GDR INSIGHT

HANDBOOK 2021

HANDBOOK
2021

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

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

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-266-4

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Privacy

Cybersecurity

Data in practice

PREFACE

Global Data Review is delighted to publish this second edition of the *GDR Insight Handbook*.

The handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of legislation that a ects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of arti cial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell datasets, and the intersection of privacy, data and antitrust. A chapter is dedicated to the use of arti cial intelligence in cross-border forensic investigations.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at November 2020. Although every e ort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing eld of practice, and therefore speci c legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

Global Data Review
London
November 2020

PART 1

Privacy

UNITED STATES: PRIVACY

Miriam H Wugmeister, Julie O'Neill, Nathan D Taylor and Gina M Pickerrell
Morrison & Foerster LLP

The United States has adopted myriad federal and state privacy laws that give protections to individuals regarding the collection, use and disclosure of personal information by both the public and private sectors. These laws are often targeted to address specific instances of abuse or perceived market failures or to protect particularly sensitive information, such as health information, or groups deemed worthy of special protections, such as children. The US approach stands in sharp contrast to the approach found in over 100 other countries around the world that have adopted omnibus privacy laws.

Legal and historical reasons largely account for the differences in privacy regulatory approaches. The US approach to the regulation of the handling of information typically relies on the concept of the 'marketplace of ideas'. Reflected in the First Amendment to the US Constitution, the United States has a long-standing history of rectifying inaccurate and inappropriate speech with more speech rather than less. As a result of these legal traditions, the United States focuses on the misuse of information rather than prohibiting or strictly regulating the collection or use of personal information. In contrast to the privacy regimes in other countries, the focus of a privacy inquiry in the United States is typically whether an individual can be harmed by the misuse of personal information. The premise under US law is not that the mere collection of personal information is improper and must be justified. Rather, under US law, an organisation usually can collect any information it desires if it does so in a way that is not deceptive or unfair to individuals, but it may not misuse that information in ways that may harm an individual.

In addition, information privacy regulation in the United States often differs across states, sectors, information type and data subject. Historically, individuals, government and industry shared a belief that a 'one-size-fits-all' legislative approach would lack the necessary precision to avoid interfering with the benefits resulting from the free flow of information. Similarly, the states, rather than the federal government, often enact their own versions of sectoral laws aimed at protecting certain data types or correcting specific issues of misuse or preventing harm in specific situations.

Federal law and regulation

The United States has a federal system in which laws are enacted at the levels of national government, state government and local government (eg, cities and counties). In general, privacy and information security laws are enacted at the state and national levels of government.

The federal government, for example, has enacted detailed privacy and information security rules that apply to financial institutions regarding the use of information relating to individual consumers, even though the states are also authorised to regulate these same entities (with certain exceptions) with respect to the same information. As a result, an organisation can be subject to the laws of the state in which the organisation is located, as well as subject to the laws of other states in which the organisation conducts activity, and also subject to all of the federal laws regulating those activities. Moreover, state laws continue to be enforceable even if a national law regulates the same conduct, unless certain conflicts between the laws cannot be reconciled under certain principles of constitutional law. In that case, the national law prevails over, or pre-empts, the state or local law.

Sectoral regulations

Regulation in the United States generally focuses on information viewed as particularly sensitive on a sectoral basis, such as financial information, health information, consumer report information, information collected online from children and information that can be used for identification theft or fraud.[1]

Financial information

Title V of the Gramm–Leach–Bliley Act (1999) (GLBA) imposes privacy obligations on financial institutions with respect to the privacy of non-public personal information about consumers, including limiting disclosures of information to non-affiliated third parties.[2] The GLBA also directs various financial regulators to prescribe information security standards for financial institutions with respect to the security of customer records and information.[3]

The GLBA is implemented functionally by certain financial regulators that have oversight authority over different types of financial institutions. In general, the Consumer Financial Protection Bureau (CFPB) has primary authority to implement the GLBA with respect to privacy, although this authority does not extend to certain types of financial institutions, such as broker-dealers and insurance companies. With respect to security, various financial regulators implement and enforce information security standards, including the federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC).

1 It is interesting to note that omnibus privacy laws outside the United States often do not treat financial information or information about children as sensitive information.

2 The Gramm–Leach–Bliley Act, Pub L 106-102, 113 Stat 1338 (1999); see 15 USC sections 6801–6809, 6821–6827 (2019).

3 See 15 USC section 6804 (authorising rulemaking for the Safeguards and Financial Privacy Rules).

Financial Privacy Rule

The CFPB has issued the Financial Privacy Rule that governs the privacy practices of most financial institutions.[4]

In general, the Financial Privacy Rule requires financial institutions to provide 'consumers' with privacy notices and prescribes requirements relating to the content, timing and methods of delivering those notices. For example, the Financial Privacy Rule requires that a financial institution provide its 'consumers' and 'customers' with its privacy policy in various instances (eg, an annual notice to customers).[5] In addition, the Financial Privacy Rule prohibits a financial institution from disclosing 'nonpublic personal information' about a 'consumer' to a non-affiliated third party unless: (1) the institution has provided the consumer with notice and an opportunity to opt out of the disclosure of his or her information and the consumer has not opted out; or (2) an exception applies that permits the financial institution to disclose the information.[6] In addition, the Financial Privacy Rule places limitations on the ability of any party that receives non-public personal information from a financial institution to re-disclose and reuse the information.[7]

Safeguards Rule

The GLBA also requires various financial regulators to establish standards regarding the administrative, technical and physical safeguards that financial institutions must implement to protect customer information.[8] Each agency is charged with issuing its own security rule that imposes specific security requirements on institutions subject to its jurisdiction. These rules are similar in many respects.

For example, the rule issued by FTC (the Safeguards Rule) for financial institutions that are not subject to the authority of the other financial regulators requires that covered financial institutions 'develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to [the institution's] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue'.[9] As part of this information security programme, the Safeguards Rule requires that financial institutions, among other things, conduct a risk assessment of the reasonably foreseeable internal and external threats to the security, confidentiality and integrity of customer information to inform the development and maintenance of its information security programme, designate employees to coordinate

4 See 12 CFR pt 1016. Certain other financial regulators have issued rules to implement the GLBA's privacy provisions for certain financial institutions. See, eg, 17 CFR pt 248. Nonetheless, the various GLBA privacy rules are substantively the same.

5 See 12 CFR sections 1016.4, 1016.5.

6 See 12 CFR section 1016.10.

7 12 CFR section 1016.11.

8 15 USC section 6801.

