THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2022
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGERS
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Leke Williams

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

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

www.TheLawReviews.co.uk

ISBN 978-1-80449-116-4

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

ACKNOWLEDGEMENTS

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

ANDERSON LLOYD

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

KALUS KENNY INTELEX

KHODEIR AND PARTNERS

K&K ADVOCATES

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

CONTENTS

Chapter 29

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, and it is easy to consider Warren 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 to address potential risks created by government databases to US states adopting laws imposing data breach notification and information security requirements on private entities, the United States has long innovated in the face of technological and societal change.

---

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

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

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) and, more recently, China's Personal Information Protection Law. In the United States, a series of high-profile data breaches in both the public and private sectors and concerns about misinformation and the misuse of personal information have also created a 'crisis of new technologies' or 'techlash' that is shifting popular views about privacy and cybersecurity.

This past year, concerns about the privacy have been amplified in the wake of the US Supreme Court's 2022 decision in *Dobbs vs. Jackson Women's Health Organization*, as it appears that states that restrict abortion access may seek to obtain sensitive location information and private communications to investigate women seeking abortion care. Federal agencies, particularly the FTC and the Securities and Exchange Commission (SEC), have been active in both privacy and cybersecurity, through proposed rulemaking and enforcement actions. Additionally, legislators in the US Congress made significant progress towards passage of a bi-partisan federal privacy bill, the American Data Privacy and Protection Act (ADPPA), although passage in the current legislative session is uncertain. As in years past, there is much happening at the state level, too. California's new privacy agency commenced rulemaking regarding elaboration and clarification of the requirements of the state's comprehensive data privacy law; the California legislature passed bills around children and teen privacy and mental health data; more states passed comprehensive data privacy laws; and New York regulators proposed new rules to strengthen cybersecurity requirements for insurance companies and other financial institutions.

Overall, issues relating to privacy and cybersecurity are increasingly front-of-mind of 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. The chapter will begin by describing, with a focus on the concrete developments over the past year, the significant shift in how the United States is thinking about privacy and cybersecurity regulation that appears to be underway:

a how the *Dobbs* decision placed issues concerning the collection and use of health data and other types of sensitive personal data front and centre, and along with the growing epidemic of cyberattacks, is prompting intense discussions over the need for further privacy and cybersecurity regulation in the United States;

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

efforts in this regard may face heightened scrutiny in the courts after the US Supreme Court's ruling in *West Virginia v. EPA* limiting Executive Branch authority under the 'major question' doctrine, a novel theory adopted by the Court; and

c how much of the concrete action continues to be not in Washington, DC, but rather in the 50 US states – in California and New York, and now other states including Virginia, Colorado, Connecticut and Utah. In addition to being laboratories for comprehensive privacy legislation, the states have also passed new laws around children and teen privacy (California), employee surveillance and automated decision making. Enforcement efforts and private litigation under state laws such as the Illinois Biometric Privacy Act continues to address evolving technologies and methods of data collection. On the cybersecurity front, New York continues to lead the way with proposals to strengthen the already strict cybersecurity laws for financial institutions regulated by the Department of Financial Services.

Following the detailed discussion of the extensive and significant recent developments, the chapter provides a basic overview of the existing US regulatory and enforcement framework. The chapter will also briefly note certain relevant international developments such as the announcement of a forthcoming US–EU Trans-Atlantic Data Privacy Framework to replace the invalidated Privacy Shield, the Global Cross-Border Privacy Rules Declaration (that will likely supersede the APEC system), the Declaration for the Future of the Internet, and the Cloud Act agreement between the United States and United Kingdom.

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. Privacy concerns moved to the forefront in the aftermath of *Dobbs vs. Jackson Women's Health Organization*, particularly with respect to the commercial availability of health- and location-related data. Soon after the FTC regained its 3-person Democratic majority, it proposed far-reaching new rulemaking around 'commercial surveillance' and data security issues and initiated an enforcement action calling into question the ad tech business model with respect to the sale of location data. Additionally, substantial progress was made on comprehensive federal privacy legislation which, if not passed this legislative session, will likely provide the framework for future federal privacy legislation. And now, in addition to California, four other states will see their own comprehensive data privacy laws come into effect in 2023.

With respect to cyberattacks, noting that rising cyber losses have the potential to 'greatly exceed' what the insurance market is able to absorb, Lloyd's of London announced beginning in March 2023, it would no longer cover losses arising from any state-sponsored cyberattack.[4] Lawmakers and regulators at the federal and state level are working to respond to cyber threats and help businesses identify and implement defences against the significant damages such attacks can inflict. In particular, Congress has adopted legislation imposing

4 Lloyd's Market Bulletin, Ref: Y5381, 'State backed cyber-attack exclusions' (16 August 2022), https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf.

significant new reporting requirements on operators of critical infrastructure, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[5] The requirements will become effective after a regulatory proposal and comment period being conducted by the Cybersecurity and Infrastructure Agency (CISA). The first set of public comments on CISA's proposals are due in November 2022. The SEC also published regulatory proposals to impose new cybersecurity standards and reporting rules for publicly traded companies and for SEC-regulated investment advisers. A further SEC proposal is also expected soon that would impose data breach notification requirements and new data security standards applicable to protect the personal information of investors held by securities firms.

In short, the privacy and data security landscape in the United States is continuing to undergo extensive development and change with the federal government, state governments and private industry all taking consequential steps

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 A heightened focus on privacy in the wake of *Dobbs v. Jackson Women's Health Organization*

The US Supreme Court's decision in *Dobbs*, which held that the US Constitution does not confer a right to an abortion (under 'privacy', 'liberty' or 'equal protection' theories), has precipitated a flurry of data privacy activity at the state and federal levels. The absence of the Constitutional right to abortion allows states to enact or revive laws criminalising activity in support of prohibited abortions. The risk of criminal investigation and prosecution has sparked concerns about privacy for health data and other types of data, including messages on social media platforms, search histories and precise geolocation data, which could be used to identify those seeking abortion access or providing assistance.

Soon after the *Dobbs* opinion was released, on 29 June 2022, the Biden administration's Department of Health and Human Services (HHS) issued guidance directing health care providers that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) prohibits the disclosure to law enforcement (or any third party) about reproductive health care, including an individual's decision to seek an abortion 'in the absence of a mandate enforceable in a court of law.'[6]

The HHS guidance was followed by the Biden administration's 8 July 2022 Executive Order which, among other things, directed the FTC and HHS to 'address the potential threat to patient privacy caused by the transfer and sale of sensitive health-related data and by digital surveillance related to reproductive healthcare services' and expressly 'encouraged' the FTC Chair to consider actions to protect consumers' privacy in this regard.[7]

5 CISA, 'Cyber Incident Reporting for Critical Infrastructure Act of 2022' (CIRCIA), at https://www.cisa.gov/circia.

6 HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care, at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html (last accessed on 1 September 2022).

