2656 – PKC-PK (E.D.N.Y. 9 August 2023).

36 Kids PRIVACY Act, H.R. 2801, 118th Cong (2023).

that interact with individuals and establish chief AI officer positions at each agency. Proposals also include the establishment of a federal Office of Global Competition Analysis to bolster US efforts to stay competitive on the global stage with respect to AI technologies.[37]

Judicial branch – a new threat to agency rule-making

The biggest privacy news from the US Supreme Court this year may have been what the Court declined to do in a case involving a California law, Proposition 12, enacted to prohibit the sale of pork in California if pigs are housed in poor conditions. Petitioners alleged that the Proposition 12 violated the dormant Commerce Clause in the US Constitution by imposing an 'impermissible extraterritorial effect' or 'excessive burden' on interstate commerce because it burdened pig farmers in states other than California. Privacy advocates were keenly focused on this case because they feared the same theory could potentially be used to invalidate the far-reaching CCPA which many argued creates significant burdens on businesses outside the state. In the end, the US Supreme Court upheld the law.[38]

Federal courts around the country experienced a surge of putative class action suits based on the use of the pixels from companies like Meta and Google, especially in the healthcare and financial services fields. These suits allege that pixel technologies that share information with third-party advertising platforms about website visitors' conduct on a website, which can be used for targeted advertising and analytics, allegedly violate health privacy laws (e.g., HIPAA) and financial privacy laws, among others. Several suits were filed in the wake of investigatory reporting about the widespread use of pixel technologies on websites of hospitals and online tax preparation services.[39]

Pixel technology has also been central to new litigation under the federal Video Privacy Protection Act (VPPA). The VPPA, enacted first in the era of video tape rental stores, requires 'video tape service providers' to obtain consent from consumers before disclosing video viewing histories and includes a private right of action with statutory penalties. Plaintiffs' lawyers have brought hundreds of putative class actions under the VPPA, alleging that the use of embedded videos in websites violates the statute. This year saw some courts dismiss VPPA claims on the pleadings, ruling that companies that post videos for brand awareness or in ways that are ancillary to its business are not 'video tape service providers' within the meaning of the law.[40] However, as in pixel- and wiretapping-related cases (see below), VPPA rulings are by no means consistent, with some courts allowing similar claims to proceed to trial.

Federal courts also continued to hear claims based on state wiretapping laws, particularly under the California Invasion of Privacy Act (CIPA), with sometimes conflicting rulings being issued by district courts in the Ninth Circuit, none of which have been litigated to trial and successfully appealed. These suits, brought under CIPA's private right of action

37 Committee Passes Peters & Cornyn Bipartisan Bill to Ensure Federal Government is Properly Using and Managing Artificial Intelligence (27 July 2023) at https://www.hsgac.senate.gov/media/dems/committee-passes-peters-cornyn-bipartisan-bill-to-ensure-federal-government-is-properly-using-and-managing-artificial-intelligence/.

38 *National Pork Producers Council, et al. v. Ross, Secretary of the California Department of Food and Agriculture*, 598 U.S. __ (2023).

39 The Markup, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites* (16 June 2022, upated 19 July 2023) at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites; The Markup, *Tax Filing Websites Have Been Sending Users' Financial Information to Facebook* (22 November 2022; updated 28 November 2022).

40 Order Granting Motion to Dismiss, *Carroll v. General Mills, Inc.*, 2:23-cv-01746 (C.D. Cal. 26 June 2023).

that provides for statutory penalties, seek to apply provisions in state wiretap law to internet communications and the technologies used by service providers and website operators to assist in identifying, verifying and monitoring users, including their use patterns. The inconsistent rulings issued by lower courts have continued to spur litigation and demand letters from the plaintiffs' bar, most often concerning the use of chatbot technologies and third-party heatmapping software that uses session cookies.[41]

ii State privacy laws and enforcement actions

Passage of several new comprehensive state data privacy laws

There was a surge in state legislative action to enact comprehensive consumer data privacy laws this year, likely fueled at least in part by increasing public awareness about data privacy issues and the failure of Congress to enact a federal privacy law.[42] Following California's lead, several states enacted laws that extend protections similar to those found in the CCPA to residents of their states. As at the date of publication, 12 states have passed comprehensive data privacy legislation,[43] four of which are now in effect (California, Colorado, Connecticut, and Virginia),[44] eight of which have been enacted and will be in effect at a later date (Florida, Iowa, Indiana, Montana, Oregon, Tennessee, Texas, and Utah).[45] Additionally, a comprehensive privacy bill is awaiting gubernatorial action in Delaware.[46] These are in addition to state laws enacted to address consumer health data not protected by HIPAA, which are discussed in a later section.

In addition to new state privacy laws, legislators in Connecticut also passed amendments to that state's data privacy law, just months in advance of that law's effective date. Those amendments include new provisions relating to consumer health data and children's data.[47]

Applicability and scope of laws

Most of the state data privacy laws apply to for-profit entities that process a meaningful amount of personal data or generate a minimum amount of annual revenue, or both; however, there is no one-size-fits-all approach. Several states use a threshold focused on

41 Order Denying Defendant's Motion to Transfer, or Alternatively, Dismiss Plaintiff's First Amended Complaint, *Byars v. Goodyear Tire & Rubber Co*., No. 5:22-cv-01358-SSS-KKx (C.D. Cal. 3 February 2023); Order Granting Defendant's Motion to Dismiss and Vacating the 27 February 2023 Hearing, *Byers v. Hot Topic, Inc. et al.*, No. EDCV 22-1652 JGB (KKx) (C.D. Cal. 14 February 2023).

42 Brenna Goth, The Rise in State Online Consumer Data Privacy Laws: Explained, Bloomberg Law (2 August 2023), https://news.bloomberglaw.com/in-house-counsel/the-rise-in-state-online-consumer-data-privacy-laws-explained.

43 Hunton Andrews Kurth, Delaware Could Become the 13th State to Enact a Comprehensive State Privacy Law, Hunton Andrews Kurth: Privacy & Information Security Law Blog (20 July 2023), https://www.huntonprivacyblog.com/2023/07/20/delaware-could-become-the-13th-state-to-enact-a-comprehensive-state-privacy-law/.

44 *See* Cal. Civ. Code Section 1798.100 et seq.; Colo. Rev. Stat. Sections 6-1-1301 et seq.; Conn. Gen. Stat. Sections 42-515 et seq.; Va. Code Ann. Sections 59.1-575 et seq.

45 *See* Fla. Stat. Sections 501.702 et seq.; Iowa Code Sections 715D.1 et seq.; Ind. Code Sections 24-15-1-1 et seq; Mont. Code Ann. Sections 30-14-1 et seq.; S.B. 619-B, 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Sections 47-18-3201 et seq.; Tex. Bus. & Com. Code Sections 541.001 et seq.; Utah Code Ann. Sections 13-61-101 et seq.

46 *See* Del. Code Ann. tit. 6 Sections 12D-101 et seq.

47 Subst. S.B. 3, Gen. Assemb., Reg. Sess. (Conn. 2023).

the number of state residents whose personal data the entity processes and that number can range from 100,000 for some of the more populated states, to 50,000 in Montana and 35,000 under a privacy bill in Delaware, some of the least populous states in the country.[48] California uses a revenue-based threshold (e.g., entities that generate annual gross revenue in excess of US$25 million),[49] while Tennessee and Utah take a hybrid approach and look to the number of state residents whose personal data is processed and the revenue of the entity.[50] Most provisions in Florida's law appears to be intended to reach only a very small number of companies doing business in its state, as the law applies only to entities that generate in excess of US$1 billion in global gross annual revenue in addition to satisfying other conditions. The Texas law takes a unique approach and generally excludes entities that meet the definition of a 'small business' as defined by the US Small Business Administration, a definition that varies by industry.[51] Several of these laws include an alternative threshold that requires entities to process the personal data of at least 25,000 residents and derive a significant percentage of annual revenue from the 'sale' of personal data (a term that is, however, defined differently under various laws).[52] With the exception of California's CCPA, all of the laws exempt employment and commercial or business-to-business (B2B) data.[53] Further, non-profit organisations are largely exempt from most of these laws[54] except for laws in Colorado, Oregon, and Delaware.[55]

Each of the laws carves out personal data that is already subject to federal privacy laws, including the Gramm-Leach-Bliley Act (GLBA), HIPAA, and their state counterparts

48 These states include Colorado (100,000), Connecticut (100,000), Delaware (35,000), Indiana (100,000), Iowa (100,000), Montana (50,000), Oregon (100,000), and Virginia (100,000). *See* Colo. Rev. Stat. Sections 6-1-1304(1)(b)(I); Conn. Gen. Stat. Sections 42-516; Del. Code Ann. tit. 6 Sections 12D-103(a)(1); Ind. Code Sections 24-15-1-1(a)(1); Iowa Code Sections 715D.2(1)(a); Mont. Code Ann. Sections 30-14-3(1); S.B. 619-B(2)(1)(a), 82nd Leg. Assemb., Reg. Sess. (Or. 2023) Va. Code. Ann. Sections 59.1-576(A).