9 FTC Standards for Safeguarding Customer Information, 16 CFR section 314.3 (2019).

the programme, train employees, contractually require service providers to safeguard personally identifiable information about customers, test and monitor the programme's effectiveness, and update the programme in response to testing results and changed circumstances.[10]

Health information

The Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA),[11] as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) under the American Recovery and Reinvestment Act of 2009,[12] regulates the use and disclosure of certain types of 'individually identifiable health information' (ie, protected health information (PHI)).[13] Healthcare providers, health plans and healthcare clearing houses (covered entities), as well as their business associates, may use or disclose PHI only for treatment, payment or healthcare operations, unless a particular exception applies or if a patient provides written authorisation. Under HIPAA, patients have a right to access and amend their PHI held by a covered entity and to receive an accounting of past disclosures and annual privacy notices.

HIPAA requires that covered entities and their business associates implement and maintain a broad range of administrative, technical and physical safeguards to protect the confidentiality, availability and integrity of electronic PHI (ePHI).[14] Covered entities and business associates are also required to carry out a periodic risk analysis of the threats and vulnerabilities facing their ePHI.[15]

Business associates must report actual and potential breaches involving PHI to the covered entity.[16] The covered entity must determine whether a notifiable breach occurred, which involves assessing the risk that the privacy or security of the PHI was compromised.[17] Covered entities must report breaches to impacted individuals, the US Department of Health and Human Services Office for Civil Rights, and in certain cases, the media.[18]

10 16 CFR section 314.4.

11 Health Insurance Portability and Accountability Act of 1996, Pub L 104–191, 110 Stat 1936 (1996) (amended 2009).

12 American Recovery and Reinvestment Act of 2009, Pub L 111–5, 123 Stat 226 (codified as amended at 42 USC sections 300jj et seq).

13 42 USC section 1320d (defining 'individually identifiable health information'); HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information, 45 CFR sections 160, 164 (using the term 'protected health information').

14 HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information, 67 Fed Reg 53,182 (14 August 2002) (codified at 14 CFR pt 160, 162, 164); HIPAA Security Rule: Health Insurance Reform: Security Standards, 68 Fed Reg 8,334 (20 February 2003) (codified at 14 CFR pt 160, 162, 164).

15 45 CFR section 164.308(a)(1)(ii)(A).

16 42 USC section 17932(b).

17 42 USC section 17932.

18 42 USC section 17932(e).

Genetic information

The Genetic Information Nondiscrimination Act (2008) (GINA)[19] prohibits both employers and group health plans from discriminating on the basis of genetic information relating to employees (including family medical histories). GINA also places significant limits on the ability of employers and group health plans to collect genetic information or use any such information once collected. GINA adopts a broad definition of 'genetic information' that encompasses not only genetic test results relating to, but also any manifestation of disease or disorder in, an individual and his or her family members (the individual's blood relatives to the fourth degree of relation and any person who is a dependent of that individual as a result of marriage, birth or adoption).[20]

Consumer report information

The Fair Credit Reporting Act (FCRA)[21] regulates the use and disclosure of consumer reports information compiled and disclosed by consumer reporting agencies. For example, the FCRA regulates the type of information that consumer reporting agencies can include in consumer reports and for how long, as well as limits when and for what purposes consumer reporting agencies may provide consumer reports to third parties. The FCRA also requires that prospective users of consumer reports, such as lenders, insurers, employers and landlords, must have a statutorily permitted purpose before obtaining a consumer report. In addition, the FCRA imposes obligations on companies that furnish information about consumers to consumer reporting agencies to be included in consumer reports focused on ensuring the accuracy of information that ultimately will be included in consumer reports.

Information collected online from children

The Children's Online Privacy Protection Act of 1998[22] and the FTC's rule promulgated pursuant to the Act[23] (together, COPPA) apply to operators of websites or other online services that are directed to children under the age of 13 or that knowingly collect personal information from children under the age of 13.[24] Such operators must provide a privacy notice that explains their practices regarding children's personal information.[25] The collection of personal information from a child, in most instances, requires the prior opt-in consent of the child's parent or legal guardian.[26] COPPA imposes additional use, security, access, deletion

19 Genetic Information Nondiscrimination Act, Pub L No 110-233, 122 Stat 881.

20 42 USC section 2000ff.

21 Fair Credit Reporting Act, 15 USC section 1681 et seq.

22 Children's Online Privacy Protection Act of 1998, Pub L No. 105-277, 15 USC sections 6501–6506.

23 16 CFR Part 312.

24 15 USC section 6501.

25 15 USC section 6502.

26 15 USC section 6502.

and other obligations on covered operators. Interestingly, COPPA also applies to foreign websites that collect personal information from children in the United States.[27] Violation of the COPPA rule can give rise to civil penalties of up to US$43,280 per violation.[28]

Regulatory focus on electronic information

US regulation on information misuse focuses on information stored electronically because of a perception that such information can be misused more easily and exploited on a larger scale, causing greater problems. Other countries with omnibus laws tend not to distinguish among the forms in which information is maintained.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) imposes criminal and civil liability on any individual who: (1) accesses information without authorisation or exceeds any such authorisation; (2) obtains information from any protected computer, a broad term encompassing any computer 'used in or affecting interstate or foreign commerce'.[29] The CFAA requires typical plaintiffs to show losses of at least US$5,000 in any one-year period.[30] This can be an aggregate figure, including lost revenue associated with a service interruption and the company's cost of investigating the violation.[31]

US federal courts have developed varying approaches to analysing authorised access in the context of terms of use violations and third-party access (ie, password-sharing, in which a user shares his or her log-in credentials with a third party who then accesses the network using those credentials). In *Facebook, Inc v Power Ventures, Inc*, the Ninth Circuit declared mere 'violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA'.[32] However, when a defendant's 'permission to access a computer . . . has been revoked explicitly . . . technological gamesmanship or the enlisting of a third party to aid in

27 15 USC section 6501.

28 16 CFR 312 section 312.10.

29 18 USC section 1030(a)(2)–(e)(2); see also *United States v Nosal*, 676 F.3d 854, 859 (9th Cir 2012) (interpreting a 'protected computer' to include any 'computer connected to the Internet'); *United States v Trotter*, 478 F.3d 918, 921 (8th Cir 2007) (finding that connection to the internet made a computer 'protected' under the CFAA).

30 18 USC section 1030(c).

31 18 USC section 1030(e)(11) (defining 'loss' to include 'any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service').