7 Executive Oder No. 14076, 87 Fed. Reg. 42053-54 (8 July 2022).

Four high-profile Democrats also called upon the FTC for assistance in protecting reproductive privacy rights, in a letter to the agency calling for investigations into companies engaged in collecting and selling mobile phone location data that could be obtained by law enforcement to prosecute people who visit abortion providers and those who assist them.[8]

The FTC responded to these calls and soon thereafter published a blog post highlighting 'unprecedented intrusion' created by the combination and sale of sensitive personal data collected through smartphones, wearable fitness trackers and browsers and the 'particularly sensitive subset' of location and health data that could be used to, among other things, target women considering abortion.[9] That post foreshadowed the FTC's action, filed on 29 August 2022, against ad tech company Kochava, which claims the company engages in unfair practices in violation of Section 5(a) of the FTC Act by allegedly selling and otherwise making available to others, consumers' precise geolocation data that could reveal consumers' visits to sensitive locations, including 'locations associated with medical care [and] reproductive health'.[10] The FTC complaint is notable in that it does not allege that Kochava misrepresented or did not disclose that it collected and disclosed personal data, including location data; rather, the complaint alleged Kochava was engaged in 'unfair' practices by the nature of the business in which it was engaged which, the FTC alleged, could 'cause or [be] likely to cause substantial injury to consumers'.[11]

Concerns about the privacy of reproductive health choices have also spurred legislative proposals to limit the type of information collected through personal health mobile apps and to prevent the use of data collected through such apps from being used against consumers seeking an abortion.[12]

ii Key federal government privacy and data protection actions

Over the past year, all three branches of the federal government have taken significant steps with respect to privacy and data protection.

Executive branch – recent enforcement cases and proposed rules

The FTC had another active year with several enforcement actions and the issuance of its Advanced Notice of Proposed Rulemaking released in August 2022. Many of the agency's actions highlight the intersection between data privacy and data protection, with settlements and consent orders that address both concerns.

For much of the year, the FTC was deadlocked on a number of issues because the Commission was evenly split between two Democratic appointees (Chair Lina Kahn and

8 Letter to FTC Chair Lina Kahn from Senators Ron Wyden, Elizabeth Warren and Cory A. Booker and US Representative Sara Jacobs (24 June 2022), https://assets.law360news.com/1506000/1506062/letter-to-ftc-chair-lina-khan-on-ad-ids-and-privacy.pdf.

9 FTC Business Blog, Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data (11 July 2022) at https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use (last accessed on 4 September 2022).

10 Complaint for Permanent and Injunction and Other Relief, *Federal Trade Commission v. Kochava Inc.*, Case No. 2:22-cv-00377-DCN (D.C. Idaho 29 August 2022).

11 ibid.

12 For example, on 16 June 2022, US Representative Sarah Jacobs introduced the My Body, May Data Act of 2022 which would limit the ability to collect personal reproductive or sexual health information in instances where HIPAA does not apply. H.R. 8111, 117th Congress (2021–2022).

Rebecca Slaughter) and two Republican appointees (Noah Philips and Christine Wilson) following the October 2021 departure of Democratic-appointed Commissioner Rohit Chopra to head the Consumer Financial Protection Agency. In May 2022, the US Senate confirmed Democratic nominee Alvaro Bedoya as a new FTC Commissioner which will allow the FTC to pursue a more aggressive agenda, as evidenced by several of its actions taken after the confirmation, including a new Advanced Notice of Proposed Rulemaking, which was opposed by the two Republican Commissioners. In August 2022, long-time FTC Commissioner Noah Phillips announced his plan to resign in the autumn of 2022. Because only three FTC commissioners may be appointed from the same party, the Biden administration will need to nominate a Republican (or Independent) to succeed Mr Phillips.

Notable privacy and security enforcement actions

In response to and on the heels of the various calls on the FTC to take action in response to the *Dobbs* decision, in August 2022 the FTC filed an enforcement action against ad tech company Kochava, previewed above, which alleges the company engaged in 'unfair' practices under the FTC Act because it collects sensitive personal information from third parties, such as location and health-related data, and allows others to purchase or otherwise access such information. Other than the putative unfairness of the business model, the FTC has not made any other specific allegations of wrongdoing, such as undisclosed secondary uses of data or lax security measures, that were at issue in other FTC enforcement actions this year. At the time of writing, there is no proposed settlement with Kochava; the company appears to be challenging the FTC's action; just weeks before the FTC filed its action, the company pre-emptively filed its own suit against the FTC seeking a declaratory judgment to prevent the FTC's action from going forward.

The FTC also brought enforcement actions focusing on children's privacy, which the agency has identified as one of its enforcement priorities. In one such action, the FTC announced a US$2 million settlement with OpenX, an online advertising platform, regarding allegations the company had collected personal information from children under 13 without parental consent in violation of the Children's Online Privacy Protection Act (COPPA). The December 2021 complaint alleged the company had reviewed several apps and classified them as child-directed, yet allegedly allowed the apps to participate in an ad exchange that collected and sold personal information about app users under age 13 without obtaining parental consent, allowed targeted advertisements to be delivered to children, and failed to recognise opt-out requests. The FTC also alleged that the company's privacy policy disclosures were inconsistent with its practices. In addition to the monetary penalty, the settlement also requires OpenX to delete any ad request data that it collected prior to the date of the settlement.

Children's privacy issues were also at issue in the agency's March 2022 settlement with WW International, Inc, formerly known as Weight Watchers, and its subsidiary Kurbo, Inc. This case also involved the collection of personal information from children under 13 allegedly without parental consent, in violation of COPPA. The complaint alleged that, while the company implemented an age gate requiring users to enter their age and prevented access to the app for users who indicated they were younger than 13 years of age, it was relatively easy for minors to falsify their age after being initially locked out. The settlement includes a US$1.5 million fine and also requires the company to destroy any algorithms it developed using the data allegedly collected without parental consent.

Other FTC actions focused on secondary uses of personal information, where data is collected for one stated reason, but then used by a business for other undisclosed purposes. For example, in May 2022, the FTC filed an action against Twitter for violation of the FTC Act and a prior consent decree based on allegations the company collected phone numbers and email addresses to facilitate account security, but subsequently allegedly used that data for targeted advertising. While the company's privacy policy disclosed that it would use contact information for advertising, the FTC alleged this did not suffice to 'override or negate' the company's representations that it was collecting phone numbers and email addresses for authentication purposes.[13] Twitter settled and agreed to pay a US$150 million fine and undertake various remedial actions, including not using, providing access to or disclosing, for the purpose of serving advertising, any of the phone numbers and emails originally collected to enable account security features. It also requires that Twitter implement multi-factor authentication that does not rely upon phone number-based verification.

