Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

USA: Law & Practice

Frankfurt Kurnit Klein & Selz

chambers.com

2019

Law and Practice

Contributed by Frankfurt Kurnit Klein & Selz

Contents

Frankfurt Kurnit Klein & Selz was founded more than 40 years ago as a boutique law firm servicing the entertainment and arts communities in New York City and today provides the highest-quality legal services to clients in a wide range of industries and disciplines worldwide. The firm has a Privacy & Data Security team consisting of six partners, one counsel, and seven associates based in Los Angeles and New York. The team focuses on a number of areas, including: US privacy and data security compliance programmes; international privacy compliance and cross-border data transfers; ad tech and big data analytics issues; vendor management, cloud computing and other tech transactions; and security incident preparedness and response.

Author

Tanya L. Forsheit is a partner at the firm and Chair of the Privacy & Data Security Group, based in Los Angeles, and Supervising Partner of the Los Angeles office. She advises on the protection, processing and monetisation of data, including matters related to interest-based advertising, mobile apps, cloud computing, smart devices, and data analytics. She is a member of the International Association of Privacy Professionals, the Advisory Council of the Center for Democracy & Technology, and the American Bar Association: Science and Technology Law Section. She has published numerous articles relating to the practice of data protection law, and acted as Adjunct Professor at Loyola Law School, Spring 2018 and Spring 2019, teaching European Union Cybersecurity & Data Privacy.

1. Basic National Legal Regime

1.1 Laws

Privacy, data protection, cybersecurity and data-breach notification laws enacted in the United States prior to 2018 are generally sectoral and/or state-based. There is no comprehensive US privacy or cybersecurity law.

There are highly significant privacy and data security laws at the state level that regulate organisations in almost every industry sector. These include the Massachusetts Data Security Regulations, 201 CMR 17.00 et seq, and the California Online Privacy Protection Act, Civil Code 22575 et seq ('CalOPPA'). Some states have laws that focus on certain kinds of information – for example, Illinois, Texas and Washington have laws that restrict the use and sharing of biometric information without consent. Most of these state laws are enforced by the State Attorneys General, who may seek injunctive relief and/or fines and penalties. However, Illinois' Biometric Information Privacy Act (the 'BIPA') has a private right of action through which individuals can seek statutory damages of USD1,000 per violation. California also has a unique law, the Shine the Light law, that allows individuals to obtain information regarding what kinds of personal information have been shared by a company with third parties, and in some cases affiliates, for those third-parties' own marketing purposes.

There are also sectoral laws, at the federal and state level, that impose considerable compliance obligations on organisations in certain industries. These include the Health Information Portability and Accountability Act (the 'HIPAA') for healthcare providers, health-insurance carriers, and similar covered entities; the Gramm-Leach-Bliley Act (the 'GLBA') for financial institutions; the Children's Online Privacy Protection Act (the 'COPPA') for the collection of information online of minors under the age of 13; and the Video Privacy Protection Act (the 'VPPA') restricting the sharing of personally identifiable information associated with video viewing activity. Some of these sectoral laws, such as HIPAA and GLBA, are enforced by federal regulators such as the Department of Health and Human Services (HHS) and the Consumer Financial Protection Board (CFPB), respectively. The Federal Trade Commission (FTC) enforces COPPA and may seek penalties of more than USD40,000 per violation. The VPPA has a private right of action with statutory damages of USD2,500 per violation and has therefore spawned a considerable volume of class action litigation.

The US has a complex set of data security breach notifications laws, including laws in each of the 50 states and several territories, which apply to businesses across all industry sectors and are triggered by the kind of information and incident at issue, HIPAA, and the FTC breach notification rules that govern certain kinds of electronic health records. Most states allow the relevant State Attorney General to enforce the law and seek injunctive relief and/or fines and penalties. Some states have a private right of action.

Perhaps the most significant privacy and data protection development of the last year was the enactment of the California Consumer Privacy Act (the 'CCPA'), the first comprehensive privacy law in any state or federal jurisdiction in the United States. The CCPA will take effect on 1 January 2020. It applies to any sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organised or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on whose behalf such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of California, and that satisfies one or more of certain thresholds whereby:

- it has annual gross revenues in excess of USD25 million;
- alone or in combination, it annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; and/or
- it derives 50% or more of its annual revenues from selling consumers' personal information.