32 *Facebook, Inc v Power Ventures, Inc*, 844 F.3d 1058, 1067 (9th Cir 2016). The case involved a social media aggregator, with its customers' permission, using their Facebook accounts to send promotional messages on Facebook. The court ruled that the aggregator's actions did not violate the CFAA until Facebook sent a cease-and-desist letter explicitly revoking any arguable permission, and the aggregator continued accessing Facebook anyway, switching Internet Protocol (IP) addresses to evade the IP block Facebook instituted. id. at 1063, 1069.

access will not excuse liability.'[33] Other courts have found that violating terms of use related to log-ins can run afoul of the CFAA if the defendant knew about the term in question. For instance, where a licensing agreement prohibited sharing log-in credentials, the Eleventh Circuit found third-party access by a defendant who knew about the prohibition breached the CFAA.[34] In contrast, the Eastern District of Virginia found no CFAA violation when a third party flouted the terms of use by downloading screenshots. Because users did not need to accept the user agreement every time they logged in, there was no evidence that the third party, logging in with the user's shared credentials, knew about the terms of use.[35]

Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986[36] (ECPA) prohibits unauthorised interception or disclosure of wire, oral and electronic communications.[37] However, the ECPA's prohibitions on interception do not apply if a company: intercepted the communication in the ordinary course of business; or one of the parties consented to the interception.[38] Under certain conditions, they may permit service providers to intercept customer communications.[39]

Regulatory focus on deception and unfairness

US laws also protect against unfair and deceptive practices. The FTC has broad regulatory authority over most companies. Relying on its powers to regulate unfair and deceptive trade practices, the FTC prosecutes businesses that, for example, fail to comply with their public statements regarding their privacy protections and practices, or fail to provide reasonable security protections for sensitive personal information. Thus under US law, one of the key ways in which companies are held accountable is if they make a public promise that they do not in fact keep or if they fail to disclose an information practice that is material to consumers.

Federal Trade Commission Act

Section 5 of the Federal Trade Commission Act (FTC Act) prohibits 'unfair or deceptive acts or practices in or affecting commerce' and grants the FTC the authority to prosecute such unlawful activity against all companies except those listed as exceptions in section 5 (such

33 id. at 1067.

34 *State Analysis, Inc v Am Fin Servs Assoc*, 621 F Supp 2d 309, 313 (ED Va 2009).

35 *EarthCam, Inc v OxBlue Corp*, 703 F App'x 803, 810 (11th Cir 2017).

36 18 USC sections 2510–2523.

37 18 USC section 2511.

38 18 USC sections 2511(c)–(d).

39 See *United States v Ross*, 713 F.2d 389, 392 (8th Cir 1983) (finding that random monitoring of a telephone conversation by repairman fell within the 18 USC section 2511(2)(a)(i) service provider business purpose exception).

as banks and telecommunication providers).[40] The FTC has relied heavily on this section, bringing actions against companies allegedly engaged in 'deceptive' or 'unfair' practices. For example, a company's failure to abide by its own privacy policy may be deemed a deceptive practice. In addition, even if a company follows its privacy policy, its practice may be deemed 'unfair' if the FTC determines that the company's actions cause substantial harm to a consumer that he or she could not reasonably have avoided, with no countervailing benefits to consumers or competition.[41] The FTC can impose injunctive relief for violations of section 5, which could include equitable monetary relief (eg, disgorgement of ill-gotten gains or consumer redress), by bringing an action in federal district court. The FTC may also seek voluntary compliance for alleged violations by entering into a consent order with a company that will impose FTC oversight and be in effect for 20 years. The FTC may enter into consent orders of its own accord, but penalties for violating such orders are assessed by a federal district court in a suit brought to enforce the FTC's order.

Deceptive business practices: deviations from stated privacy policies

The FTC's interpretation of 'deceptive' practices includes noncompliance with, and material omissions in, stated privacy policies as well as failure to obtain affected individuals' consent when materially changing those policies and seeking to apply the change retroactively, as demonstrated by its first-of-its-kind 2004 enforcement action against Gateway Learning Corporation (Gateway).[42] The Gateway website privacy policy had stated that the company would 'not sell, rent, or loan any personally identifiable information regarding our consumers with any third party . . . [without the] customer's explicit consent'.[43] Gateway indicated that it would inform consumers and provide the opportunity to 'opt out' if the policy changed.[44] According to the FTC, however, Gateway rented consumers' personal information to target marketers for use in mailings and telemarketing calls, without such consumers' consent. The FTC charged Gateway with violating section 5 of the FTC Act because its practice of sharing consumers' personal information in this way violated its privacy policy and was thus deceptive.

The FTC has also taken action against companies for falsely claiming compliance with specific privacy frameworks and using deceptive tactics to collect information. For instance, in 2019, background screening company SecurTest, Inc reached a settlement with the FTC over allegations that it falsely represented itself as a certified participant in the Swiss–US Privacy

40 15 USC section 45 (2019). Section (a)(2) excludes banks, savings and loan institutions, federal credit unions, common carriers subject to the acts to regulate commerce, certain domestic and foreign air carriers, and most persons, partnerships or corporations subject to the Packers and Stockyards Act of 1921. id.

41 15 USC section 45(n).

42 See 'Gateway Learning Settles FTC Privacy Charges: Company Rented Customer Information it Pledged to Keep Private', Fed Trade Comm'n (7 July 2004), https://www.ftc.gov/news-events/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges.

43 id.

44 id.

Shield and EU–US Privacy Shield agreements.[45] The FTC issued warning letters to 15 companies making similar claims, instructing them to remove these claims from their websites and privacy policies.[46] The FTC has also entered settlement agreements with companies over allegedly deceptive harvesting tactics. For example, the FTC alleged that information analytics company Cambridge Analytica falsely claimed that it did not collect Facebook users' personal information. Similarly, the FTC alleged that digital advertising company Turn Inc had deceived consumers about the extent of online tracking in which it engaged.[47]

Unfair business practices: inadequate information security measures and surreptitious monitoring

Under the 'unfairness' prong of section 5, the FTC has taken action against companies for, for example, allegedly failing to adequately safeguard consumer information and monitoring consumers without their consent. FTC guidance collates lessons learned from its enforcement actions on how to design products and services in a privacy-protective way.[48] This guidance emphasises that businesses should:

- collect only the personal information they need;
- retain personal information only as long as they have a legitimate business need for it;
- restrict access to sensitive personal information and limit administrative access, which may allow a user to make system-wide changes;
- require strong passwords and authentication procedures;
- secure sensitive personal information during transmission and storage;
- securely dispose of sensitive personal information;
- segment and monitor networks;
- verify and test privacy and security features in new products; and
- contractually require service providers to implement appropriate security measures and verify their compliance.[49]

45 'FTC Takes Action against Companies Falsely Claiming Compliance with the EU-US Privacy Shield, Other International Privacy Agreements', Fed Trade Comm'n (14 June 2019), https://www.ftc.gov/news-events/press-releases/2019/06/ftc-takes-action-against-companies-falsely-claiming-compliance-eu.