49 Cal. Civ. Code. Sections 1798.140(d)(1)(A).

50 *See* Tenn. Code Ann. Sections 47-18-3202; Utah Code Ann. Sections 13-61-102.

51 *See* Fla. Stat. Sections 501.702(9); Tex. Bus. & Com. Code Sections 541.002.

52 Texas and Florida are not included in this list. *See* Cal Civ. Code. Sections 1798.140(d)(1)(B)-(C); Colo. Rev. Stat. Sections 6-1-1304(1)(b)(I)-(II); Conn. Gen. Stat. Section 42-516; Del. Code Ann. tit. 6 Section 12D-103(a)(2); Ind. Code Section 24-15-1-1(a)(2); Iowa Code Section 715D.2(1)(b); Mont. Code Ann. Section 30-14-3(2); S.B. 619-B(2)(1)(b), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3202(2)(A); Utah Code Ann. Section 13-61-102(1)(c); Va. Code Ann. Section 59.1-576(a).

53 Colo. Rev. Stat. Section 6-1-1303(6)(b); Conn. Gen. Stat. Section 42-515(7); Del. Code Ann. tit. 6 Section 12D-102(8); Fla. Stat. Section 501.702(8); Ind. Code Section 24-15-2-8(b); Iowa Code Section 715D.1(7); Mont. Code Ann. Section 30-14-1(6)(b); S.B. 619-B(1)(7), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3201(7)(B); Tex. Bus. & Com. Code Section 541.001(7); Utah Code Ann. Section 13-61-101(10)(b); Va. Code Ann. Section 59.1-575.

54 Cal. Civ. Code. Section 1798.145 Conn. Gen. Stat. Section 42-517(a)(2); Fla. Stat. Section 501.703(2)(d); Ind. Code Section 24-15-1-1(b)(4); Iowa Code Section 715D.2(2); Mont. Code Ann. Section 30-14-4(1)(b); Tenn. Code Ann. Section 47-18-3210(5); Tex. Bus. & Com. Code Section 541.002(4); Utah Code Ann. Section 13-61-102(2)(d); Va. Code Ann. Section 59.1-576(B).

55 *See generally* Colo. Rev. Stat. Section 6-1-1304(2); *see also* Del. Code Ann. tit. 6 Section 12D-103(b)(3) (exempting only nonprofit organizations dedicated exclusively to preventing and addressing insurance crime); S.B. 619-B(2)(r), 82nd Leg. Assemb., Reg. Sess. (Or. 2023) (same).

(e.g., California Confidentiality of Medical Information Act)[56] Several states take this a step further, and include entity-based exemptions for entities that are subject to the GLBA and/or that function as covered entities or business associates under HIPAA.[57]

Data subject rights

All of the state data privacy laws provide residents of their states with familiar data privacy rights: the rights to know, access, correct, and delete personal information.[58] Each state law also provides consumers with the right to opt-out of the sale of their personal information, the use or sharing of their personal information for targeted or cross-context behavioural advertising, and profiling for certain purposes.[59] What constitutes a 'sale' under these laws varies: some states define 'sale' narrowly to refer only to personal data disclosed in exchange for monetary compensation),[60] while others define it broadly to refer to personal data disclosed in exchange for valuable consideration, including non-monetary consideration.[61]

56 Cal. Civ. Code Section 1798.145(c)(1)(A), (e); Conn. Gen. Stat. Sections 42-517(a)(5), (b)(1); Colo. Rev. Stat. Sections 6-1-1304(2)(a), (j)(II); Del. Code Ann. tit. 6 Sections 12D-103(b)(2), (14); Fla. Stat. Sections 501.703(2)(b), 501.704(1); Ind. Code Sections 24-15-1-1(b)(1)(2), 24-15-1-2(1); Iowa Code Section 715D.2(2)-(3); Mont. Code Ann. Sections 30-14-4(1)(e), (2)(a); S.B. 619-B(2)(2)(b), (k)(A), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Sections 47-18-3210(a)(2), (7); Tex. Bus. & Com. Code Section 541.002(b)(2); Utah Code Ann. Sections 13-61-102(2)(g)(i), (k); Va. Code Ann. Section 59.1-576(B)-(C).

57 Only 10 states have entity-level exemptions for entities subject to GLBA and HIPAA. *See* Colo. Rev. Stat. Sections 6-1-1304(2)(e), (q); Conn. Gen. Stat. Section 42-517(a)(5)-(6); Fla. Stat. Section 501.703(2)(b)-(c); Iowa Code Section 715D.2(2); Ind. Code Section 24-15-1-1(b)(1)(2)-(3); Mont. Code Ann. Section 30-14-4(1)(e)-(f); Tenn. Code Ann. Sections 47-18-3210(a)(2), (4); Tex. Bus. & Com. Code Section 541.002(b)(2)-(3); Utah Code Ann. Sections 13-61-102(2)(e)-(f), (k); Va. Code Ann. Section 59.1-576(B). Delaware only has an entity-level exemption for GLBA, not HIPAA. *See* Del. Code Ann. tit. 6 Section 12D-103(b)(2).

58 *See* Cal. Civ. Code Sections 1798.105-06, 110, 115, 120-21, 125; Colo. Rev. Stat. Section 6-1-1306(1); Conn. Gen. Stat. Section 42-518(a); Del. Code. Ann. Section 12D-104(a); Fla. Stat. Section 501.705; Iowa Code Section 715D.3; Ind. Code Section 24-15-3-1(b); Mont. Code Ann. Section 30-40-5(1); S.B. 619-B(3)(1)-(2), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3203; Tex. Bus. & Com. Code Section 541.051(b); Utah Code Ann. Section 13-61-201; Va. Code Ann. Section 59.1-577.

59 *See* Cal. Civ. Code Section 1798.120; Colo. Rev. Stat. Section 6-1-1306(1)(a); Conn. Gen. Stat. Section 42-518(a); Del. Code. Ann. Section 12D-104(a)(6); Fla. Stat. Section 501.705(e)-(g); Iowa Code Section 715D.3(d) (opt-out rights for sale of personal data only); Ind. Code Section 24-15-3-1(b)(5); Mont. Code Ann. Section 30-40-5(1)(e); S.B. 619-B(3)(1)(d)(A)-(C), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3203(E); Tex. Bus. & Com. Code Section 541.051(b)(5); Utah Code Ann. Section 13-61-201(4) (opt-out rights limited to targeted advertising and/or sale of personal data); Va. Code Ann. Section 59.1-577(5).

60 These states include Indiana, Iowa, Utah, and Virginia. *See* Ind. Code Section 24-15-2-27; Iowa Code Section 715D.1(25); Utah Code Ann. Section 13-61-101(31)(a); Va. Code Ann. Section 59.1-575.

61 These states include California, Colorado, Connecticut, Delaware, Florida, Montana, Oregon, Tennessee, and Texas. *See* Cal. Civ. Code Section 1798.140(ad)(1); Colo. Rev. Stat. Section 6-1-1303(23)(a); Conn. Gen. Stat. Section 42-515(26); Del. Code Ann. tit. 6 Section 12D-102(29); Fla. Stat. Section 501.702(29); Mont. Code Ann. Section 30-14-2(23); S.B. 619-B(1)(17), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3201(25); Tex. Bus. & Com. Code Section 541.001(28).