The law imposes European-style requirements to provide high levels of transparency to consumers regarding how their personal information is used and shared, and gives individual consumers rights to access, delete, correct and prevent the sale of their personal information, among other things. Personal information is very broadly defined to include any information capable of being associated with a person. The California Attorney General may enforce the CCPA beginning 1 July 2020 (or six months after issuing Regulations, if sooner) and may seek USD2,500 to USD7,500 per violation. There is also a private right of action in the event of unauthorised access and exfiltration, theft or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and a private plaintiff may recover USD100 to USD750 per violation without any show of harm.

1.2 Regulators

Like the privacy and data security laws in the US, the regulators are largely determined by jurisdiction and/or sector. For 'non-regulated' entities (ie, not financial services or healthcare, mentioned in section 1 above), the FTC is the privacy regulator in the US. The FTC uses its Section 5 authority to investigate unfair or deceptive acts or practices in or affecting commerce to police privacy and data security practices of concern. The FTC has brought more than 100 cases under its Section 5 authority involving privacy and/or data security. The vast majority of these cases resulted in consent decrees in which the FTC, which lacks authority to assess monetary penalties, imposes terms of FTC oversight (sometimes as long as 20 years), and requires companies to implement privacy and security programmes and to be the subject of independent assessments of the company's privacy and security practices.

State Attorney Generals have taken an even more aggressive role in certain parts of the country, using their authority under 'little FTC Acts' to file complaints and enter into consent decrees with similar oversight plus fines ranging from a few thousand to hundreds of millions of dollars. Often the states co-operate in multi-state enforcement actions in connection with larger matters.

Investigations by both the FTC and the State Attorneys General are likely to start with an informal inquiry or a formal Civil Investigative Demand (CID) that includes interrogatories and document requests. This might follow a publicly disclosed data breach (many states require notice to state regulators) or media coverage of revelations regarding previously undisclosed uses of personal information by a company.

1.3 Administration and Enforcement Process

The FTC may prosecute any inquiry necessary to its duties and may "gather and compile information concerning, and to investigate from time to time the organisation, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce" with the exception of banks, savings and loan institutions, federal credit unions and common carriers. Pre-complaint investigations are generally confidential. The FTC has subpoena power to compel attendance and testimony of witnesses and the production of all documentary evidence relating to any matter under investigation. Following an investigation, the FTC can initiate an enforcement action if it has 'reason to believe' that the law is being or has been violated. The FTC enforces Section 5 through both administrative and judicial processes. The Commission must go to court to obtain civil penalties or consumer redress for violations of its orders to cease and desist.

Practices are 'unfair' if they cause or are likely to cause "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

Similarly, the State Attorneys General have authority to compel production of documents, attendance and testimony in support of an investigation into acts or practices declared to be unlawful under state unfair practices acts.

1.4 Multilateral and Subnational Issues

The United States is considered 'inadequate' as a country for purposes of transfers of personal data from the EU to the US. Thus, in order for such data transfers to proceed, organisations in the US must:

- self-certify under the Privacy Shield Framework overseen by the Department of Commerce (the successor to the now-defunct Safe Harbor Framework struck down by the EU Court of Justice in 2015);
- enter into controller-to-controller or controller-to-processor standard contractual clauses; or
- have Binding Corporate Rules (BCRs) approved by the EU data protection authorities.

In late 2017, the US became the first Asia-Pacific Economic Co-operation (APEC) economy to join the APEC Privacy Recognition for Processors System. That system offers a trustmark certification to personal information processors in the region.

As noted above, much of the regulation of privacy, data protection and cybersecurity in the United States is at the state or territory level, with 50 state data breach notification laws and similar numbers of state laws governing data disposal and protection of social security numbers.

1.5 Major NGOs and Self-Regulatory Organisations

The advertising industry has robust self-regulatory mechanisms in the US with associated enforcement mechanisms to address privacy abuses. Most well-known to consumers is the AdChoices icon, a creation of the Digital Advertising Alliance (DAA). Companies participating in the programme agree to follow the DAA principles for transparency and choice for interest-based advertising. The principles apply to the collection and use of interest-based advertising data and provide other protections for data collection across sites and apps. These include controls for the use of mobile location and personal directory information, and prohibitions on the use of interest data for eligibility determinations.

The AdChoices icon appears on web pages and gives the consumer information and control over the types of ads that use information about the consumer's likely interests. The consumer can opt out from participating in company trackers. In that case, the consumer continues to see non-targeted ads.

The advertising industry issued a comprehensive self-regulatory programme for online behavioural advertising in 2014. The initiative includes the American Association of Advertising Agencies (4A's), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA) and the Interactive Advertising Bureau (IAB) in conjunction with the Council of Better Business Bureaus (CBBB).