46 id.

47 'FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer: FTC alleges they deceived Facebook users about data collection', Fed Trade Comm'n (24 July 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer; 'FTC Approves Final Consent Order with Online Company Charged with Deceptively Tracking Consumers Online and Through Mobile Devices', Fed Trade Comm'n (21 April 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-consent-order-online-company-charged.

48 See 'Start with Security: A Guide for Business', Fed Trade Comm'n (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; see also 'Protecting Personal Information: A Guide for Business', Fed Trade Comm'n (October 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

49 See 'Start with Security: A Guide for Business', Fed Trade Comm'n (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

This guidance applies to both electronic information (proper encryption of sensitive information, securely wiping hard drives, etc) and tangible items (shredding prescriptions, not leaving laptops containing sensitive files in cars, etc).[50]

The FTC has considered inadequate information security a violation of section 5's prohibition against 'unfair and deceptive' practices. For instance, after the 2017 Equifax breach affecting 147 million people, the FTC brought an enforcement action against the consumer credit reporting agency for its alleged failure 'to take reasonable steps to secure its network'.[51] While at other times the FTC has gone so far as to take actions against companies for inadequate security measures even in the absence of express promises of protection to consumers,[52] Equifax did have a privacy policy at the time of the breach, claiming it protected consumer information with 'reasonable physical, technical and procedural safeguards'. However, the FTC alleged that the company 'failed to implement basic security measures'. Specifically, the FTC criticised Equifax for storing sensitive information like passwords and Social Security numbers in plain text and failing to patch security vulnerabilities, segment its network so hackers who accessed one part could not access the rest, and install robust programmes to detect intrusions.[53]

FTC information security settlement agreements under section 5 often require companies to establish, implement and maintain comprehensive security programmes that include key elements required under the GLBA's Safeguards Rule.[54] For instance, in June 2019, the FTC entered a settlement agreement with a provider of auto dealer software that, the FTC alleged, failed to implement reasonable security measures for consumer personal information and thereby engaged in 'unfair and deceptive' practices, as well as violations of the GLBA's Safeguards Rule. The settlement, which will remain in effect for 20 years, obliged the software

50 See *Fandango, LLC*, No. 132-3089 (FTC, 19 August 2014) (despite using SSL encryption, SSL certificate validation in mobile app was allegedly turned off); *Goal Financial, LLC*, No. 072-3013 (FTC, 15 April 2008) (extra hard drives containing customer information in clear text were allegedly sold); *Accretive, Inc*, No. 122-3077 (FTC, 24 February 2014) (allegedly left laptop in car's locked passenger compartment resulting in theft); *Rite Aid Corp*, No. 72-3121 (FTC, 22 November 2010) (prescriptions and other sensitive papers were allegedly tossed in dumpsters).

51 'Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach', Fed Trade Comm'n (22 July 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

52 See 'BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards', Fed Trade Comm'n (16 June 2005), https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges (BJ's did not have a declared privacy or security policy, but the FTC still alleged BJ's engaged in unfair business practices by failing to take appropriate security measures to protect its customers' information).

53 'Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach', Fed Trade Comm'n (22 July 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

54 See 'Financial information', above.

provider to: implement a comprehensive information security programme; obtain security programme assessments from third parties approved by the FTC; and file those assessments with, and certify compliance to, the FTC biennially for 20 years.[55]

The FTC has also alleged that companies have engaged in unfair practices through surreptitious monitoring of consumers. For instance, in 2013, the FTC took action against DesignerWare, LLC, which provided software to rent-to-own companies to assist with recovering stolen computers.[56] According to the FTC, DesignerWare installed monitoring and geolocation tracking software on rented computers then used that software to take screenshots of sensitive information, log keystrokes and take webcam photographs – all without notifying or obtaining the consent of users.[57] In the consent order, DesignerWare and its affiliates agreed to: stop using monitoring software on consumers or providing third parties with such software on computers rented to consumers; and limit its use of geolocation tracking software to users who expressly consent to the technology before renting the computers and re-notify users prior to each use.[58]

State laws

Many states in the United States have also passed privacy laws. These states often have constitutions enshrining broad privacy rights, in addition to specific laws that typically focus on regulating sensitive information in certain sectors, information misuse and misrepresentations about how information may be used or protected.

State constitutions

Several states guarantee the right to privacy in their state constitutions. For example, California's state constitution includes an explicit right to privacy[59] and the New Jersey Supreme Court has recognised that '[w]ith its declaration of the right to life, liberty and the pursuit of happiness, Article I, Section 1 of the New Jersey Constitution encompasses the right to privacy.'[60]

55 See also *Fed. Trade Comm'n v Equifax Inc*, No. 1:19-cv-03297-TWT (ND Ga, 22 July 2019) (additionally requiring Equifax to submit reports detailing specific administrative, technical and physical safeguards it implements to the FTC biennially for 20 years); *BJ's Wholesale Club, Inc*, No. 042-3160 (FTC, 16 June 2005) (articulating similar requirements).

56 'FTC Approves Final Order Settling Charges Against Software and Rent-to-Own Companies Accused of Computer Spying', Fed Trade Comm'n (15 April 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-and.

57 id.

58 *DesignerWare, LLC*, Docket No. C-4390 (FTC, 13 April 2013).

59 Cal Const article 1, section 1.

60 *Doe v Poritz*, 142 NJ 1, 89, 662 A.2d 367, 412 (1995).

Broad laws and regulations

Some states have implemented broad privacy statutes, including California and Nevada. After California passed its landmark privacy bill in 2018, 23 other states introduced similar bills, though some have narrower scopes.[61]

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) and its implementing regulations[62] establish a set of protections for California residents.[63] The CCPA, which became enforceable by the California Attorney General on 1 July 2020, imposes obligations on for-profit businesses that pass a size threshold by having annual gross revenues greater than US$25 million, handle personal information of over 50,000 California residents or devices per year, or garner at least half of their annual revenues from selling the personal information of California residents.[64] The CCPA also defines personal information broadly, as 'information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'.[65] At the least, this includes information like names, contact information, IP addresses, search history, browsing history, and location information; however, it excludes de-identified, aggregated information or certain information lawfully collected from government records.[66]

The CCPA establishes five key rights for California residents[67] whose information has been collected by a covered business:

- the right to know what personal information has been collected about the individual and the right to access '[t]he specific pieces of personal information' collected in the past 12 months;
- the right to have the business delete the personal information, subject to limitations including free speech, compliance with subpoenas, research in the public interest and internal uses a consumer would reasonably expect;

61 See, eg, Nev. Rev. Stat. § 603A.300 (2019) (requires an operator to establish a designated request address through which a consumer may direct the operator not to sell his or her covered information); Me. Rev. Stat. Ann. tit. 35A, § 9301 (2019) (applying to internet service providers only); An Act concerning commercial Internet websites, consumers, and personally identifiable information, S. 1257, 219th Leg, 1st Reg. Sess. (NJ 2020); The New York Privacy Act, A. 8526, 2019-2020 Reg. Sess. (NY 2020); The Consumer Data Privacy Act, H.B. 1049, 2019-2020 Reg. Sess. (Pa. 2019); The Rhode Island Transparency and Privacy Act, H.B. 7778, 2020 Reg. Sess. (RI 2020).