The FTC's focus on undisclosed secondary uses of personal information was also highlighted in its June 2022 action against the former owner of CaféPress.com, a customised merchandise website, that initially came onto the FTC's radar as a result of a large data breach. During the course of the FTC's breach investigation, the agency uncovered that the company had allegedly been using addresses collected for 'order notifications and receipt' to deliver marketing emails. CaféPress entered into a Consent Agreement that, in addition to a US$500,000 fine, includes highly detailed information security requirements.[14]

Advance Notice of Proposed Rulemaking and a New ISP Report

In the wake of Commissioner Bedoya's appointment and renewed 3-2 Democratic majority on the Commission, on 22 August 2022, the FTC issued an Advance Notice of Proposed Rulemaking (ANPR) that seeks public comment on a list of 95 multi-part questions primarily regarding what the FTC characterises as the 'prevalence of commercial surveillance and data security practices that harm consumers.'[15] While it could take several years for this rulemaking to conclude, the ANPR nevertheless signals the issues that are top of mind for the agency and could be used to build a record of 'unfair' or 'deceptive practices' for future enforcement actions. The ANPR's questions focus on ways in which data collection and lax security practices arguably harm consumers, harm children and teenagers, and how the FTC should balance the costs and benefits of data collection practices. Other questions concern data

13 Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter In the Matter of Twitter, Inc., FTC Commission File No. 2023062 (25 May 2022) at https://www.ftc.gov/system/files/ftc_gov/pdf/2023062TwitterChairStatement_0.pdf (last accessed 5 September 2022).

14 For example, multi-factor authentication is required, but the Consent Agreement mandates the company cannot rely upon security questions. Additionally, the company is required to implement procedures to encrypt all Social Security numbers, restrict inbound access to approved IP addresses, review for vulnerabilities all web application code, and implement data minimisation requirements, among other measures.

15 FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (22 August 2022). In the ANPR, the FTC defines 'commercial surveillance' as the 'collection, aggregation, analysis, retention, transfer, or monetisation of consumer data and the direct derivatives of that information' and notes that it encompasses data that consumer actively provide as well as identifiers and other data companies collect passively when, for example, browsing the web or opening an app.

security requirements, the effectiveness of data minimisation, automated decision-making systems and whether the FTC should ban certain types of companies from engaging in any personalised or targeted advertising.

A notable feature of the ANPR rulemaking is that it focuses on how these issues affect employees and workers, not only consumers. This may signal a new flank in FTC enforcement actions, as the FTC has not typically regulated employees and represents a notable development. It comes on the heels of a July 2022 Memorandum of Understanding between the FTC and the National Labor Relations Board regarding information sharing designed to 'help protect workers against unfair methods of competition, unfair or deceptive acts or practices, and unfair labour practices', including the impact of algorithmic decision-making on workers.[16]

Commissioners Wilson and Phillips objected to the issuance of the ANPR, with Commissioner Phillips stating he views the ANPR as 'recast[ing] the Commission as a legislature', based upon the far-reaching scope and content of the questions posed.[17] The process nevertheless continues, with public hearings and general public comment period well underway. Commissioner Phillips also criticised the ANPR for adopting a 'dystopic' view of modern commerce and using the 'academic pejorative' term 'commercial surveillance'.

Many of the themes articulated in the ANPR were foreshadowed by the FTC's October 2021 report on the privacy practices of internet service providers, 'A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers'.[18] The report summarised and analysed the responses the FTC received from six ISPs about their data collection and use practices. The report identified several issues of concern to the agency, including transparency about use cases, confusing consumer choice interfaces, low rates of data access by consumers, and data retention and minimisation policies.

Cybersecurity

The Biden administration and federal agencies remain actively engaged in cybersecurity matters, as cyberattacks steadily continue. In January 2022, President Biden signed a National Security Memorandum which implemented requirements from Executive Order 14028 ('Improving the Nation's Cybersecurity') by setting out specific cyber requirements for government agencies and contractors, such as multifactor authentication, encryption, cloud technologies and endpoint detection services.[19] In March 2022, Congress passed and President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which would require critical infrastructure entities to report cyber incidents

16 https://www.ftc.gov/system/files/ftc_gov/pdf/ftcnlrb%20mou%2071922.pdf (last accessed 6 September 2022).

17 FTC, Dissenting Statement of Commissioner Noah Joshua Phillips Regarding the Commercial Surveillance and Data Security Advanced Notice of Proposed Rulemaking (11 August 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf (last accessed 6 September 2022).

18 FTC, A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers (21 October 2022).

19 The White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (19 January 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems//.

within 72 hours and ransomware payments within 24 hours to CISA.[20] On its Shields Up website, CISA issues regular updates about cybersecurity news, alerts and guidance for organisations to fortify cybersecurity systems and incident response, cyber-related recommendations for corporate leaders and CEOs, ransomware response information and information for individuals about how to protect themselves online.[21] A consistent theme in these developments is the critical role public–private partnerships play and will continue to play in the future of cyber defence.[22]

In October 2021, the FTC announced a newly updated Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA) that applies to financial institutions regulated by the agency (such as mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counsellors and other financial advisers, tax preparation firms, non-federally insured credit unions, and investment advisers that are not registered with the SEC).[23] The substantive provisions of the Safeguards Rule comes into force in December 2022 and will impose detailed security requirements. The requirements in the new Rule are patterned on the rigorous standards imposed by the New York Department of Financial Services, and include requirements to institute multi-factor authentication, encrypt customer information at rest and in transit, and to designate a qualified individual to be responsible for an institution's security program.

The SEC has also been active in cybersecurity matters. In February 2022, the SEC proposed cybersecurity risk management and reporting rules for investment advisers registered with the SEC.[24] A month later, it announced new cybersecurity rules for public companies.[25] Notable features of the proposed rules include new requirements to make disclosures about cybersecurity risk management, strategy, governance, and incident reporting. Additionally, the proposed rule appliable to public companies requires reports to the SEC of all 'material' cybersecurity incidents within four business days of determining the event's materiality. This provision that has garnered criticism from the cybersecurity community because the short reporting period does not include exceptions for active investigations by law enforcement or coordination with intelligence and national security agencies, nor does it provide a reporting exception where disclosure of the incident could be required before the vulnerability could be patched.[26]

20 CISA, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), https://www.cisa.gov/circia.

21 https://www.cisa.gov/shields-up.

22 See Sasha Hondagneu-Messner, Steve McInerney, Alan Charles Raul, 'Cyclops Blink' Shows Why the SEC's Proposed Cybersecurity Disclosure Rule Could Undermine the Nation's Cybersecurity (30 August 2022), https://www.lawfareblog.com/cyclops-blink-shows-why-secs-proposed-cybersecurity-disclosure-rule-could-undermine-nations.

23 16 Code of Fed. Regulation Section 314.1 et seq.

24 SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds (9 February 2022), https://www.sec.gov/news/press-release/2022-20.

25 SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (9 March 2022), https://www.sec.gov/news/press-release/2022-39.

26 See Sasha Hondagneu-Messner, Steve McInerney, Alan Charles Raul, 'Cyclops Blink' Shows Why the SEC's Proposed Cybersecurity Disclosure Rule Could Undermine the Nation's Cybersecurity (30 August 2022), https://www.lawfareblog.com/cyclops-blink-shows-why-secs-proposed-cybersecurity-disclosure-rule-could-undermine-nations.