Several states also require, entities to recognise universal opt-out signals, such as the Global Privacy Control, that will allow consumers to set their opt-out preferences on a browser and have those preferences applied across websites they visit.[62]

Enforcement mechanisms

None of these state privacy laws can be enforced through a private right of action.[63] Rather, they each grant exclusive enforcement authority to state attorney generals and, in Colorado, to district attorneys.[64] California is the only state with a dedicated privacy agency, the California Privacy Protection Agency (CPPA). The CPPA has concurrent CCPA enforcement authority with the California Office of Attorney General[65] All of these laws provide for a initial mandatory cure period, although several phase it out within one or two years after the law's effective date.[66] Indeed, the CCPA's initial mandatory cure period requirement has already expired.

Some states treat a violation of their data privacy laws as an unlawful or deceptive practice, or both, under state unfair and deceptive acts and practices (UDAP)laws.[67] Statutory damages are available under each law, either directly or indirectly if the law is enforced through state UDAP laws.[68] This means when prosecuting alleged violations of these laws, regulators who seek statutory damages may in some cases need not prove consumer harm or quantify damages.

62 *See* Cal. Code Regs. tit. 11, Section 7025; Colo. Rev. Stat. Section 6-1-1306(1)(a)(II), (IV)(A)-(B); Conn. Gen. Stat. Section 42-520(e)(1)(A)(ii); Del. Code Ann. Section 12D-105(a); Mont. Code Ann. Section 30-40-6(1); S.B. 619-B(4)(4), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tex. Bus. & Com. Code Section 541.055(e).

63 The California Consumer Privacy Act ('CCPA') includes a private right of action for negligent data breaches involving certain categories of personal information, but this does not relate to enforcement of the CCPA. *See* Cal. Civ. Code Section 1798.150. See also Colo. Rev. Stat. Sections 6-1-1310(1)-11(1)(b); Conn. Gen. Stat. Section 42-525(d); Del. Code Ann. Section 12D-111(d); Fla. Stat. Section 501.72(1); Iowa Code Section 715D.8(4); Ind. Code Section 24-15-10-4; Mont. Code Ann. Section 30-40-12(3); S.B. 619-B(9)(8), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3212(e); Tex. Bus. & Com. Code Section 541.156; Utah Code Ann. Section 13-61-305; Va. Code Ann. Section 59.1-584(E).

64 Colo. Rev. Stat. Section 6-1-1311(1)(a); Conn. Gen. Stat. Section 42-525(a); Del. Code Ann. Section 12D-111(a); Fla. Stat. Section 501.72(1); Iowa Code Section 715D.8(1); Ind. Code Section 24-15-10-1; Mont. Code Ann. Section 30-40-12(1); S.B. 619-B(9)(8), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3212(a); Tex. Bus. & Com. Code Section 541.151; Utah Code Ann. Section 13-61-402(1); Va. Code Ann. Section 59.1-584(A).

65 Cal. Civ. Code Sections 1798.155, 1798.199.10.

66 Colo. Rev. Stat. Section 6-1-1311(1)(d); Conn. Gen. Stat. Section 42-525(b); Del. Code Ann. Section 12D-111(b); Fla. Stat. Section 501.72(2); Iowa Code Section 715D.8(2); Ind. Code Section 24-15-10-3; Mont. Code Ann. Section 30-40-12(2); S.B. 619-B(9)(5), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3212(a); Tex. Bus. & Com. Code Section 541.154; Utah Code Ann. Section 13-61-402(3)(a); Va. Code Ann. Section 59.1-584(B).

67 Colo. Rev. Stat. Section 6-1-1311(1)(c); Conn. Gen. Stat. Section 42-525(e); Del. Code Ann. Section 12D-111(e); Fla. Stat. Section 501.72(1).

68 Cal. Civ. Code Sections 1798.155, 1798.199.90; Colo. Rev. Stat. Section 6-1-1311(1)(c); Conn. Gen. Stat. Section 42-525; Fla. Stat. Section 501.72(1); Iowa Code Section 715D.8(3); Ind. Code

Rule-making activities

State privacy laws in California and Colorado are the only ones that authorise or contemplate that regulations will be drafted to implement the law. This year saw regulations promulgated under both laws.

California regulations

In March 2023, California regulators finalised the first tranche of regulations under amendments to the CCPA enacted through the California Privacy Rights Act (CPRA), after several months of deliberation and public comment. There are more regulations to come, either in 2023 or soon thereafter. In 2022, the California Privacy Protection Agency (CPPA), the body charged with rule-making under CPRA amendments, decided to take a staged approach to drafting required regulations due to staffing and timing limitations.

In late August 2023, the agency released a proposed draft of a second tranche of CCPA regulations. These focused on areas of risk assessments and cybersecurity audits. It is unlikely this second tranche of regulations will be finalised before the end of 2023.

Enforcement of the first tranche of CPRA regulations has, been delayed until March 2024. Soon after these regulations were issued, the California Chamber of Commerce filed suit to stop their enforcement, alleging the CCPA gives businesses one year to comply with regulations once they have been finalised.[69] In July 2023, a state court largely agreed with the Chamber, ruling that regulations issued in March 2023 could not be enforced until March 2024 and imposing a one-year enforcement pause for all CCPA regulations enacted in the future.[70] The court's order does not apply to enforcement of the CCPA generally, nor does it apply to regulations that were implemented pursuant to the CCPA before the 1 January 2023 effective date of CPRA amendments to the CCPA. In August 2023, the CPPA appealed the court's decision; the appeal is pending.

Colorado regulations

In March 2023, Colorado regulators finalised regulations to implement the Colorado Privacy Act in advance of the statute's 1 July 2023 effective date.[71] These regulations covered implementation of the Colorado Privacy Act writ large, unlike California's phased approach to issuing regulations.

Enforcement and investigations

California

Under the CCPA, the California Privacy Protection Agency (CPPA) has concurrent enforcement power with the California Office of the Attorney General. This year saw the increased development of the agency, as it hired several key senior positions, including a

Section 24-15-10-2; S.B. 619-B(9)(4)(a), 82nd Leg. Assemb., Reg. Sess. (Or. 2023); Tenn. Code Ann. Section 47-18-3212(d)(1); Tex. Bus. & Com. Code Section 541.155; Utah Code Ann. Section 13-61-402(3)(d); Va. Code Ann. Section 59.1-584(C).

69 Complaint, *California Chamber of Commerce vs. California Privacy Protection Agency, et al.*, No. 34-2023-80004106-CU-WM-GDS (Sup. Court of Sacramento 30 March 2023).

70 Order and Judgment, *California Chamber of Commerce vs. California Privacy Protection Agency, et al.*, No. 34-2023-80004106-CU-WM-GDS (Sup. Court of Sacramento 20 July 2023).

71 Attorney General's Office files finalised Colorado Privacy Act rules (13 March 2023) at https://coag.gov/press-releases/3-15-23/.

new Deputy Director of Enforcement, Senior Privacy Counsel, Chief Information Officer, Chief Administrative Officer, and Deputy Director of Public and External Affairs, in addition to building out staff to support each of these roles. The staff notably includes several 'technologists' who play an integral role in helping the agency understand and navigate the technically complex business models they are charged with regulating.

The agency's authority to commence enforcement of the CCPA began on 1 July 2023 and the agency has started enforcement activity, despite the limitations imposed by the California state court's order regarding the March 2023 regulations. In August 2023, the agency announced it was investigating the privacy practices of connected vehicles and related technologies, noting that the data collected could potentially be subject to CCPA rights to know, delete, and stop the sale or sharing (for advertising purposes) of such information. The agency also has undertaken investigations relating to the enforcement of provisions of the CCPA that are not encompassed by the state court order.