The DAA principles and the IAB initiative are similar to but slightly different from the FTC's own self-regulatory framework for online behavioural advertising, issued in February 2009.

These self-regulatory activities in the targeted advertising space have extended to mobile. In May 2015, the National Advertising Initiative (NAI) released a guide setting forth best practice for providing transparency about non-cookie technologies. In November 2015, the DAA released its own guidance on the application of DAA principles to cross-device tracking, confirming the application of the transparency and consumer control obligations.

In early 2017, the FTC issued a report on cross-device tracking, largely mirroring its 2009 principles. Specifically, the FTC called for companies to be transparent, give consumers choices, not engage in cross-device tracking on sensitive topics, only collect data as needed, and not keep data longer than necessary for business purposes. The transparency principles include an obligation to notify consumers of third-party installations that may enable tracking on services or devices and of devices they may not expect to collect their information for cross-device tracking (eg, smart TVs).

1.6 System Characteristics

Although the US does not have an omnibus federal privacy law like Europe, it has literally hundreds of privacy and data security laws across states and industries (as discussed above). Moreover, US regulators, particularly at the state level, have been far more active than EU regulators (prior to the effective date of the European General Data Protection Regulation (GDPR) in May 2018) in investigating privacy and data security practices and taking enforcement action.

Nonetheless, the perception remains that the US is not sufficiently protective of consumer privacy rights, particularly in the wake of the Edward Snowden revelations of 2013.

1.7 Key Developments

Media coverage of extensive and previously undisclosed data sharing by Facebook, which came to light in the 2018 Cambridge Analytica incident, resulted in Mark Zuckerberg, the CEO of Facebook, being called before Congress. These events were also likely the impetus for the success of Alastair Mactaggart in launching the California ballot initiative that resulted in the rushed enactment of the European-style comprehensive CCPA in the summer of 2018, with the backing of large Silicon Valley technology companies such as Facebook and Google. Early 2019 saw the emergence of similar bills in Washington, New York and New Mexico.

1.8 Significant Pending Changes, Hot Topics and Issues

The country will be watching California, which is considering amendments to the CCPA under intense pressure from businesses, and where the Attorney General is engaged in rule-making. Other states are likely to follow suit.

There is also a much higher likelihood that omnibus federal privacy law will pass sometime in the next few years. For the first time in US history, executives at the largest technology companies – including Apple, Google and Facebook – are calling for a federal privacy law.

There are already many federal bills on the table, some of them bi-partisan, that are competing for attention. Some frame the obligations that organisations have with respect to personal information as comparable to a fiduciary duty (eg, the 'Data Care Act' introduced in December 2018 by 15 senators). Others require an annual data protection report and call for jail time for CEOs who falsely certify information in the report (eg, the 'Consumer Data Protection Act,' introduced in November 2018).

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

At the time of writing, the US does not have any omnibus laws currently in effect.

With the exception of HIPAA, there is no US federal or state law that calls for the appointment of a privacy or data protection officer.

The US does not have criteria necessary to authorise collection of data. The concept of 'legitimate interest' does not exist, and consent is not required for data collection. However, there are certain sectoral laws that restrict a company's ability to use or share personal information in certain ways in the absence of consent. These include:

- the Telephone Consumer Protection Act (TCPA), which requires prior affirmative express consent for text messages and auto-dialled marketing calls;
- the VPPA, which requires prior affirmative consent for the sharing of personally identifiable video viewing information; and
- the California Financial Information Privacy Act ('CalFIPA'), and Vermont's Financial Privacy Act, which both require affirmative consent for a financial institution to share non-public personal information with third parties and unrelated companies.

The FTC has also articulated a principle that companies should obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected, or collecting sensitive data (health and financial information, children's information, social security numbers, precise geolocation information etc) for certain purposes.

There are no 'privacy by design' or 'by default' concepts under existing US law.

There are no strict requirements for private sector organisations to conduct privacy impact analyses under US law, but both HIPAA and the GLBA require that covered healthcare organisations and financial institutions, respectively, conduct risk assessments in connection with protecting and securing protected health information and non-public personal information, respectively.

Certain government agencies are required to conduct privacy impact assessments under federal law (the 'E-Government Act').

Many US state laws require companies to adopt internal or external privacy policies. Several states require the posting of privacy policies covering online data collection and processing. These include CalOPPA, the Delaware Online Privacy and Protection Act, and Nevada law. Other states require the adoption of internal policies to address data security or protection of social security numbers. These include Massachusetts, which requires a Written Information Security Programme (or 'WISP'); Connecticut, which requires a publicly posted policy addressing protection of social security numbers; Michigan, which requires a privacy policy in an electronically available employee manual; and New Mexico, New York and Texas (which each require internal policies or regulations addressing protection of social security numbers).