Continued cyberattacks on the healthcare system have given rise to several sector-specific responses. In June 2022, the White House sponsored a Healthcare Cybersecurity Executive Forum, hosted by White House Cyber Director Chris Inglis and attended by senior government cybersecurity officials, and CEOs and other senior executives in the healthcare security area.[27] In April 2022, the Federal Drug Administration (FDA) refreshed its existing draft guidance on Cybersecurity in Medical Devices, noting the need for effective cybersecurity in the medical device area has become more important with the proliferation of wireless, internet- and wireless-connected devices and the frequent exchange of medical device-related health information.[28] Additionally, the Healthcare Sector Cybersecurity Coordination Center (HC3) continues to serve as the HHS focal point for cybersecurity collaboration within the healthcare sector.[29]

Future of the internet

In April 2022, the White House issued a Declaration for the Future of the Internet, also known as the DFI.[30] The Declaration sets forth the shared principles regarding how parties should comport themselves with respect to the internet, the digital ecosystem, and the digital economy. Signatories commit to defending the internet, to governing it by a multi-stakeholder approach, and to promoting an open, free, global, interoperable, reliable, and secure internet for the world. The Declaration responds to a variety of developments around the world that pose a challenge to the idea of an open internet, such as limiting access to the internet, the rise in cyberattacks threatening the security of critical infrastructure and healthcare systems, and the proliferation of disinformation on the internet.

Legislative actions

Perhaps the most significant federal legislative development was the progress made on the bi-partisan federal privacy bill, the ADPPA. The bill includes familiar privacy rights to access and delete personal data and limitations on the use of sensitive data, has data minimisation provisions and restricts the purposes for which companies would be allowed to collect personal information, including targeted advertising. It would impose strict limits on targeted advertising, including prohibiting targeted ads for minors and targeted ads based upon individuals' browsing histories and behaviours and other types of sensitive data. Adoption of ADPPA has stalled primarily on two issues: whether the new federal law would pre-empt state privacy laws and whether individuals would have private right of action to enforce the law (in addition to the FTC and state Attorneys General). Nevertheless, privacy advocates believe the contents of this bill and the privacy framework it established will likely be able to be used in future attempts to pass a federal privacy bill.

27 https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/16/readout-of-healthcare-cybersecurity-executive-forum-hosted-by-national-cyber-director-chris-inglis/.

28 Food and Drug Administration, HHS, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions; Draft Guidance for Industry and Food and Drug Administration Staff, 87 Fed. Reg. 20873 (8 April 2022).

29 HHS, HC3 FAQs, https://www.hhs.gov/about/agencies/asa/ocio/hc3/faq/index.html.

30 White House, A Declaration for the Future of the Internet (28 April 2022).

Judicial branch – A new threat to agency rulemaking

The US Supreme Court's June 2022 decision in *West Virginia vs. EPA* represents one of the most potentially consequential decisions for the future of federal privacy and cybersecurity regulation in the United States, as it signals the US Supreme Court's desire to limit the power of agencies (i.e., the Executive Branch of government) to regulate matters of critical political or economic significance without a clear statement to that effect by Congress. In *West Virginia vs. EPA*, the Court struck down regulations promulgated by the Environmental Protection Agency to combat climate change that would have required existing coal-fired power plants to shift their fuel sources to natural gas, wind or solar power.[31] The Court characterised the regulation as an 'assertion . . . of extravagant statutory power over the national economy' and invalidated it under the 'major questions doctrine'. Under that doctrine, when agencies 'claim the power to make decisions of vast 'economic and political significance', they must point 'clear congressional authorization'. In articulating the parameters of what constitutes a 'major question', Justice Gorsuch's concurring opinion explained it may apply when 'an agency claims the power to resolve a matter of "political significance"', when it seeks to regulate a 'significant portion of the American economy' or when the agency seeks to 'intrude into an area that is a particular domain of state law'.[32]

It is conceivable that the newly announced major questions doctrine could be used to invalidate privacy and cybersecurity regulations based on broad consumer protection statutes like the 'unfair or deceptive' standard administered by the FTC. For example, the FTC's grandiose new ANPR might run afoul of 'major question' doctrine.

Across the country, federal courts continued to hear matters touching privacy and cybersecurity issues. In the Ninth Circuit, these include a new wave of lawsuits brought under California wiretap law, the California Invasion of Privacy Act (CIPA). These suits seek to apply provisions in state wiretap law to internet communications and the technologies that service providers and website operators use to assist in identifying, verifying and monitoring users, including their use patterns. In an unpublished decision on 31 May 2022 in *Javier vs. Assurance IQ, Inc.*, the Ninth Circuit interpreted CIPA to require express prior consent be obtained before a company's service providers can monitor communications between a user and service provider.[33] These CIPA cases are being closely watched as they are increasingly being used to threaten litigation and demand pay-outs from consumer-facing companies.

iii Key state privacy and data protection actions

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

31 *West Virginia vs. Environmental Protection Agency*, 597 U.S. ___ , slip op. at 2 (2022).

32 id. at 9-11.

33 Memorandum, *Javier v. Assurance IQ, Inc. et al.*, D.C. No. 4:20-cv-02860-JSW (9th Cir. 31 May 2022).

California's data privacy regime

California Consumer Privacy Act

California privacy law continues to dominate the state data privacy landscape. The California Consumer Privacy Act (CCPA),[34] a comprehensive privacy bill that commentators have called 'California's GDPR', continues to be the focal point of privacy law in the state and nationwide. The Amendments to CCPA enacted through the California Privacy Rights Act (CPRA) that come into effect on 1 January 2023 have been the subject of ongoing rulemaking. Significantly, the CCPA's exemptions for employment and B2B data have not been added to the CPRA, which means that beginning on 1 January 2023, the CCPA will apply in full to the personal information of employees, job applicants and business contacts. This significant expansion of the law makes California the outlier, as other state data privacy laws scheduled to come into effect in 2023 (and the proposed federal ADPPA) broadly exempt employment and commercial data. Given California's size and the fact that it is the home of Silicon Valley, the CCPA and CPRA are having a wide impact, and companies across the United States and around the world are considering what it might mean for them.

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

a Modification of the definition of a covered 'business': the CCPA applies to for-profit entities that are doing business in California; that collect or determine the means of processing personal information; and that meet one of three size thresholds.[35] The CPRA modifies the definition of a covered business that both increases and decreases the number of businesses currently subject to the CCPA.

b Expansion of disclosure requirements: the CCPA mandates broad privacy policy disclosure requirements on companies that collect personal data about California residents.[36] The CPRA introduces 'sensitive personal information' as a new regulated dataset in California. The category is subject to new disclosure and purpose limitation requirements, and consumers have new rights designed to limit businesses' use of their sensitive personal data. Businesses must also disclose the length of time the business intends to retain each category of personal information or the criteria that would be used to determine the retention period.

c Creation and expansion of consumer privacy rights: the CCPA mandates that businesses provide California residents with the rights to access and delete their personal information, as well as the right to stop the sale of their information to third parties.[37] The CPRA provides new rights and amends existing rights. Some of the new rights include the right to correction, the right to opt-out of automated decision-making technology, the right to access information about automated decision making and the right to limit use and disclosure of sensitive personal information. Some of the modified rights include a modified right to delete, an expanded right to know, an expanded right to opt-out and an expanded right to data portability. Perhaps the most

34 Cal. Civ. Code § 1798.100 et seq.

35 Cal. Civ. Code Section 1798.140 (c).

36 id. Section 1798.140 (g).