62 California Consumer Privacy Act Regulations, 11 CCR § 999.300 et seq.

63 California Consumer Privacy Act of 2018, SB-1121, Cal Civ Code section 1798.100 et seq.

64 Cal Civ Code section 1798.140(c).

65 Cal Civ Code section 1798.140(o).

66 id.

67 Under the CCPA, California residents include those outside California for a temporary or transitory purpose. See Cal Civ Code section 1798.140(g) (defining California resident by reference to Cal Code Regs Title 18, section 17014 as of 1 September 2017); Cal Code Regs Title 18, section 17014 (2017) (defining the term 'resident' as those living in California 'for other than a temporary or transitory purpose', including those temporarily outside California).

- the right to opt out of the sale of personal information to third parties (with extra protections for children's information);
- the right to be free from price or service discrimination despite exercising these rights; and
- the right to sue for at least US$100 per consumer and per incident, if the business's failure to maintain reasonable security results in a breach of personal information, as 'personal information' is defined by California's Customer Records Law[68] (and not as the term is defined more broadly by the CCPA) (although the consumer must first give the business targeted written notice and an opportunity to cure the violation).

The CCPA also empowers the California Attorney General to bring enforcement actions against covered businesses, with civil penalties of US$2,500 for unintentional violations and US$7,500 for intentional violations.[69] A business is not deemed in violation of the CCPA if it cures any alleged violation within 30 days after being notified of alleged non-compliance.

A business may need to take a number of steps to comply with the CCPA, such as:

- updating or creating a privacy disclosure on its website. A business must provide detailed information on its website, including what personal information it collects about consumers and the purposes for which it will use that information, how a consumer may submit requests concerning his or her personal information, and the categories of consumer personal information that were actually collected and sold or disclosed for business purposes in the preceding 12 months;[70]
- posting a clear and conspicuous 'Do Not Sell My Personal Information' link on its website, if it 'sells' personal information;[71]
- establishing a process for responding to verifiable consumer requests within a 45-day response window;[72] and
- ensuring that appropriate agreements with service provider agreements are in place.

Nevada

In May 2019, Nevada expanded its online privacy statute to include a 'do not sell' component.[73] Under its pre-existing 2017 online privacy statute, Nevada already required online services and websites collecting specific types of personal information from Nevada consumers (first and last name, contact information, personally identifiable information, etc.) to disclose what types of covered information it collected, with what kind of third parties it shared covered information, and how consumers could see and request updates to covered information about themselves.[74]

68 Cal. Civ. Code § 1798.81.5(d)(1)(A).
69 Cal. Civ. Code § 1798.155(b).
70 Cal Civ Code sections 1798.100(b) and 1798.130(a)(5).
71 Cal Civ Code sections 1798.120 and 1798.135(a).
72 Cal Civ Code section 1798.130(a)(2).
73 SB 220 (Nev 2019), Nev Rev Stat section 603A.100 et seq.
74 See Nev Rev Stat sections 603A.010–603A.920 (2017).

An amendment to the Nevada law that took effect in October 2019 added a requirement that covered businesses respond to requests from consumers not to sell covered personal information.[75]

The Nevada law is more narrowly tailored than the CCPA as 'sale' is limited to an exchange of personal information for money rather than including non-monetary consideration, and the definition of consumer does not include all residents of Nevada.[76]

Sector-specific laws and regulations

States also have implemented statutes and regulations protecting sensitive information on a sectoral basis, along similar lines as the federal government. In many cases, these state laws provide more robust and detailed regulation than corresponding federal laws.

Financial information

The privacy provisions of the GLBA do not pre-empt state laws that offer stronger consumer protections,[77] and a number of states have enacted their own financial privacy statutes. For example, the California Financial Information Privacy Act prohibits financial institutions from disclosing non-public personal information relating to consumers to nonaffiliated third parties without obtaining affirmative 'opt-in' consent from the consumers, rather than the 'opt-out' approval permitted by the GLBA.[78] Similarly, Vermont has adopted a financial privacy regulation that bars a financial institution from disclosing non-public personal information about a customer to any non-affiliated third party unless the customer has been provided with a notice and an opportunity to authorise, or 'opt in' to, the disclosure, and the consumer opts in.[79]

Health information

A number of states have medical privacy laws. These laws are not pre-empted by HIPAA to the extent that they provide greater protections. California's Confidentiality of Medical Information Act,[80] for example, applies to '[a]ny business organized for the primary purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of healthcare', a broader scope than HIPAA.[81] It also requires 'each employer who receives medical information [to] establish appropriate procedures to ensure the confidentiality and protection from unauthorized disclosure and use of that information'.[82]

75 id.
76 id.
77 See 15 USC section 6807.
78 California Financial Information Privacy Act, Cal Fin Code section 4051.5(b)(3).
79 Vt Stat Ann Title 8, sections 10201–10205. The Vermont Department of Banking, Insurance, Securities, and Healthcare Administration promulgated a privacy rule that implements the Vermont law. 21-101-016 Vt Code R sections 1–26.
80 Cal Civ Code section 56.05 et seq.
81 Cal Civ Code section 56.06.
82 Cal Civ Code section 56.20.