The Office of the California Attorney General (OAG), which has concurrent CCPA enforcement authority (and is similarly subject to the court order delaying enforcement of regulations), has also continued its enforcement activities. To date, the enforcement activity has mostly consisted of investigative inquires that have been resolved informally. The California Attorney General's 2022 action against Sephora is the only CCPA enforcement action to date in which a complaint was filed (and, even in that case, the parties concurrently filed a proposed settlement, which the court later ratified).[72] In July 2023, the OAG announced it was focusing on employee privacy and sent letters to large employers in California inquiring about their compliance with CCPA with respect to employees and job applicants.[73]

Colorado

The Colorado Attorney General began enforcement of the Colorado Privacy Act in July 2023, initially by sending letters to businesses subject to the Colorado law informing them of their obligations under the law. The letters highlighted new legal obligations under the law and some focused more specifically on the obligation to obtain consent prior to the collection of sensitive data, and the obligation to provide a means to allow consumers to opt out of targeted advertising and certain types of profiling.[74]

iii State sectoral privacy laws and enforcement

State consumer health data laws

This year saw the passage of several state laws focused on the protection of 'consumer health data' outside the scope of HIPAA. These laws reflect concerns about the use of such data in now that several states have limited rights relating to gender-affirming care and criminalised abortion following the US Supreme Court's 2022 decision eliminating federal Constitutional protections for abortion rights.

72 Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (24 August 2022) at https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

73 Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act (14 July 2023) at https://oag.ca.gov/news/press-releases/attorney-general-bonta-seeks-information-california-employers-compliance.

74 Attorney General Phil Weiser launches enforcement of Colorado Privacy Act (12 July 2023) at https://coag.gov/press-releases/attorney-general-phil-weiser-launches-enforcement-of-colorado-privacy-act/.

The Washington state 'My Health My Data' law was the first such law to pass this year and has the potential to become a particularly significant US state privacy law both because of its breadth and the detailed and specific disclosures it requires, and because it includes a private right of action. The law applies to all entities doing business in Washington state applies broadly to 'consumer health data' of Washington residents and residents whose data is processed in the state of Washington.[75] 'Consumer health data' is defined as personal information that identifies a consumer's 'past, present, or future physical or mental health status', which, in turn, is defined as including 'social, psychological, [and] behavioral interventions', 'health-related procedures', 'reproductive or sexual health information', 'gender-affirming care', and 'biometric data' which may include keystroke patterns that identify a consumer. In addition to providing familiar data privacy rights (e.g., transparency, access, correction, deletion), the law prohibits the collection and sharing of consumer health data for purposes other than delivering the good or service a consumer has requested without consumers' 'affirmative' consent. Opt-in consent is also required to sell consumer health information (which potentially could be interpreted to include providing information for digital advertising purposes), and other provisions require the disclosure of the names and contact information of all entities that purchase consumer health data. The law will be enforced by the Washington Attorney General under that state's Consumer Protection Act as well as through private right of action.

In June 2023, Connecticut and Nevada passed similar laws, albeit somewhat more narrow. The Connecticut law amended the state's comprehensive data privacy law that went into effect on 1 July 2023 by defining 'consumer health data' as sensitive data for which consent is required prior to processing such data, with an exception for providing products or services 'specifically requested' by a consumer or performing a contract to which the consumer is a party.[76] The definition of consumer health data is more narrow under the Connecticut law than the Washington law, as it is defined to mean only such data that a regulated entity uses to identify a consumer's 'physical or mental health condition or diagnosis'. The Connecticut law does not include a private right of action and is enforceable by that state's Attorney General. It applies only to for-profit entities of a certain size or who meet sales-related thresholds.

The Nevada Consumer Health Privacy Law was also enacted in June 2023, but does not go into effect until March 2024. It defines 'consumer health data' as data that is used by a 'regulated entity' to identify an individual's physical or mental health status (past, present, or future), and applies to entities of all sizes, including non-profits. The law requires opt-in consent to collect, disclose, or sell consumer health data, unless to provide a requested good or service, much like the other laws. The law does not include a private right of action and is enforceable by the Nevada Attorney General as an unfair trade practice under the Nevada Consumer Protection Act.

State laws regulating minors' personal data

Laws focused on the personal data of minors have also passed at the state level, following last year's passage of the California Age Appropriate Design Code Act (AADCA).[77] The AADCA, which comes into effect on 1 July 2024, would impose a variety of obligations and restrictions on businesses that develop and provide online services, products or features that minors under

75 Subst. H.B. 1155, 68th Leg., 2023 Sess. (Wash. 2023).

76 Subst. S.B. 3, Gen. Assemb., Reg. Sess. (Conn. 2023).

77 Cal. Civ. Code Sections 1798.99.28 et seq. (Cal. 2022).

17 are 'likely to access'. It would require businesses to configure privacy settings to high levels of privacy and restrict their ability to profile minors and collect geolocation information for certain age groups. The law gives the California Attorney General sole enforcement powers (e.g., no private right of action) and statutory penalties are authorised (up to US$7,500 per 'affected child').

Trade groups have mounted a legal challenge to the AADCA and on 14 December 2022, the trade group NetChoice filed suit alleging the law violates the First Amendment, the 'dormant' Commerce Clause (which limits undue burdens imposed by states on interstate commerce) and is preempted by federal laws governing children's data and online speech.[78]

The challenge to the California law did not deter other states from seeking to regulate the collection and use of personal data from minors under 18, including through restrictions on the use of social media without parental consent, requirements that social media platforms take down content posted in response to a request from a minor or parent of a minor, and age verification requirements for the distribution of 'material harmful to minors' (e.g., pornographic content). Such laws were passed this year in several states, including in Arkansas, Connecticut, Florida, Louisiana, Mississippi, Montana, Texas, Utah and Virginia.[79] Several age-verification laws are the subject of challenges brought by industry groups.[80]

Social media laws

While many of the children's laws mentioned above are focused on regulating children's online presence and data collection, including on social media platforms, there are new laws that were passed that focus on social media practices generally. For example, Montana recently passed Senate Bill 419, which bans public access to TikTok in the state of Montana starting on 1 January 2024[81] and the Florida Digital Rights Law passed this year prohibits governmental entities from moderating content on social media networks.[82]

Emerging technologies/artificial intelligence

States also are continuing to regulate emerging technologies. Increased attention on the use of monitoring technologies and algorithms in the employment context prompted New York City to pass Local Law 144 requiring businesses using such technologies to certify they have conducted bias audits, disclose the use of these technologies and offer reasonable accommodations for employees and job applicants whose disabilities present difficulties when interacting with these technologies.[83] Enforcement of Local Law 144 began on 5 July 2023, after several delays while regulators finalised implementing regulations and related guidance.[84]

78 NetChoice Sues California to Protect Families & Free Speech Online (14 December 2022) at https://netchoice.org/netchoice-sues-california-to-protect-families-free-speech-online/.

79 S.B. 66, 2023 Reg. Session (Ark. 2023); Subst. S.B. 3, Gen. Assemb., Reg. Sess. (Conn. 2023); S.B. 262, 2023 Reg. Session (Fla, 2023); H.B. 61, 2023 Reg. Session (La., 2023; S.B 384, 2023 Reg. Session (Mont. 2023); H.B. 18, 2023 Reg. Session (Tex., 2023)H.B. 311, 2023 Reg. Session (Utah, 2023); .

80 Porn industry group sues over Utah age verification law (4 May 2023) at https://www.wric.com/news/u-s-world/porn-industry-group-sues-over-utah-age-verificaiton-law/?ipid=promo-link-block1.

81 S.B. 0419, 68th Leg., 2023 Session (Mont. 2023).

82 S.B. 262, 2023 Reg. Session (Fla, 2023).

83 N.Y. City Local Law 144 (2021).

84 New York City Consumer and Worker Protection, Automated Decision Tools: Frequently Asked Questions (2023) at https://www.nyc.gov/assets/dca/downloads/pdf/about/DCWP-AEDT-FAQ.pdf.