Until the enactment of the CCPA in June 2018, there were no US federal or state laws addressing data subject rights. The CCPA in its current form at the time of writing requires businesses to provide two or more designated methods for consumers to submit rights requests, including at a minimum a website address if the business has one, and a toll-free number. After receiving a consumer request, the business has 45 days to respond to a consumer's verifiable request and deliver the information free of charge and without requiring account registration. A 'verifiable consumer request' is defined to mean one that was made by the consumer, on behalf of a minor child, or by someone authorised to act on the consumer's behalf, that the business can reasonably verify the consumer's identity. The business must take steps promptly to respond to consumer requests within the 45 days. However, one 45-day extension is permitted when reasonably necessary as long as the consumer is given notice of the extension within the initial 45-day period.

Californian consumers have the right to request access to the personal information a business holds about them, including an associated right to portability. Businesses are required to disclose the specific information pertaining to the consumer and provide copies of their information. Upon a verifiable consumer request, businesses must provide, in a reasonably accessible form, on an individualised basis, information including:

- categories of personal information collected, disclosed for a business purpose or sold about the specific consumer;
- categories of sources from which the personal information was collected;
- the personal information collected about that consumer;
- the business and commercial purposes for which the personal information was collected;
- categories of personal information disclosed for a business purpose; and
- categories of third parties to which that personal information was sold or disclosed to for a business purpose.

Consumer requests are limited to a 12-month look-back, meaning disclosures are only required to report activities in the preceding 12 months. (Note, however, that the right to delete and do not sell requests are not limited to a 12-month look-back.)

The law also gives consumers a right to request that their personal information be deleted, as discussed below.

There are few US laws that directly address anonymisation, de-identification or pseudonymisation. The HIPAA Privacy Rule is one of the rare exceptions, providing the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

The HIPAA Privacy Rule provides two methods by which health information can be designated as de-identified. One method requires that a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information, and documents the methods and results of the analysis that justify such determination.

Alternatively, there is a 'Safe Harbor' method. Under the 'Safe Harbor' method, certain identifiers of the individual or of relatives, employers, or household members of the individual, must be removed, including:

- names;
- all geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
- the geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
- the initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000;
- all elements of dates (except the year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including the year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- telephone numbers;
- vehicle identifiers and serial numbers, including licence plate numbers;
- fax numbers;
- device identifiers and serial numbers;
- email addresses;
- web universal resource locators (URLs);
- social security numbers;
- internet protocol (IP) addresses;
- medical record numbers;
- biometric identifiers, including finger and voice prints;
- health plan beneficiary numbers;
- full-face photographs and any comparable images;
- account numbers;
- any other unique identifying number, characteristic, or code; and
- certificate/licence numbers.

Further, to satisfy the 'Safe Harbor' de-identification method, the covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

The FTC has also articulated a standard for de-identification, albeit not incorporated into any law. The FTC describes de-identified data as data that is not 'reasonably linkable' to a consumer, where the company processing the data "takes reasonable measures to ensure that the data is de-identified; publicly commits not to try to re-identify the data; and contractually prohibits downstream recipients from trying to re-identify the data."

See Fed Trade Communication, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers (March 2012).

Finally, the CCPA introduces for the first time in US privacy law a concept of pseudonymisation, defining it as "processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."

However, pseudonymised information is still considered personal information under the law and it is only referenced in one other location in the statute. The term is referenced in connection with the definition of 'research' under the law, which specifies that research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be, among other things, subsequently pseudonymised and de-identified, or de-identified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

There is little actual law addressing profiling, automated decision-making, Big Data or artificial intelligence.

In 2018, Vermont became the first state to enact legislation regulating non-consumer-facing data brokers that buy and sell personal information. The law requires data brokers to register annually with the Vermont Attorney General, make annual disclosures regarding their practices related to the collection, storage or sale of consumers' personal information and for allowing consumers to opt out. The law also requires data broker reporting of the number of data breaches experienced during the prior year and the total number of consumers affected by the breaches (with breach being defined more broadly than in the regular Vermont statute). Additional disclosure requirements apply if the data broker knowingly collects information from minors.

The FTC has also issued a number of reports addressing best practices for data brokers and other players in the Big Data ecosystem.