The Texas Medical Privacy Act, similarly, applies to a broader range of entities than HIPAA,[83] does not allow a patient's health information to be used for marketing without the patient's consent, and prohibits re-identification of de-identified information.[84]

Certain states have privacy laws relating to HIV/AIDS status,[85] mental health records[86] and substance abuse records.[87] In certain states, recipients of such sensitive information must receive a written notice explaining how unauthorised re-disclosure is restricted by state law.[88] Some states also limit genetic testing of employees and the disclosure of genetic test results and require 'each employer who receives medical information [to] establish appropriate procedures to ensure the confidentiality and protection from unauthorised disclosure and use of that information'.[89]

Finally, a number of state breach laws address the unauthorised access or acquisition of treatment, diagnosis or other medical or health insurance information.[90] Some of these breach laws also state that if HIPAA applies to a business, or if the business complies with HIPAA, then that state's breach notice laws will not apply.[91] In California, healthcare providers must report breaches of medical information to impacted patients and the California Department of Public Health within 15 days of discovery (compared to 60 days under HIPAA).[92]

Biometric information

Illinois, Texas and Washington have enacted laws regulating the collection, disclosure and other handling of biometric information specifically, such as the Illinois' Biometric Information Privacy Act (BIPA).[93]

The BIPA covers fingerprints, voiceprints and facial geometry, as well as retina, iris and hand scans, but not writing samples, written signatures, photographs, demographic data, tattoo descriptions, physical descriptions, or human biological samples used for scientific testing,

83 These entities include those who assemble, collect, analyse, use, evaluate, store, or transmit protected health information. The statute's examples include governmental units, information or computer management entities, schools, health researchers, and those who maintain Internet sites. Tex Health & Safety Code section 181.001(b)(2)(A).

84 Tex Health & Safety Code sections 181.001–181.207.

85 See Ariz Rev Stat section 36-664(F); Cal Health & Safety Code section 120975 et seq; 410 Ill Comp Stat 305/1.

86 See Md Code, Health–General section 4-307; 740 Ill Comp Stat 110/5.

87 See 71 Pa Cons Stat section 1690.108(c).

88 See, eg, Ohio Rev Code section 37101.243(E); Conn Gen Stat section 19a-585(a).

89 Cal Civ Code section 56.17.

90 See Ariz Rev Stat sections 18-551–18-552; Haw Rev Stat sections 487N-1–487N-3.

91 See 815 Ill Comp Stat 530/50 (requiring notice to Illinois Attorney General within five days of any HIPAA breach notice made to US Dept of Health and Human Services); 10 Laws of PR sections 4051–4055 (no HIPAA compliance or applicability exception is included in the law, which does address the breach of identifiable health information).

92 Cal Health & Safety Code, section 1280.15.

93 See Biometric Information Privacy Act of 2008, 740 Ill Comp Stat 14/1 et seq; Tex Bus & Comm Code section 503.001; Wash Rev section 19.375; see also Biometrics Laws and Private Policies, PrivacyPolicies.com (last updated 27 December 2018), https://www.privacypolicies.com/blog/privacy-policy-biometrics-laws/#laws-regulating-biometrics-use.

donated organs or tissues, or information used for healthcare treatment.[94] The statute prohibits private entities collecting and disclosing biometric information without informed consent, bars them from selling or profiting from biometrics, and obliges them to securely store, transmit and ultimately destroy biometrics no later than three years after the last interaction with the associated individual or after the purpose of collection has terminated, whichever occurs sooner.[95]

Unlike Texas and Washington biometric privacy laws, the BIPA also creates a private right of action with minimum damages of US$1,000 per negligent violation and US$5,000 for intentional or reckless damages.[96] In February 2019, the Illinois Supreme Court decided that plaintiffs need not show 'some actual injury or harm' to sue for violation of their rights under the BIPA, rejecting any characterisation of an individual's right to 'biometric privacy vanish[ing] into thin area' as a 'mere "technicality"'.[97] A month later in March 2019, the Appellate Court of Illinois upheld and clarified the state Supreme Court's decision holding that 'a plaintiff who proves a violation of the Biometric Information Privacy Act may recover liquidated damages without proof of actual damages beyond the violation of the Act.'[98] Similarly, in September 2019, the US District Court for the Northern District of Illinois, Eastern Division, denied in part a defendant's motion to dismiss a plaintiff's and a proposed class's BIPA claim of harm arising from a violation of privacy rights in biometric data.[99]

The National Biometric Information Privacy Act was introduced in the US Senate in August 2020 and is substantially similar to the BIPA, requiring notice and written consent before collection, use, retention, disclosure, or sale of individuals' biometric data and providing a private right of action for consumers to bring class action lawsuits for alleged violations.[100] Further, the Act would provide that consumers have standing to pursue their claims even if their injury is merely a technical violation without real-world harm.[101] The Act would not pre-empt any state law that imposes more stringent limitations.[102] It is unknown whether the Act will become law, but it illuminates the trend towards more defined protections for consumers and their biometric data.

94 See 740 Ill Comp Stat 14/10.

95 id. 14/15.

96 id. 14/20.

97 *Rosenbach v Six Flags Entertainment Corp*, 2019 IL 123186, paragraph 34 (quoting *Patel v Facebook Inc*, 290 F Supp 3d 948, 953 (ND Cal 2018)) (finding that a child and his mother need not allege actual harm to sue Six Flags for scanning his thumbprint to access his season pass without obtaining written consent or informing them of the purpose and length of retention).

98 *Rottner v. Palm Beach Tan, Inc.*, 2019 IL App (1st) 180691-U (1st Dist. 2019) (post-*Rosenbach* case finding that plaintiff could maintain a BIPA action when the only allegations were that defendant never informed plaintiff of its data retention policy and plaintiff never signed a release permitting collection).

99 *Rogers v. CSW Intermodal Terminals, Inc.*, 409 F. Supp. 3d 612 (N.D. Ill. 2019) (concluding plaintiff had standing when biometric data was disseminated to third-party vendors without providing notice to and obtaining plaintiff's informed written consent).

100 National Biometric Information Privacy Act of 2020, S.4400, 116th Congress (2019-2020).

101 id.

102 id.

Consumer report information

The FCRA is not the exclusive source of restrictions on the use of information gathered by consumer reporting agencies. State laws also apply and in some cases may be more restrictive than the FCRA. California, for example, has two applicable statutes. California's Investigative Consumer Reporting Agencies Act (ICRAA) limits the circumstances in which a person can initiate an investigative consumer report, requires a consumer to be provided with an option to receive a copy of the report, constrains the information that can be included in the report, and makes investigative consumer reporting agencies liable for breaches.[103] In addition, the Consumer Credit Reporting Agencies Act (CCRAA) includes provisions for consumers to request security alerts be placed in their credit reports to notify the report recipient that the consumer may have been the victim of identity fraud. [104]

Protection of information

State legislatures also have passed laws requiring that personal information be protected. These laws often cover a greater number of areas and contain broader requirements than comparable federal laws against misuse.

Procedures and practices

The California Security Safeguard Act[105] applies to any company that owns or licenses unencrypted 'personal information' about California residents. The Security Safeguard Act requires these companies to implement and maintain 'reasonable security procedures and practices' to protect such information. Texas and Rhode Island[106] followed with similar laws. These laws apply to businesses that maintain unencrypted personal information about their employees.