37 id. Section 1798.105 (a), 120 (a).

significant feature of the CPRA is the provision that gives consumers the right to stop a business from sharing their personal information with third parties for the purpose of engaging in 'cross-context behavioural advertising'.

d Strengthening of opt-in rights for minors: the CCPA prohibits businesses from selling personal information of individuals under the age of 16, absent affirmative authorisation.[38] As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her personal data after the minor has declined to provide it. The CPRA also increases fines for violations of the opt-in right for minors.

e Expansion of triggering data for a breach: the CCPA provides a private cause of action for certain data breaches that result from a business's violation of the duty to implement and maintain reasonable security procedures and practices.[39] The CPRA expands the CCPA's private right of action for breaches of certain login credentials that would permit access to an account if the business failed to maintain reasonable security.

f Creation of a new privacy enforcement authority: the CCPA authorises the California Attorney General to enforce its provisions with statutory fines of up to US$7,500 per violation.[40] The CPRA restructures this enforcement regime by establishing the California Privacy Protection Agency (CPPA), the first data protection agency in the United States, empowered to promulgate regulations supporting the CPRA and to enforce the CCPA and CPRA after it becomes effective. Moreover, the CPRA essentially removes the 30-day cure period that businesses currently have under the CCPA after being formally notified of an alleged violation. Instead, the CPPA has discretion to provide businesses with a time period to cure and may take into account 'voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of [a] complaint' made by any person. Businesses will still have the opportunity to cure violations of personal information security breaches within 30 days, but only to the extent the violations are curable.

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

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

The Office of the California Attorney General (OAG) has been actively enforcing the CCPA, sending violation notice letters in various 'enforcement sweeps'.[41] In August 2022, the OAG filed its first public enforcement action under the CCPA and negotiated a proposed settlement that would fine the defendant, cosmetics company Sephora, US$1.2 million and require the company to undertake various actions to comply with the law and submit

38 id. Section 1798.120 (d).

39 id. Section 1798.140 (w)(2)(B).

40 id. Section 1798.155 (b).

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

compliance reports to the OAG. The enforcement action is significant because it highlighted the CCPA's focus on respecting opt-outs for the sale of personal information, including the use of third-party advertising trackers. The action also communicated OAG's expectation that businesses recognise the Global Privacy Control's opt-out preference signal, include opt-out mechanisms on their webpages, and ensure service provider contracts are in place with all vendors to prevent shared personal information from being characterised as a 'sale' under the statute. The OAG's announcement was accompanied by additional guidance pointing to other enforcement priorities, including disclosures around financial incentives and ensuring opt-out choices are clearly described without confusing toggles and buttons.[42]

Moreover, since the CCPA went into effect on 1 January 2020, there have been many cases filed around the country under the CCPA's private right of action for data breaches resulting from the failure to implement reasonable security practices. The vast majority of those cases have been filed in federal courts in California.

The new CPPA has been active in rulemaking efforts. The CPPA also came out strongly against the federal privacy bill, issuing a detailed letter criticising the proposed legislation for pre-empting California and other states' privacy laws.[43]

New California privacy bills

The California legislature passed two significant privacy bills in the 2021–22 legislative session, both of which are still on the desk of the Governor as of this writing. The California Age Appropriate Design Code Act (AADCA) would impose a variety of obligations and restrictions on businesses that develop and provide online services, products or features that minors under 17 are 'likely to access.' Modelled after the UK's Age Appropriate Design Code, the AADCA would first come into effect on 1 July 2024 and would require businesses to configure privacy settings to high levels of privacy, and restrict their ability to profile minors and collect geolocation information. Data protection impact assessments would also be required, including for products already in existence when the law would come into effect. Just like the original version of CCPA, the Attorney General has sole enforcement powers (e.g., no private right of action) and statutory penalties are authorised (up to US$7,500 per 'affected child'). Unlike the CCPA, there is a mandatory 90-day cure period for businesses that are in 'substantial compliance' with the law.

The California legislature also passed another bill that would classify providers of mental health apps as healthcare providers under the California Confidentiality of Medical Information Act (CMIA). As a provider subject to CMIA, mental health apps would be subject to HIPAA-like constraints on their ability to use and share data collected and will have increased litigation exposure, as CMIA includes a private right of action. Passage of the bill comes on the heels of US Congressional inquiries about the use and protection of health data collected by mental health apps and an uptick in private litigation in the area. If this bill becomes law, it will be effective beginning on 1 January 2023.

42 CCPA Enforcement Case Examples, https://oag.ca.gov/privacy/ccpa/enforcement.

43 https://cppa.ca.gov/pdf/hr8152_oppose.pdf.

Other state privacy laws

California has long been a privacy bellwether, as its legislative actions have often prompted other states to follow suit: for example, California was the first state to enact a data breach notification law, and all 50 states now have one. It is thus unsurprising that the passage of the CCPA has prompted numerous other states to consider privacy legislation. Nevada became the first state to follow the CCPA trend when, on 29 May 2019, it enacted a law that grants consumers the right to opt-out of the sale of personal information. While Nevada's law is not as comprehensive as the CCPA, it entered into force earlier on 1 October 2019.[44] Recent amendments to the law, signed by the Nevada Governor, include exemptions of certain persons and information collected about a consumer from the law's privacy requirements, expansion of the types of entities that must facilitate consumer privacy opt-out rights, provision of new and updated definitions, authorisation of the opportunity to remedy a failure to comply with certain requirements and updated provisions to reflect the addition of data broker entities.[45] Maine also followed California's footsteps, with the Governor signing into law the 'Act to Protect the Privacy of Online Consumer Information' on 6 June 2019, which officially went into effect on 1 August 2020.[46] Again, this law is not as comprehensive as the CCPA, but it does obligate internet service providers in Maine to obtain permission from their customers before selling or sharing their data with a third party.

More recently, Connecticut and Utah joined Virginia and Colorado in passing comprehensive privacy legislation.[47] Both laws contain familiar new rights and obligations, including the right to opt out of targeted advertising and profiling, new limits on collection and required appeals process, restrictions on the use of 'sensitive data' and the requirement to conduct data protection assessments for certain processing activities.