On 26 May 2023, the Colorado Division of Insurance (CDOI) issued a revised draft of its Algorithm and Predictive Model Governance Regulation. The draft regulation aims to ensure that the use of external consumer data and information sources (ECDIS), algorithms, and predictive models by Colorado-licensed life insurance companies do not result in unfairly discriminatory insurance practices with respect to race. It would require life insurers that use ECDIS in insurance practices to establish a governance and risk management framework to determine whether their use of ECDIS results in unfair discrimination with respect to race. Reflecting broader trends, the draft regulation would require corporate boards to oversee the governance and risk management framework and senior management would be held accountable for compliance. The draft regulations require frameworks to include written policies, processes for consumer complaints and inquiries, and mechanisms to oversee vendor compliance.

On 7 June 2023, Connecticut enacted a new law concerning AI and automated decision-making.[85] The law establishes an Office of Artificial Intelligence as well as a task force to study AI and develop an AI bill of rights. It also requires the Department of Administrative Services to inventory AI systems in use by any state agency by 31 December 2023.

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 and 'consumer health data'. These laws 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 use of industry standards of care to protect the data.

iv State data protection laws and enforcement activities

Several states have also passed laws adopting prescriptive data security and reporting requirements for insurers that generally track the Insurance Data Security Model Law adopted by the National Association of Insurance Commissioners (NAIC). This year Illinois and Pennsylvania joined 22 other states in the past year (bringing the total to 24 states).

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.

State insurance regulations

States continue to pass 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). This year Illinois and Pennsylvania passed such laws, joining 22 other states who have adopted some version of the NAIC's model law.

85 An Act Concerning Artificial Intelligence, Automated Decision-Making and Personal Data Privacy, Senate Bill No. 1103 at https://www.cga.ct.gov/asp/CGABillStatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB1103.

NYDFS – proposed amendments and enforcement actions

The New York Department of Financial Services (DFS) continues to be an active regulator in the state cybersecurity space. DFS is responsible for the supervision of financial services companies operating in New York, including, but not limited to, New York state chartered banks, insurance companies, virtual currency companies, money services business, mortgage lenders and servicers, other non-depository lenders and credit reporting agencies.

In July 2022, DFS introduced proposed amendments to the Cybersecurity Regulation and has since released two additional iterations of such amendments, on 9 November 2022 and 28 June 2023, respectively. The latest version of the proposed amendments, which was released on 28 June 2023, retains many of the obligations initially proposed in July 2022, including mandatory annual penetration tests, multi-factor authentication (MFA) and considerable involvement by senior officers and board members.[86] However, the most recent amendments go further, requiring annual approval of cybersecurity policies by the covered entity's board; CISO reports of material cybersecurity issues; annual review of access privileges; annual risk assessments (or whenever there has been a material change); asset inventory documentation; and a written business continuity and disaster recovery plan.[87] The June 2023 amendments also add another tight notification timeline, requiring entities to notify DFS within 24 hours of making an extortion payment.[88] The public comment period for the proposed regulations recently closed on 14 August 2023.

DFS has also continued to vigorously enforce the Cybersecurity Regulation. Several of its enforcement actions this year have focused on mortgage companies and entities operating in the virtual currency space.[89]

State courts

While a complete canvas of all state court decisions impacting privacy and cybersecurity is beyond the scope of this chapter, highlighting a couple of examples serves to demonstrate the general point.

State courts, particularly those in California, saw dozens of claims brought under state wiretap laws, as did federal courts, as discussed above.

In Illinois, the state's Supreme Court handed down two significant rulings under the Illinois Biometric Information Privacy Act (BIPA), which includes a private right of action and has been the source of waves of biometric privacy litigation, buttressed by rulings of the Illinois Supreme Court, including its 2019 ruling that bare procedural violations of the statute are sufficient to establish legal standing.[90] A wide range of technology companies, including Facebook, Shutterfly, Snapchat and Google, are finding themselves defending their implementation of facial and voice recognition technology against BIPA claims in Illinois courts.

This year, the Illinois Supreme Court issued a significant ruling in *Cothron v. White Castle Systems*. The Court found that a separate claim accrues under BIPA each time that entity scans or transmits an individual's biometric identifier or information in violation of

86 23 NYCRR Part 500.

87 23 NYCRR Sections 500.3, 500.4, 500.7, 500.9, 500.16.

88 23 NYCRR Section 500.17(c).

89 NY Dept. of Financial Services, Enforcement and Discipline: Banking, Licensed Financial, and Other Products and Services, at https://www.dfs.ny.gov/industry_guidance/enforcement_actions_lfs.

90 *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (2019).

the statute. This has the potential to significantly inflate damage awards because the statute provides for statutory damages of US$1,000 or US$5,000 per violation.[91] In another impactful ruling, the Illinois Supreme Court held that the statute of limitations under BIPA is five years, not the one-year limitations period under Illinois law that applies generally to the ' "publication" of matters that violate the right of privacy'.[92]

III REGULATORY FRAMEWORK

As noted in the detailed discussion of recent, significant developments 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 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 business acts or trade 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 not 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 United States that 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 United States.[93] 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.[94] 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

91 *Cothron v. White Castle System, Inc.* 2023 IL 128004 (2023).

92 *Tims v. Black Horse Carriers*, 2023 IL 127801 (2023).

93 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. Section 45(a)(4) (1914).

94 *id*. at Section 5.

practices in or affecting commerce'.[95] 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 (i.e., 'unfairness' is subject to a statutory cost-benefit test). The FTC has significantly expanded its understanding of unfairness this year, as described above with reference to enforcement actions in the health privacy area.

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.[96] (Note, however, that unless the FTC's position is embodied in a final regulation, or adopted following adjudication in court, the FTC's views do not have the force of law. In other words, settlements, consent decrees, commissioner statements, staff reports, etc., are not generally legally binding – other than on the individual parties to a specific settlement or consent decree of course.)

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 express or implied consent.[97]

In terms of enforcement, the FTC has frequently brought 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. This year, the agency included uses of digital advertising technologies with health data and the failure to have certain policies and procedures in place with respect to such technologies. 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 obtaining consent decrees. Such decrees generally provide for ongoing monitoring by the FTC for 20 years, prohibit further

95 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. 9 September 2009).

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

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

violations of the law and subject businesses to substantial financial penalties for subsequent violations of the consent decrees. These enforcement actions have been loosely characterised as shaping a common law of privacy that could help guide companies' privacy practices.[98]

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 for the protection of personal data.

That said, recent years have brought a flurry of federal action related to cybersecurity. In 2015, Congress enacted the Cybersecurity Information Sharing Act,[99] 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. The law also authorises network monitoring and certain other defensive measures, notwithstanding any other provision of law. In addition, 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.[100] 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. On 8 August 2023, NIST released a draft of a significant update to the NIST Cybersecurity Framework (CSF) 2.0 that reflects changes in the cybersecurity landscape since the first Framework was released in 2014.[101]

In March 2022, President Biden also signed into law the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which requires all critical infrastructure entities to report any cybersecurity incidents or ransomware attacks to the Cybersecurity and Infrastructure Security Agency (CISA) within a specified time frame. Covered entities that experience a covered cyber incident must report the incident to CISA within 72 hours once the entity has reasonable belief that an incident has occurred. If the covered cyber incident also qualifies as a ransomware attack, the covered entity must report the incident to CISA within 24 hours if a ransomware payment has been made. CIRCIA aims to give CISA enough time to help and resource the impacted entities and victims, while using the reports to examine

98 See, for example, Solove and Hartzog, *The FTC and the New Common Law of Privacy*, 114 *Columbia Law Review* 583 (2014).

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

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

101 NIST Releases Cybersecurity Framework 2.0 Draft & Implementation Examples (8 August 2023) at https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft.

prospective attack trends across industries and share that knowledge with potential targets in the critical infrastructure sector. CISA is in the process of rule-making efforts that are required to implement portions of this law.

Specific regulatory areas – federal law

In addition to the foregoing, 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;
c information about children and students;
d telephone, internet and other electronic communications and records;
e credit and consumer reports; and
f miscellaneous consumer privacy statutes such as VPPA and DPPA.