Nevada enacted an information security law that mandates encryption for the transmission of personal information.[107] Specifically, the Nevada encryption statute prohibits businesses in Nevada from transferring 'any personal information through an electronic transmission', except via facsimile, 'unless the business uses encryption to ensure the security of electronic transmission'.[108] The 'personal information' covered by the Nevada encryption law is the same information subject to that state's security breach notification law:

> *a natural person's first name or first initial and last name in combination with [his or her] . . . . (1) Social Security number[;] (2) driver's license number or identification card number[; or] (3) account number, credit card number or debit card number, in combination with any required security code, access code or password.*[109]

103 Cal Civ Code sections 1786–1786.60.
104 Cal Civ Code sections 1785.1–1785.36.
105 Cal Civ Code section 1798.81.5(b).
106 RI Gen Laws section 11-49.2-2(2); Tex Bus & Comm Code section 48.102(a).
107 Nev Rev Stat section 597.970.
108 id.
109 Nev Rev Stat section 603A.040.

The Nevada encryption law states that entities 'doing business in th[e] [s]tate' are subject to the law, but does not define the scope of this phrase.[110]

The Massachusetts Office of Consumer Affairs and Business Regulations has adopted a rule that requires '[e]very person that owns, licenses, stores or maintains personal information about a [Massachusetts] resident [to] develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information'.[111] This rule requires a covered entity to implement, maintain and update a risk-based security programme tailored to the size, complexity and nature and scope of its activities. The rule also prescribes particular requirements that an organisation's risk-based security programme must include, such as '[t]aking reasonable steps to select and retain third-party service providers that are capable of' – and requiring them by contract to – implement and maintain 'appropriate security measures to protect such personal information'.[112] In addition, the rule prescribes several specific required elements of a company's comprehensive information security programme relating to its computer systems, including any wireless system.[113]

Security breach notification

All 50 US states have enacted security breach notification requirements.[114] These laws generally require organisations to expeditiously notify individuals when unencrypted computerised personal information has been, or is reasonably believed to have been, accessed or acquired by an unauthorised person. In addition, several of these laws also apply to security breach incidents affecting personal information stored in any medium, including paper records, rather than only computerised records.[115] While state laws vary in their nuances, personal information that commonly triggers notification includes an individual's name in combination with one or more of the following:

- a national or government-issued identification number, such as a Society Security number (SSN), individual taxpayer identification number, driver's licence number or passport number;
- a financial account number in combination with a security code, access code, password or PIN that is necessary to access the account;
- health or medical information;
- health insurance policy number or a subscriber identification number; or
- online credentials, such as username and password to an online account.

110 Nev Rev Stat section 603A.200.

111 201 Mass Regs Code section 17.03(1).

112 201 Mass Regs Code section 17.03(2)(f).

113 201 Mass Regs Code section 17.04.

114 See Security Breach Notification Laws, Nat'l Conf of State Legislatures (29 September 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

115 See, eg, Haw Rev Stat sections 487N-1–487N-3.

Most of these laws also require notification of state regulators as well as individuals.[116] Congress has considered, but not passed, bills that would enact national requirements to notify individuals about a breach of security.[117]

Social Security Number laws

At least 32 states, as well as Guam and Puerto Rico, have passed laws restricting the use of SSNs.[118] Many of these laws prohibit a person or entity from:

- publicly posting or publicly displaying in any manner an individual's SSN;
- printing SSNs on any card required for the individual to receive products or services provided by the person or entity;
- requiring SSNs to access an internet website, unless a password or other authentication device is also required;
- requiring an individual transfer his or her SSN over the internet unless the connection is secure or the number is encrypted; and
- printing a number known to be the individual's SSN on materials that are mailed to the individual unless required by federal or state law.[119]

Some states, such as Connecticut, Massachusetts, Michigan, New Mexico, New York, and Texas, also require that an organisation adopt a policy designed to ensure that SSNs are properly safeguarded.[120] Examples of policy components include implementing information security mechanisms protecting SSNs, limiting access to SSNs within the organisation, providing for proper disposal of materials including SNNs, and penalising policy violations.[121] The scope of these laws varies markedly; for instance, Massachusetts imposes these obligations on any organisation handling any personal information of Massachusetts residents, while the Texas law only applies to entities that requires a customer to disclose his or her SSN to complete a transaction.[122]

116 Statutory deadlines for notifying state officials (usually attorney generals) range from 30 days after discovering a breach in Florida to five business days in Iowa, while the threshold numbers of state residents affected triggering notification of state officials range from 250 in Oregon to 1,000 in Virginia. See Fla Stat section 501.171; Iowa Code section 715C.2; Or Rev Stat section 646A.604; Va Code section 18.2-186.6.

117 See, eg, Personal Data Notification and Protection Act of 2017, HR 3806, 115th Cong (2017); Personal Data Notification and Protection Act of 2015, HR 1704, 115th Cong (2015).

118 See US Gov't Accountability Office, GAO-08-1009R Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring (noting that at least 25 states had statutes limiting SSN display in public records).

119 See, eg, Alaska Stat sections 45.48.400–45.48.480.

120 See Conn Gen Stat sections 42-470–42-471; 201 Mass Code Regs sections 17.01–17.05; Mich Comp Laws section 445.84; NM Stat sections 57-12B-2–3; NY Gen Bus Law section 3990dd(4); Tex Bus & Com Code sections 501.051–501.053 (effective 1 April 2009).

121 See Conn Gen Stat section 42-470 (penalties for violations); 201 Mass Code Regs sections 17.04 (computer system security requirements); Mich Comp Laws section 445.84 (disposal of documents containing SSNs); NM Stat section 57-12B-3 (limiting access to employees authorised to access SSNs).

122 See 201 Mass Code Regs sections 17.01–17.04; NM Stat sections 57-12B-2–3.

Monitoring

Businesses that intend to engage in surveillance of communications also must be aware of relevant state law. The federal wiretap statute discussed above, ECPA, does not pre-empt state wiretap statutes that offer privacy protections greater than those available under federal law, and many states do restrict surveillance activities. For example, 15 states (California, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Oregon, Pennsylvania, Vermont and Washington) all generally require both parties' consent in at least some circumstances before a conversation may be overheard, intercepted, or recorded.[123] In addition to state wiretap laws, some states prohibit video surveillance in certain locations.[124] Two states, Connecticut and Delaware, have laws requiring private employers to notify employees if their email or internet access is being monitored.[125] Two others, Colorado and Tennessee, require public and state employers to adopt written policies on email monitoring of their employees.[126]

Unfair or deceptive acts or practices

Similar to the federal approach to regulating the misrepresentation of information, all states have adopted laws that regulate unfair or deceptive acts or practices (UDAP).[127] Some of these are modelled after section 5 of the FTC Act and are often referred to as 'Mini-FTC Acts'. Other states have modelled their UDAP laws after the FTC Act. States have used these laws to bring enforcement actions against companies, alleging failures to protect the security of customer information.