If federal privacy legislation does not pass, it is anticipated several states will again attempt to pass comprehensive privacy bills. Attempts to pass legislation in Washington state, Massachusetts, New York and other states fizzled out again this year. Several states have also passed laws adopting prescriptive data security requirements for insurers that generally track the Insurance Data Security Model Law adopted by the National Association of Insurance Commissioners (NAIC), with Kentucky, Maryland and Vermont joining 19 other states in the past year.[48]

States are continuing to take the lead in regulating emerging technologies, although there has been some cooling of moves in 2020 to ban the use of facial recognition technologies and some states and cities have reversed earlier bans.[49] Increased attention on the use of monitoring technologies and algorithms in the employment context has given rise to new laws requiring transparency around the use of such technologies[50] and guidance from the Equal Employment Opportunity Commission (EEOC) regarding how to comply with the Americans With Disabilities Act when using software that relies upon algorithmic

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

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

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

47 Connecticut Enacts Comprehensive Consumer Data Privacy Law (11 May 2022), https://iapp.org/news/a/connecticut-enacts-comprehensive-consumer-data-privacy-law/.

48 2022 Ky. Acts 149; Md. Code Ann, Ins. § 33-109 (2022); 8 V.S.A. Section .4278 (2022).

49 U.S. Cities are Backing Off Banning Facial Recognition as Crime Rises, https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/.

50 NYC Local Law Int. 1894-A (11 December 2021); 6 NYCRR Section 52-c.

decision-making.[51] 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. These laws, which generally require notice and opt-out, limitations on the commercial use of acquired biometric data, destruction of the data after a certain amount of time, and employment of industry standards of care to protect the data, will likely continue to be an area of focus.

State data protection actions

Besides taking the lead on enacting broad, cross-sectoral privacy and data security legislation and updating their data breach notification laws, states are also taking the lead in putting in place and enforcing cybersecurity regulatory regimes. One regulator that continues to be active in this space has been the New York Department of Financial Services (DFS). With its ground-breaking Cybersecurity Regulation, which took effect in March 2017, DFS is now actively enforcing its prescriptive cybersecurity requirements.

On 29 July 2022, DFS posted proposed amendments to the Cybersecurity Regulation that would impose even more stringent requirements on all companies subject to its jurisdiction and impose even stricter requirements on larger companies, based on the size of their workforce or global annual revenue.[52] Taken as a whole, the proposed new requirements usher in more prescriptive cyber controls (e.g., mandating annual penetration testing; multi-factor authentication (MFA); phishing testing) and will require increased involvement by senior officers and board members in cybersecurity matters, coupled with the potential for increased legal exposure. The proposed DFS regulations would truncate cybersecurity incident reporting periods, including by requiring regulated institutions to report, within 24 hours, any ransom payments made in response to an incident. As of this writing, the proposed regulations are still subject to a public comment period.

In June 2022, DFS announced a US$5 million settlement with a cruise ship company based on the company's alleged failure to implement adequate cybersecurity protections, including its delayed implementation of MFA, and its failure to timely report to DFS the first of four cybersecurity incidents.[53] On 2 August 2022, DFS announced another settlement, a US$30 million penalty against a crypto currency exchange, based on allegations the company was not compliant with cybersecurity and transaction monitoring requirements and, in addition, improperly certified its compliance with those DFS regulations.[54]

51 The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees (12 May 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence.

52 NYDFS Proposes Significant Changes to Its Cybersecurity Rules, NYU School of Law Program on Corporate Compliance and Enforcement (1 August 2022), https://wp.nyu.edu/compliance_enforcement/2022/08/01/nydfs-proposes-significant-changes-to-its-cybersecurity-rules/.

53 DFS Superintendent Harris Announces $5 Million Penalty on Cruise Company Carnival Corporation and Its Subsidiaries for Significant Cybersecurity Violations (24 June 2022), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202206241.

54 DFS Superintendent Harris Announces $30 Million Penalty on Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations (2 August 2022), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202208021.

State courts

Just as the federal courts have decided a number of recent important privacy and data security cases, so too have state courts. While a complete canvas of all of these decisions is beyond the scope of this chapter, highlighting a couple of examples serves to demonstrate the general point.

The Illinois Biometric Information Privacy Act (BIPA) provides a private right of action for aggrieved individuals, and the Illinois Supreme Court has held that bare procedural violations of the statute are sufficient to establish standing.[55] A wide range of technology companies, including Facebook, Shutterfly, Snapchat and Google, are finding themselves defending their implementation of facial, and more recently, voice recognition technology against BIPA claims in Illinois courts. In one of the most publicised BIPA actions against Clearview AI, the court approved a settlement between Clearview and the American Civil Liberties Union that prohibits Clearview from making its faceprint database available to most businesses and private entities in the US and bars the company from selling access to its database to any entity in Illinois for a period of five years.[56] Another notable development in BIPA litigation was the ruling by the Illinois Supreme Court that state workers compensation law did not pre-empt BIPA claims for statutory damages, a defence many employers relied upon in defending such claims.[57] As of this writing, the Illinois Supreme Court is considering one of the most potentially consequential BIPA issues that focuses on claim accrual, including whether statutory damages are available only the first time a business violates the statute (e.g., the first time an employee's fingerprint is scanned without notice) or whether damages accrue with each violation (e.g., every subsequent fingerprint scan).[58] If the court decides that damages accrue with each violation, resulting damages claims could be astronomical because the statute provides for statutory damages of US$1,000 or US$5,000 per violation, without the need to establish actual harm.

III REGULATORY FRAMEWORK INCLUDING PUBLIC AND PRIVATE ENFORCEMENT

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

55 740 Ill. Comp. Stat. § 14/1 – 99 (2008); *Rosenbach v. Six Flags Ent Corp*, No. 123186, 2019 IL 123186 (25 January 2019).

56 *ACLU v. Clearview AI* – Court Cases (11 May 2022), https://www.aclu.org/cases/aclu-v-clearview-ai.

57 *McDonald v. Symphony Bronzeville Park, LLC, et al.*, 2022 IL 126511 (3 February 2022).

58 BIPA Claims Don't Mean Ruinous Damages, Ill. Justices Hear (17 May 2022), https://www.law360.com/articles/1494223/bipa-claims-don-t-mean-ruinous-damages-ill-justices-hear.

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.[59] 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.[60] 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 practices in or affecting commerce'.[61] An act or practice is deceptive under Section 5 if there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and the representation or omission is 'material'. The FTC has taken action against companies for deception when companies have made promises, such as those relating to the security procedures purportedly in place, and then not honoured or implemented them in practice. An act or practice is 'unfair' under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition. (This statutory framework for determining when the FTC can penalise a practice as unfair is widely acknowledged to be a cost-benefit analysis test.) The FTC understands unfairness to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context.

A few examples of what the FTC believes constitutes unfair or deceptive behaviour follow. First, the FTC takes the position that, among other things, companies must disclose their privacy practices adequately and that, in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses.[62]

---

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

60 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).

61 id. at Section 5.