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

Financial information

The GLBA[102] addresses financial data privacy and security by establishing standards, known as the privacy and safeguard rules, pursuant to which financial institutions must provide transparency about and safeguard their customers' 'non-public personal information' (or 'personally identifiable financial information'), to the extent such information is to be used primarily for personal, family, or household purposes. 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 regulators have the authority to promulgate rules to implement the GLBA and to enforce the statute, including federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency), the SEC, the FTC (for certain non-bank financial institutions), and the Consumer Financial Protection Bureau (CFPB) (for certain banks and non-bank financial institutions). The FTC and the SEC also have authority to enforce consumer privacy and data protection under the GLBA. Insurance is regulated at the state level, so GLBA financial privacy in that sector is administered by state insurance commissions.

102 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)).

In 2022, the FTC updated and substantially strengthened provisions of its safeguards rule to address increasing cybersecurity threats by, among other things, requiring regulated entities to assess security risks, implement access-controls, assess security practices of services providers, and implement multi-factor authentication for anyone accessing customer information.[103] In 2023, the SEC proposed amendments to its privacy and safeguards rules as applied to broker-dealers and investment advisers that would strengthen cybersecurity requirements and the 'disposal rule', which requires proper disposal of consumer report information by SEC-registered transfer agents.[104]

The SEC has authority beyond the GLBA to regulate cybersecurity matters. In July 2023, the agency finalised its rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies that applies to all public companies subject to the reporting requirements of the Securities Exchange Act of 1934.[105] This rule requires disclosure of material cybersecurity incidents on Form 8-K and Form 20-F and periodic disclosure of cybersecurity risk management, strategy, and governance in annual reports on Form 10-K and Form 20-F.

Federal banking regulators also regulate cybersecurity notification obligations of banking organisations through the Computer-Security Incident notification Requirements for Banking Organizations and Their Bank Service Providers, first issued in 2021.[106] This rule, jointly promulgated by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve, and the Federal Deposit Insurance Corporation, requires covered banking organisations to notify their federal regulator of any 'computer-security incident' that meets the criteria of a 'notification incident', and to do so within 36 hours of the banking organisation determining that a notification incident has occurred. It also includes customer notification obligations if the incident has caused, or is reasonably likely to cause, a material service disruption or degradation of service for four or more hours. The computer-security incidents covered by this rule are not limited to incidents that involve unauthorised access to personal data; rather, the rule encompasses occurrences that harm information systems generally and the information (both personal data and non-personal data) that such systems process, store, or transmit.

Healthcare information

HIPAA, the Health Insurance Portability and Accountability Act of 1996, including as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), regulates entities engaged in providing healthcare services and includes

103 Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 16 C.F.R. Section 314.1 *et seq*.

104 Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, 88 FR 20212 (5 April 2023) at https://www.federalregister.gov/documents/2023/04/05/2023-05767/cybersecurity-risk-management-rule-for-broker-dealers-clearing-agencies-major-security-based-swap.

105 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure – Final Rule, 88 Fed. Reg. 51896 (4 August 2023) at https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure.

106 Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed.Reg. 66424 (23 November 2021).

standards to protect the privacy and security of electronic protected health information (PHI), known as the 'Privacy Rule' and the 'Security Rule'.[107] The Office for Civil Rights within the Department of Health and Human Services enforces these rules and has the authority to issue civil penalties and enter into corrective action plans or other agreements with covered entities or business associates.[108] 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 require covered entities obtain patient authorisation before using or disclosing PHI for marketing purposes, selling PHI or disclosing PHI to other organisations for purposes other than providing healthcare services.[109]

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'.[110] 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.[111] Notably, HIPAA does not apply to 'de-identified' data, provided the de-identification is conducted in accordance with specifications set forth in HIPAA regulations.[112]

HIPAA places obligations on 'covered entities', which include health plans, healthcare clearing houses and healthcare providers that engage in electronic transactions. Under the Privacy and Security Rules require covered entities to provide transparency about their data collection practices through privacy notices; offer rights to access and amend PHI they collect; conduct regular risk assessments; ensure the confidentiality, integrity, and availability of PHI; implement administrative, physical, and technical safeguards to protect PHI from unauthorized access; and document privacy and security protocols in written policies and procedures, among other requirements.[113]

The Privacy and Security Rules also apply to business associates, entities that create, receive, maintain, or transmit PHI on behalf of covered entities – essentially, service providers to covered entities.[114] Business associates are required to enter into agreements with covered entities they service, and such agreements must include provisions limiting the business

107 HIPAA Administrative Simplification Regulations, 45 C.F.R. Parts 160, 162, and 164.

108 45 C.F.R. Section 160.312; How OCR Enforces the HIPAA Privacy and Security Rules at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html.

109 45 C.F.R. Section 164.508(a).

110 45 C.F.R. Section 160.103.

111 45 C.F.R. Section 160.103.

112 45 C.F.R. Section 164.145(b) and (c).

113 45 C.F.R. Sections 164.303 *et seq*. and 164.500 *et seq*.

114 45 C.F.R. Section 160.103.

associate's use and disclosure of PHI only as permitted or required by the agreement or as required by law and to directing the business associate to use appropriate safeguards to prevent the unauthorized use or disclosure of PHI.[115]

The HIPAA Breach Notification Rule applies to covered entities and business associates and imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI they maintain.[116]

The FTC is focused on enforcement efforts with respect to health data that is not within HIPAA's purview, including through the Health Breach Notification Rule and enforcement actions brought under the FTC Act.[117]

Information about children

The Children's Online Privacy Protection Act (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 and obtain verifiable parental consent before collecting personal information from children and other actions.[118]

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records and applies to all educational institutions that receive federal funds, including colleges and universities.[119] FERPA gives parents or eligible students certain rights with respect to their education records, including the rights to inspect, review, and amend student records. Parents or eligible students can also prohibit schools from disclosing a student's records without consent.

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;[120]

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

115 45 C.F.R. Section 164.504(e) and HHS Sample Business Associate Agreement Provisions at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

116 45 C.F.R. Section 164.400 *et seq*.

117 For example, Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief, *United States of America v. GoodRx Holdings, Inc.*, Case No. 3:23-cv-460 (N.D. Cal. 1 February 2023).

118 Children's Online Privacy Protection Act of 1998, 15 U.S.C. Sections 6501–6505.

119 Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232g; 34 CFR Part 99.

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

invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks;[121]

c various sections of the Communications Act protect telecommunications information, including what is known as customer proprietary network information, or CPNI;[122]

d the Telephone Consumer Protection Act (TCPA) governs robocalls and texts;[123] and

e the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act governs commercial email messages, generally permitting companies to send commercial emails to anyone provided that the recipient has not opted out of receiving such emails from the company, the email identifies the sender and the sender's contact information, and the email has instructions on how to easily and at no cost opt-out of future commercial emails from the company.[124]

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),[125] as amended by the Fair and Accurate Credit Transactions Act of 2003,[126] 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 and the Office of the Comptroller of the Currency) share authority for enforcing the 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.[127]

121 Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 (1984).

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

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

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

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

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

127 Fair Credit Reporting Act, 15 U.S.C. Section 621.

Miscellaneous statutes – VPPA and DPPA

The Video Privacy Protection Act of 1988 (VPPA) was passed by Congress in 1988 after the video rental history of US Supreme Court nominee Robert Bork was leaked to the press by a store clerk.[128] The VPPA applies to 'video tape service providers' that are engaged in the business of 'rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials' The law prohibits such entities from disclosing, without consent, personally identifiable information, which includes information that identifies a person as having requested or obtained video materials or services from such video tape service providers. The consent that must be obtained is required to be distinct and separate from other legal documentation (e.g., privacy policies) and must be provided either at the time of disclosure or no more than two years prior to the time of disclosure. The law includes several exemptions, including for disclosures that are 'incident to the ordinary course of business' of the video tape service provider. The VPPA provides for statutory damages and attorneys' fees and, as such, has been the subject of numerous class action claims since its passage. The newest wave of VPPA lawsuits has focused on claims alleging VPPA violations through the use of online tracking technologies on websites that embed videos (e.g., to advertise a product) and then, through the use of the tracking technologies, relay information about which videos a website visitor has watched to a third party.[129]