For instance, Ohio's Attorney General relied on that state's UDAP law[128] to bring a complaint against DSW, Inc, a large shoe retailer, after it experienced a security breach affecting customers' personal information and failed to identify and notify all affected

123 Some caveats apply. For instance, Massachusetts prohibits 'secret' recordings. Nevada's statutory text requires only one party's consent, but the Nevada Supreme Court has required all parties to consent to recordings of telephone conversations. Michigan's law prohibits eavesdropping 'without the consent of all parties', but defines eavesdropping as referring only to others' private conversations. Oregon's law applies only to in-person conversations. See Cal Penal Code section 631; Conn Gen Stat section 52-570(d); Del Code Ann Title 11, section 2402; Fla Stat section 934.03; 720 Ill Comp Stat 5/14-2, 5/14-3; Md Code Ann, Cts & Jud Proc section 10-402; Mass Gen Laws Chapter 272, section 99; Mich Comp Laws section 750.539 et seq; Mont Code Ann section 45-8-213; Nev Rev Stat sections 200.620–650; NH Rev Stat Ann section 570-A:2; Or Rev Stat section 165.540; 18 Pa Cons Stat sections 5703–5704; Wash Rev Code section 9.73.030; *Vermont v Geraw*, 795 A2d 1219 (Vt 2002); *Lane v Allstate Ins Co*, 114 Nev 1176 (1998).

124 For instance, California's law prohibits video recording in places like restrooms, while Michigan's law applies to all statutorily defined 'private' places. See Cal Lab Code section 435; Mich Comp Laws section 750.539d.

125 See Conn Gen Stat section 31-48(d); Del Code Title 19, section 705; see also Notice of Monitoring of Employee E-mail Communications and Internet Access, Nat'l Conf of State Legislatures (13 May 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#Monitoring.

126 Colo Rev Stat section 24-72-204.5; Tenn Code section 10-7-512.

127 See State-by-State Summaries of State UDAP Statutes, Nat'l Cons L Ctr (10 January 2009).

128 Ohio Rev Code sections 1345.01–1345.13.

customers.[129] The Attorney General claimed that DSW's conduct was both deceptive and unfair, although the complaint made no allegation that DSW had made any commitments to consumers regarding the disclosure of information security incidents; at the time, Ohio did not have a security breach notification law in force.[130]

129 See *State of Ohio v DSW, Inc*, Case No. 05CV06-6128 (Ct of Common Pleas, Franklin County, Ohio, 6 June 2005) (complaint for declaratory judgment).

130 id.

Miriam H Wugmeister
Morrison & Foerster LLP

Miriam H Wugmeister co-chairs the global privacy and data security group at Morrison & Foerster. Based in New York, she advises on the privacy challenges of some of the world's largest multinationals and has helped hundreds of clients respond to data security incidents, including some of the most complex and noteworthy in recent years. She advises organisations on the planning and execution of complex global compliance efforts, assists in the negotiation of strategic deals, and defends regulatory and litigation matters relating to privacy and data security in the United States and internationally. Ms Wugmeister is also the leader of the Global Privacy Alliance, which encourages the rational development of privacy laws around the world and monitors privacy practices, laws and regulations globally.

Julie O'Neill
Morrison & Foerster LLP

Julie O'Neill is a partner in the global privacy and data security group at Morrison & Foerster, based in Washington, DC and Boston. She advises on cutting-edge issues at the intersection of privacy and consumer protection laws, including online and offline tracking, interest-based advertising, geo-targeting and other mobile tracking, personalisation, and cross-device tracking. A former FTC staff attorney, she regularly defends companies in investigations by the FTC and before data protection authorities around the world. She also creates compliance programmes for clients' use of a wide variety of channels for communicating with and marketing to consumers, including email, telephone, text message, and fax both in the United States and globally.

Nathan D Taylor
Morrison & Foerster LLP

Recognised as an authority on financial privacy issues, Nathan D Taylor helps financial institutions and other companies develop practical solutions for complying with privacy and data security laws. In particular, Mr Taylor tackles the most complex issues relating to the privacy and security of financial information. As state privacy law appears to be entering a new era with the adoption of the California Consumer Privacy Act (CCPA), Mr Taylor is assisting many banks, insurance companies, broker dealers and other financial institutions in making sense of the complex law and the challenges presented by significant, but often confusing, new privacy obligations. He also continues to help companies across industries develop solutions to comply with the myriad state data breach and data security laws that have been enacted since 2003. Mr Taylor is co-author of the leading financial privacy treatise, *The Law of Financial Privacy*.

Gina M Pickerrell
Morrison & Foerster LLP

Gina M Pickerrell is a member of Morrison & Foerster's market-leading privacy and data security team, based in the firm's Washington, DC office. Ms Pickerrell helps clients across industries craft global privacy compliance strategies and data security solutions. She also has experience assisting clients in response to security incidents and counselling clients on privacy and data security issues in mergers and acquisitions. Prior to joining Morrison & Foerster, she worked at the US Federal Trade Commission's Bureau of Consumer Protection, where she investigated consumer complaints and assisted in federal court litigations. Ms Pickerrell previously served as a Non-Commissioned Military Police Officer in the Army National Guard and was deployed to Iraq in support of Operations Iraqi Freedom and Iraqi Endurance.

MORRISON
FOERSTER

Morrison & Foerster is a leading global law firm with 17 offices across the United States, Europe and Asia. Our clients include some of the largest financial institutions, investment banks, and Fortune 100, technology and life sciences companies. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. The firm also has a long history of commitment to the community through providing pro bono legal services, including litigating for civil rights and civil liberties, improving public education for poor children, advocating for veterans, promoting international human rights, winning asylum for the persecuted and safeguarding the environment.

250 West 55th Street
New York, NY 10019-9601
United States
Tel: +1 212 468 8000
Fax: +1 212 468 7900

www.mofo.com

Miriam H Wugmeister
mwugmeister@mofo.com

Julie O'Neill
joneill@mofo.com

Nathan D Taylor
ndtaylor@mofo.com

Gina M Pickerrell
gpickerrell@mofo.com

The GDR Insight Handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-266-4