62 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

Second, the FTC also takes the position that Section 5 generally prohibits a company from using previously collected personal data in ways that are materially different from, and less protective than, what it initially disclosed to the data subject, without first obtaining the individual's additional consent.[63]

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

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

b maintaining data security and limiting data retention;

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

d express consent before using sensitive data for behavioural advertising.[64]

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

In terms of enforcement, the FTC has frequently brought successful actions under Section 5 against companies that did not adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments, or failed to provide a 'fair' level of security for consumer information. Although various forms of relief (such as injunctions and damages) for privacy-related wrongs are available, the FTC has frequently resorted to settling cases by issuing consent decrees. Such decrees generally provide for ongoing monitoring by the FTC, prohibit further violations of the law and subject businesses to substantial financial penalties for consent decree violations. These enforcement actions have been characterised as shaping a common law of privacy that guides companies' privacy practices.[65]

Cybersecurity and data breaches – federal law

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

That said, recent years have brought a flurry of federal action related to cybersecurity. In 2015, Congress enacted the Cybersecurity Information Sharing Act,[66] which seeks to

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).

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

64 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.

65 See, for example, Solove and Harzog, see footnote 4.

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

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.[67] The latter, in particular, has been a noteworthy development: while the NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, there is a general expectation that use of the framework (which is laudably accessible and adaptable) is a best practice consideration for companies holding sensitive consumer or proprietary business data. (The federal government's response to the recent wave of cyberattacks is further detailed in Section II.)

Specific regulatory areas – federal law

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

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

We briefly examine each of these categories,[68] and the agencies with primary enforcement responsibility for them, below.

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

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

Financial information

The GLBA[69] addresses financial data privacy and security by establishing standards pursuant to which financial institutions must safeguard and store their customers' 'non-public personal information' (or 'personally identifiable financial information'). In brief, the GLBA requires financial institutions to notify consumers of their policies and practices regarding the disclosure of personal information; to prohibit the disclosure of such data to unaffiliated third parties, unless consumers have the right to opt-out or other exceptions apply; and to establish safeguards to protect the security of personal information. The GLBA and its implementing regulations further require certain financial institutions (i.e., banks) to notify regulators and data subjects after breaches implicating non-public personal financial information, often referred to as NPI.

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

The SEC has also increasingly used its broad investigative and enforcement powers over public companies that have suffered cybersecurity incidents. In doing so, the SEC has relied on multiple theories, including that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to do so and that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. In 2018, the SEC published interpretive guidance to assist publicly traded companies in disclosing their material cybersecurity risks and incidents to investors.[70] As noted earlier, the SEC has recently proposed updates to that include prescriptive cybersecurity requirements. The SEC has suggested that all public companies adopt cyber disclosure controls and procedures that enable companies to:

a identify cybersecurity risks and incidents;
b assess and analyse their impact on a company's business;
c evaluate the significance associated with such risks and incidents;
d provide for open communications between technical experts and disclosure advisers;
e make timely disclosures regarding such risks and incidents; and
f adopt internal policies to prevent insider trading while the company is investigating a suspected data breach.

69 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)).

70 https://www.sec.gov/news/press-release/2018-22.

Healthcare information

For healthcare privacy, entities within the HHS administer and enforce the HIPAA,[71] as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).[72] Congress enacted HIPAA to create national standards for electronic healthcare transactions, and HHS has promulgated regulations to protect the privacy and security of personal health information. In general, HIPAA and its implementing regulations state that patients generally have to opt in before covered organisations can share the patients' information with other organisations.

HIPAA's healthcare coverage is quite broad. It defines protected health information (PHI) as 'individually identifiable health information . . . transmitted or maintained in electronic media' or in 'any other form or medium'.[73] 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.[74] Notably, HIPAA does not apply to 'de-identified' data.

With respect to organisations, HIPAA places obligations on 'covered entities', which include health plans, healthcare clearing houses and healthcare providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.[75]

Moreover, HIPAA also places obligations on 'business associates,' which are required to enter into agreements, called business associate agreements, to safeguard PHI. A business associate is defined as an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities).[76] Such agreements require business associates to use and disclose PHI only as permitted or required by the agreement or as required by law and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement. The agreements also include numerous other provisions regarding the confidentiality, integrity and availability of electronic PHI.

HIPAA and HITECH not only restrict access to and use of PHI, but also impose stringent information security standards. In particular, HHS administers the HIPAA Breach Notification Rule, which imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI maintained by covered entities and their

71 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified and amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).

72 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, 467 (codified in scattered sections of 42 U.S.C. (2009)).

73 45 C.F.R. Section 160.103.

74 45 C.F.R. Section 160.103.

75 45 C.F.R. Section 164.504(f)(3)(iii).

76 45 C.F.R. Section 164.103.

business associates. The HIPAA Security Rule also requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI.

Information about children

The COPPA applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. The FTC is generally responsible for enforcing COPPA's requirements, which include, among other things, that these website operators post a privacy policy, provide notice about collection to parents, obtain verifiable parental consent before collecting personal information from children and other actions.[77]

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;[78]

b the Computer Fraud and Abuse Act (CFAA) prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks;[79]

c various sections of the Communications Act protect telecommunications information, including what is known as customer proprietary network information, or CPNI;[80]

d the Telephone Consumer Protection Act (TCPA) governs robocalls and texts;[81] 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.[82]

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

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

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

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

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

82 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).

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),[83] as amended by the Fair and Accurate Credit Transactions Act of 2003,[84] imposes requirements on entities that possess or maintain consumer credit reporting information or information generated from consumer credit reports. Consumer reports are 'any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility' for credit, insurance, employment or other similar purposes.

The CFPB, FTC and federal banking regulators (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency) share authority for enforcing FCRA, which mandates accurate and relevant data collection to give consumers the ability to access and correct their credit information and limits the use of consumer reports to permissible purposes such as employment, and extension of credit or insurance.[85]

ii Privacy and data protection legislation and standards – state law

Oversight of privacy is by no means exclusively the province of the federal government. All 50 US states also engage in some form of privacy and data protection regulation, with particular emphasis on data security and breach notifications. Moreover, state attorneys general have become increasingly active with respect to privacy and data protection matters, often drawing on authorities and mandates similar to those of the FTC. Of particular note, as the largest of the US states, the home to Silicon Valley, and a frequent regulatory innovator, California continues to be a bellwether for US privacy and data protection legislation, with businesses across the United States often applying its regulatory approaches, whether or not they are jurisdictionally required to do so.[86] (To this end, Section II discusses the highly significant California Consumer Privacy Act of 2018, which went into effect on 1 January 2020, and amendments to the law enacted California Privacy Rights Act, which go into effect on 1 January 2023.)

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

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

84 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)).

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

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

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.[87] For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls.[88] Likewise, as discussed in Section II, the California Consumer Privacy Act contains security requirements, and a preliminary set of general safeguards went into effect in 2020 in New York, to say nothing of the sector-specific Cybersecurity Regulation issued by New York's DFS. In short, absent pre-emptive federal legislation, we should expect to see states continuing to pass new legislation in this area, creating an increasingly complicated patchwork quilt of state laws for companies to navigate.