The Drivers Privacy Protection Act (DPPA) was enacted in 1994 to protect the privacy of personal information collected by state motor vehicle departments (DMVs).[130] It prohibits state DMVs from selling personal information they collect or disclosing it for purposes other than specified purposes in the statute, including to conduct DMV business and for matters of motor vehicle safety and theft. the DPPA also includes provisions making it illegal for persons to knowingly obtain or disclose personal information from a motor vehicle record, for uses not permitted by the statute. The statute provides for liquidated damages (US$2,500) and attorneys' fees for successful suits under the VPPA. In recent years, class action attorneys have attempted to use the DPPA to bring claims arising from data breaches, alleging the disclosure of driver's license information stored on unsecured external servers amounted to a 'knowing disclosure' of such information in violation of the DPPA. But courts have generally not been responsive to such claims. For example, in 2022, the Fifth Circuit upheld a district court's dismissal for failure to state a claim of a putative class action brought under the DPPA that had sought nearly US$70 billion in liquidated damages based on the unauthorised disclosure, through a breach, of driver's licence information.[131]

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

128 Video Privacy Protection Act of 1988, 18 U.S.C. Section 2710.

129 For example, Complaint, *Louth v. NFL Enterprises LLC*, Case No. 1:21-cv-00405-MSM-PAS (D. R.I. 5 October 2021) (putative class action alleging integration of APIs in mobile app relays information about videos users watch on American football mobile application).

130 18 U.S.C. Section 2721 *et seq.*

131 *Allen v. Vertafore, Inc.*, 28 F.4th 613 (5th Cir. 2022).

on authorities and mandates similar to those of the FTC. As discussed in Section II, state privacy laws are dominating the privacy landscape in the US, with a patchwork of laws developing around the country.

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.[132] For example, Massachusetts regulations require companies to have a comprehensive, written information security programme and vendor security controls.[133] All of the comprehensive state privacy laws discussed in Section II include provisions requiring covered entities to adopt reasonable security measures; New York requires a general set of safeguards be implemented by businesses in that state.[134]

General consumer privacy enforcement – 'Little FTC' analogues

Similar to the FTC, state attorney generals 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 FTC Acts in over 40 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. In many 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

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

133 201 Mass. Code Regs. 17.00 (West 2009).

134 N.Y. Gen Bus. Law Section 899-bb.

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.

California is the only state to date that has a privacy agency, the California Privacy Protection Agency. The agency has administrative enforcement powers, rule-making authority, and is also charged with educating Californians about their privacy rights and providing technical assistance and advise to the California legislature.[135]

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,[136] cyberstalking,[137] data disposal,[138] privacy policies, employer access to employee social media accounts,[139] unsolicited commercial communications[140] and electronic solicitation of children,[141] 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 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.[142] All financial institutions licensed and regulated by DFS are required to 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. As noted earlier in this chapter, the New York DFS filed several enforcement actions in 2022 and is proposing to strengthen cybersecurity requirements for businesses subject to its jurisdiction.

135 Cal. Civ. Code Section 1798.199.40.

136 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.

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

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

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

140 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.

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

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

Moreover, a number of states are promulgating similar or even broader cybersecurity requirements. For instance, New York has also enacted 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.[143] The Act's reasonable security requirement went into effect on 21 March 2020. The law is notable for detailing what constitutes reasonable security. The SHIELD Act also makes clear that entities in compliance with data security frameworks under certain other 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.[144] 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.[145]

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.[146] 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.

143 N.Y. Gen Bus. Law Section 899-bb.

144 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.

145 Cal. Bus. & Prof. Code Sections 22580–22582 (West 2015).

146 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.

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 (and some state legislatures) have long recognised privacy torts, with the legal scholar William Prosser building on the famed work of Brandeis and Warren to create a taxonomy of four privacy torts in his 1960 article, 'Privacy'[147] – a taxonomy that was later codified in the American Law Institute's famous and influential Restatement (Second) of Torts.[148] 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 may 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.[149]

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).[150] 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.

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

148 Restatement (Second) of Torts Section 652A (Am. Law Inst. 1977).

149 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//.

150 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.

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 has also changed how the United States approaches certain transfers of information between the United States and other countries. That said, the United States has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by other countries. In particular, the United States was approved in 2012 as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and in 2022 was one of seven economies that participates in APEC that has endorsed the creation of the Global Cross-Border Privacy Forum to transition to a more global approach to cross-border data protection certification.[151] 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.[152]

The EU has long been a complex landscape for international data transfers to the United States. 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 guaranteed in principle to such individuals under EU law.[153] 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 set of updated SCCs meant to govern the transfer of personal data between companies in the EU and US. The new SCCs 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 importing 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 transfer impact 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 data protection law. The EDPB's recommendations guide companies through a six-step process they should undertake before transferring data to countries that are neither in the European Economic Area nor are declared to be adequate by the European Commission. As the US is neither of these, transfers to the

151 US Department of Commerce, Global Cross-Border Privacy Rules Declaration (21 April 2022), https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

152 https://www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs.

153 https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

US must be assessed accordingly, and per the six-step process, there must be an assessment of the risk that third-country national security access to the transferred data might not be protected in an equivalent manner to rights guaranteed by the EU.

In March 2022, the US and the European Commission announced they had committed to a new Trans-Atlantic Data Privacy Framework to foster data flows and address the concerns raised in the *Schrems II* decision.[154] On 7 October 2022, President Biden released Executive Order 14086 on Enhancing Safeguards for US Signals Intelligence.[155] This Executive Order created a series of requirements for the intelligence community and US government that are designed to create greater limitations and safeguards of surveillance activities and an independent redress mechanism of which EU individuals can avail themselves where they believe their personal data has been wrongly used by the US government.

In the months following the release of the Executive Order, US government agencies took steps to implement its requirements. In late June and early July 2023, announcements were made by both the Office of the Director of National Intelligence, confirming that the Intelligence Community related policies and procedures have been updated to implement the privacy and civil liberties safeguards specified in the Executive Order, and the US Attorney General confirmed that the redress mechanism had been established. The Attorney General further confirmed that the EU, Iceland, Liechtenstein and Norway had been declared 'qualifying states' as required for individuals from those jurisdictions to avail themselves of the redress mechanism. In order to 'qualify', the US Department of Justice (DOJ) undertook a detailed legal analysis of European surveillance laws and determined that: (1) EU/EEA Member States require appropriate safeguards in the conduct of signals intelligence activities for United States persons' personal information that is transferred from the United States to the territory of the Member States of the European Economic Area; (2) EU/EEA Member States will permit the transfer of personal information for commercial purposes between the territory of the Member States of the European Economic Area and the territory of the United States; and (3) the designation [as qualifying states] of the EU, Iceland, Liechtenstein, and Norway would advance the national interests of the United States. The DOJ's analysis draws significantly on decisions of the European Court of Human Rights which has set boundaries and limitations on EEA governmental surveillance activities. The DOJ determined the boundaries established by EEA member states were sufficient to meet requirements in the Executive Order, even though some of the EEA member states may have lesser standards than those afforded in the US.

On 10 July 2023, the European Commission released its final EU–US Adequacy Decision. This assessment declares that the United States is adequate for transfers of personal data from the EU where entities participate in the newly formed EU–US Data Privacy Framework (DPF). In order to participated in the DPF, US companies must be subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation. The Department of Commerce administers the DPF. Membership to the DPF largely aligns with membership to the no-longer valid Privacy Shield. Entities must self-certify annually to a set of principles and requirements and must perform related activities such as reflecting

154 The White House, Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework (25 March 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

155 Exec. Order No. 14086, 87 Fed.Reg. 62283 (7 October 2022); 28 C.F.R. Section 201.1 *et seq.*

membership in the DPF in their privacy policies. Entities that do not join the DPF are still able to benefit from the EU–US Adequacy Decision as they are able to rely on the assessment of the US government's practices and use of EU personal data for their transfer impact assessment.

Importantly, aside from transfers from the EU to the US, the DPF also covers transfers from Switzerland to the US and the UK to the US, though the UK portion will only be valid when the anticipated US-UK Data Bridge is finalised, whereby the UK is expected to find the US adequate for data transfers.

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.

Companies are increasingly elevating the level of attention privacy 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;

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; and

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.

In short, companies 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 US Constitution (searches and seizures of persons, houses, papers and effects), ECPA (wiretapping, collection of stored electronic communications and call records),[156] the Right to Financial Privacy Act of 1978 (banking records),[157] Rule 41 of the Federal Rules of Civil Procedure (search warrants), the Foreign Intelligence Surveillance Act of 1978 (national security communications surveillance),[158] the USA PATRIOT Act (national security business records)[159] and so forth. Executive Order 14086 – Enhancing Safeguards for United States Signals Intelligence Activities, issued on 7 October 2022, extends certain legal protections against excessive government surveillance to foreign citizens including, among other things, by providing foreign citizens with a two-level redress mechanism for the review of certain complaints relating to signals intelligence activities by the US.[160]

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 United States when responding to US legal demands and crafting their global privacy and data protection compliance programmes.

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

In 2018, the United States enacted the Clarifying Lawful Overseas Use of Data Act, or the CLOUD Act, which specifically allows foreign governments with robust privacy and civil liberty protections to enter into bilateral agreements with the United States to obtain direct access to electronic evidence for the purpose of fighting serious crime and terrorism.[161] When such an agreement is in place with another country, US law enforcement has the authority to compel US-based technology companies to provide data requested that country's law enforcement entities, regardless of whether the data is stored in the United States or

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

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

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

159 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.).

160 Exec. Order No. 14086, 87 Fed.Reg. 62283 (7 October 2022); 28 C.F.R. Section 201.1 *et seq.*

161 US Dept. of Justice, Cloud Act Resources (17 August 2022), https://www.justice.gov/dag/cloudact.

elsewhere. The United States entered into Data Access Agreements pursuant to the CLOUD Act with Australia in 2021, with the United Kingdom in 2022, and began negotiations with Canada in early 2022.[162] Negotiations with the EU have been ongoing since 2019.

VII PUBLIC AND PRIVATE ENFORCEMENT

As discussed in greater detail above in Sections II and III, the United States 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 California's new privacy agency 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 United States, private litigation also serves as a powerful deterrent. The plaintiff's bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of 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.[163]

162 ibid.

163 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.

IX CYBERSECURITY AND DATA BREACHES

As discussed in greater detail above in Sections II and III, 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 SOFTWARE DEVELOPMENT AND VULNERABILITIES

Companies that produce software procured by US federal agencies are required to comply with and, in the coming months, will be required to attest to their compliance with NIST's Secure Software Development Framework (NIST SP 800-218) and accompanying Software Supply Chain Security Guidance (together, the SSDF Guidance).[164] The NIST SSDF Guidance was developed in response to the Biden administration's May 2021 Executive Order 14028, the *Executive Order on Improving the Nation's Cybersecurity*, a roadmap laying out a plan to fortify nation's cyber defenses, including software supply chain security.[165] The Executive Order directed NIST to develop a secure software development framework and guidance that included specified standards, procedures, and criteria related to software security, and once in place, software providers to federal agencies would need to attest to their compliance with the framework.

In February 2022, NIST published the SSDF Guidance[166] and on 14 September 2022, the Office of Management and Budget issued Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, which requires agencies to obtain attestations of compliance with the NIST SSDF Guidance from producers of software developed after 14 September 2022. For software developed before that date, Memorandum M-22-18 requires attestations to be obtained if the software had a major

164 Office of Management and Budget, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (M-23-16) (9 June 2023) at https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf (Memorandum M-23-16).

165 *Executive Order on Improving the Nation's Cybersecurity* (12 May 2021) at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

166 NIST SP 800-218, Secure Software Development Framework V1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities at https://www.cisa.gov/resources-tools/resources/nist-sp-800-218-secure-software-development-framework-v11-recommendations-mitigating-risk-software; Memorandum M-23-16.

version change or update after 14 September 2022, or if it is a hosted services that deploys continuous updates. As used in Memorandum M-22-18, 'software' includes firmware, operating systems and applications, as well as products containing software.[167]

On 1 March 2023, the White House issued a National Cybersecurity Strategy[168] that included extensive discussion regarding mitigation of risks associated with the software supply chain. Significantly, the Strategy contemplates reshaping laws that govern accountability and liability for data losses and harm caused by cybersecurity errors, software vulnerabilities and other risks created by software and digital technologies.

In April 2023, the Cybersecurity & Infrastructure Security Agency (CISA) released, for public comment, a draft self-attestation form to be used by software companies, based on Memorandum M-22-18 and the NIST SSDF Guidance.[169] In recognition of the fact that initial compliance dates (12 June 2023 for critical software; 14 September 2023 for all other software) were fast approaching, in May 2023, the Office of Management and Budget released an update to Memorandum M-22-18 that extended timelines for agency compliance calculated based on the number of days after final approval of the attestation form is obtained.

CISA and other federal agencies have also begun to address risks associated with the extensive use of open source software, which is not encompassed by Memorandum M-22-18. On 12 August 2023, CISA, the Office of the National Cyber Director, the National Science Foundation, the Defense Advanced Research Projects Agency (DARPA) and the Office of Management and Budget jointly issued a request for information seeking input on where the government should focus areas for prioritisation to secure open source software.[170] The accompanying blog post noted that open source software provides the foundation for 96 per cent of the world's software, and argues it should be considered to be a public good. It characterised building a digital public works programme for open source software as a 'once in a generation' commitment that will inure to the benefit of generations to come, akin to the effort that was required to construct the national highway system in past generations.

This follows on the heels of the April 2023 publication of *Shifting the Balance of Cybersecurity Risk*: *Principles and Approaches for Security-by-Design and -Default*, a guidance document for software companies that outlines methods to make software secure by design.[171] The document was issued jointly by CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA) and the cybersecurity authorities of Australia, Canada, the United Kingdom, Germany, the Netherlands and New Zealand.

167 Office of Management and Budget, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (M-22-18) (14 September 2022) at https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

168 White House, *National Cybersecurity Strategy* (1 March 2023) at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

169 Memorandum M-23-16.

170 CISA, *We Want Your Input to Help Secure Open Source Software* (10 August 2023) at https://www.cisa.gov/news-events/news/we-want-your-input-help-secure-open-source-software.

171 CISA, et al, *Security-by-Design and -Default Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default* (12 June 2023) at https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default.

XI OUTLOOK

Looking forward, we expect the US privacy and cybersecurity landscape to continue to evolve at a rapid pace. The heightened focus on regulating artificial intelligence shows no signs of abating, and we anticipate there will be an increased focus on privacy and security concerns with these technologies. We expect the FTC to continue to leverage the FTC Act to target the agency's concerns around digital advertising tracking technologies and expect that it will take more aggressive actions in the area artificial intelligence in the year ahead. We also anticipate there will legislative or regulatory actions to further regulate data brokers. Enthusiasm at the state level for the passage of comprehensive privacy laws and sectoral laws will likely also continue, especially in the health data context, in areas impacting children and teens and around the use of algorithmic decision-making tools. The coming year will mark the effective date for several of the more onerous state privacy laws, including California's Age Appropriate Design Code Act and newly enacted consumer health privacy laws (e.g., Washington's MyHealth MyData Act), all of which will require businesses to address complex issues including age verification, prescriptive consent requirements, vendor audits and oversight, and having the technical know-how to identify each third party that has placed advertising and analytics technologies on a website or app. The litigation risks associated with the private right of action in the MyHealth MyData Act will also need to be addressed. While hopes for passage of a federal privacy bill continue to be uncertain, it is possible concerns around artificial intelligence could spur legislative action on privacy and related digital governance.

On the cybersecurity front, we expect a continued focus on reporting obligations focused on non-personal information, as sophisticated cyberattacks are being used to disrupt critical infrastructure and other systems, posing dangers well beyond the potential disclosure of personal data. Regulators will expect businesses to take more responsibility for software vulnerabilities and security, especially with respect to software and technologies procured by the federal government. New initiatives being undertaken at the SEC (e.g., the new public company reporting rule) point to the likely increased focus on cyber and AI governance at the corporate-board level as well.

ISBN 978-1-80449-214-7