General consumer privacy enforcement – 'Little FTCA' analogues

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

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

California is the only state to date that has a privacy-focused agency, the California Privacy Protection Agency. The agency has administrative enforcement powers, rulemaking authority, and is also charged with educating Californians about their privacy rights and providing technical assistance and advise to the California legislature.[89]

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

88 201 Mass. Code Regs. 17.00 (West 2009).

89 Cal. Civ. Code Section 1798.199.40.

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,[90] cyberstalking,[91] data disposal,[92] privacy policies, employer access to employee social media accounts,[93] unsolicited commercial communications[94] and electronic solicitation of children,[95] 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.[96] All financial institutions regulated by DFS – which is a wide range of US financial institutions with a presence in many states – 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.

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

90 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.

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

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

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

94 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.

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

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

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

Second, consider privacy policies. As is typical, California plays an outsized role here, with its California Online Privacy Protection Act (CalOPPA) almost serving – as many of its laws do – as a de facto national standard and thus affecting businesses operating throughout the United States.[97] 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.[98]

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.[99] And there are many other state laws concerning privacy policies, making this an excellent example of the many and diverse regulations that may be relevant to businesses operating across multiple US states.

iii Private litigation

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

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

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

97 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.

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

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

article, 'Privacy'[100] – a taxonomy that was later codified in the American Law Institute's famous and influential Restatement (Second) of Torts.[101] Thus, aggrieved parties can generally bring a civil suit for invasion of privacy (or intrusion upon seclusion), public disclosure of private facts, being cast in a 'false light', and appropriation or infringement of the right of publicity or personal likeness. Importantly, these rights protect not only the potential abuse of information, but generally govern its collection and use. However, not all states recognise all the common law torts. For example, New York does not recognise a legal claim for publication of private facts.

iv Industry self-regulation: company policies and practices

To address concerns about privacy practices in various industries, industry stakeholders have worked with the government, academics and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively developed accountability programmes establish expected practices for the use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. While there are obviously limits to industry self-regulation, these initiatives have led to such salutary developments as the Digital Advertising Alliance's 'About Advertising' icon and a policy on the opt-out for cookies set forth by the Network Advertising Initiative.[102]

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).[103] In addition, voluntary membership or certification in various self-regulatory initiatives also requires posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming deception or detrimental reliance on those policies.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

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

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

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

102 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//.

103 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.

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.[104] 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.[105]

Significantly, however, on 16 July 2020, the Court of Justice for the European Union (CJEU) decided *Data Protection Commissioner v. Facebook Ireland, Max Schrems* (*Schrems II*), which held that the EU–US Privacy Shield (a transfer mechanism used by over 5,000 organisations as a mechanism enabling transfers of personal data from the EU to the US) was invalid because the privacy protections guaranteed in principle to individuals under the Privacy Shield programme were not 'essentially equivalent' to privacy rights guaranteed in principle to such individuals under EU law.[106] The Court also required additional protections to be implemented for another key transfer mechanism, called standard contractual clauses (SCCs), requiring organisations to further evaluate and implement supplementary measures to provide additional privacy protections that afford an individual privacy protections that are 'essentially equivalent' to those guaranteed in principle under EU law. Essentially, the CJEU required companies exporting data to the US to conduct legal self-assessments of whether US national security surveillance law interferes with private companies' ability to comply with their SCC obligations for data transfers to the US.

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

Some of the long-term implications of *Schrems II* remain unclear. Regulators on both sides of the Atlantic have preached calm, and the US government and the EU leadership have also committed to work cooperatively together to address the consequences of the *Schrems II* decision and develop a successor programme to the Privacy Shield. In March 2022, the

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

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

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

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.[107] The US has committed to, among other things, implement safeguards around signals intelligence activities to ensure they are undertaken only where necessary to advance legitimate national security objectives. Additionally, the Framework allows EU individuals to seek redress from a new multi-layer redress mechanism that includes an independent Data Protection Review Court comprised of individuals outside the US who would have authority to adjudicate claims and direct remedial measures. The Framework currently exists at the conceptual level, teams of governmental officials in both the US and EU are working to translate it into binding legal documents that will need to be adopted on both sides.

V COMPANY POLICIES AND PRACTICES

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

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

While not so long ago companies were comfortable with IT and legal departments running the show with respect to privacy issues, they are now increasingly elevating the level of attention these issues receive and involving senior management and the board in oversight and decision making. The examples of this are legion, and the below are just a few examples:

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

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.

107 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/.

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

VI DISCOVERY AND DISCLOSURE

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

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

Government access to information in private hands is governed by numerous statutes, including the following selection of legal authorities: Fourth Amendment of the US Constitution (searches and seizures of persons, houses, papers and effects), ECPA (wiretapping, collection of stored electronic communications and call records),[108] the Right to Financial Privacy Act of 1978 (banking records),[109] Rule 41 of the Federal Rules of Civil Procedure (search warrants), the Foreign Intelligence Surveillance Act of 1978 (national security communications surveillance),[110] the USA PATRIOT Act (national security business records)[111] and so forth. The Presidential Policy Directive (PPD) 28, regarding Signals Intelligence Activities, extended certain legal protections against excessive government surveillance to foreign citizens.[112]

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.

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

109 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)).

110 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)).

111 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.).

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

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

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.[113] 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 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.[114] 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 the new CPPA will likely become a force to be reckoned with soon.

Moreover, compliance with the FTC's guidelines and mandates on privacy issues is not necessarily coterminous with the extent of an entity's privacy obligations under federal law – a number of other agencies, bureaus and commissions are endowed with substantive privacy enforcement authority. Specifically, agencies like the FCC, CFPB, SEC, HHS/OCR play a strong role in investigating and enforcing under their respective statutory authorities over personal data and cybersecurity.

Of course, in the United States, private litigation may be the ultimate 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,

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

114 ibid.

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.[115]

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 OUTLOOK

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

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

Appendix 1

ABOUT THE AUTHORS

ALAN CHARLES RAUL

Sidley Austin LLP

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

SHERI PORATH ROCKWELL

Sidley Austin LLP

Sheri Porath Rockwell is a lawyer in the firm's Los Angeles office and a member of the privacy and cybersecurity practice. She advises clients on a variety of federal and state privacy issues and is CIPP-US certified. Sheri serves as the acting chair of the California Lawyers Association's Privacy Law Section, which she helped found. She earned her JD from the University of Southern California Gould School of Law and her BA, with honours, from the University of California, Berkeley.

SIDLEY AUSTIN LLP

NEO Building
Rue Montoyer 51 Montoyerstraat
B-1000 Brussels
Belgium
Tel: +32 2 504 64 00
jquartilho@sidley.com

39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645 / 2509 7868 / 2509 7637
Fax: +852 2509 3110
yuetming.tham@sidley.com
linh.lieu@sidley.com
lester.fung@sidley.com

ISBN 978-1-80449-116-4