In its data broker report of May 2014 ('Data Brokers: A Call for Transparency and Accountability'), the FTC found that there are a number of potential risks to consumers from data brokers' collection and use of consumer data, including with respect to the scoring processes used in some marketing products that are not transparent to consumers. The FTC expressed concern that consumers may be unable to take actions that might mitigate the negative effects of lower scores, such as being limited to ads for subprime credit or receiving different levels of service from companies. With respect to other marketing products, these scores might also facilitate the sending of advertisements about health, ethnicity or financial products, which some consumers:

"*may find troubling and which could undermine their trust in the marketplace. Moreover, marketers could even use the seemingly innocuous inferences about consumers in ways that raise concerns. For example, while a data broker could infer that a consumer belongs in a data segment for 'Biker Enthusiasts,' which would allow a motorcycle dealership to offer the consumer coupons, an insurance company using that same segment might infer that the consumer engages in risky behavior*."

In its report, the FTC called for legislation to address some of these issues and made best practice recommendations for data brokers. For example, the report suggests that data brokers practice privacy-by-design and recommends a policy of data minimisation. The report also advises data brokers to maintain reasonable safeguards to protect consumer information. It also suggests that data brokers take reasonable steps to mitigate the risk that data brokerage customers misuse data for unlawful purposes, including contractual restrictions, seeding databases with dummy data, and conducting customer audits.

The FTC also noted in its report that the use of race, colour, religion and certain other categories to make credit, insurance and employment decisions is already a violation of non-privacy US laws such as the Equal Credit Opportunity Act.

In some situations where the FTC has sought to enforce restrictions on data brokers that go beyond the boundaries of existing law, such as the Fair Credit Reporting Act (FCRA), it has used its Section 5 authority, discussed above. In its famous ChoicePoint case, the FTC alleged a data broker had violated the FCRA by failing to employ reasonable and appropriate measures to secure the personal information it collected for sale to its subscribers, including reasonable policies and procedures to verify or authenticate the identities and qualifications of prospective subscribers. The FTC alleged that this enabled downstream illegal uses of consumers' data. Because some of ChoicePoint's activities were not FCRA-covered, the FTC alleged that ChoicePoint's failure to implement these policies and procedures was also an unfair practice under Section 5 of the FTC Act.

The concept of 'injury' or 'harm' is a loaded one under US privacy and data protection law and is probably the most hotly litigated topic under US privacy law. The United States Supreme Court's decision in Spokeo Inc v Robins 578 US _ (2016) made clear that there can be no Article III standing under the US Constitution unless and until there is in

fact a concrete and particularised injury-in-fact. However, that does not mean under the US cases that an intangible injury cannot be concrete. Spokeo arose in the context of an alleged violation of a statute, the FCRA. The Court made clear that a plaintiff does not automatically satisfy the injury-in-fact requirement "whenever a statute grants a person a statutory right and purports to authorise that person to sue to vindicate that right." Therefore, "a bare procedural violation, divorced from any concrete harm" does not satisfy the injury-in-fact requirement of Article III.

Another important US Supreme Court decision on the harm issue is Clapper v Amnesty International USA, 568 US 398 (2013). There the Supreme Court found that the plaintiff did not have standing to challenge a section of the Foreign Intelligence Surveillance Act (FISA) based on assertions that there was an "objectively reasonable likelihood" that their communications would be intercepted at some point in the future because Article III standing requires the threatened injury to "be certainly impending to constitute an injury in fact," and the plaintiff's "allegations of possible future injury [were] not sufficient."

Injury and harm becomes an even more challenging concept in the absence of a statutory violation. Federal Circuit Courts have split in their approaches to data breach standing, meaning that there is no consistent framework for assessing harm in the context of a lawsuit stemming from a data breach involving personal information. The courts have not yet directly addressed standing requirements for plaintiffs in data breach litigation. This issue may reach the Supreme Court in 2019 in the Zappos.com Inc v Stevens case in which Zappos has petitioned for a writ of certiorari. The petition has been briefed and distributed for conference as of the time of writing.

2.2 Sectoral Issues

There is no single definition of what constitutes 'sensitive' data under US privacy and data security laws. That being said, the FTC has identified certain kinds of information that it deems to be sensitive, including, at a minimum, data about children, financial and health information, social security numbers and precise geolocation data. In its 2012 Privacy Report, the FTC articulated a principle that companies should obtain affirmative express consent before collecting sensitive data for certain purposes.

Financial data institutions are subject to strict privacy regulation under the GLBA. Pursuant to the Financial Privacy Rule, a financial institution may not disclose to a non-affiliated third party any non-public personal information unless such financial institution provides or has provided to the consumer a notice, at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, of such financial institution's policies and practices with respect to:

- the categories of non-public personal information that are collected by the financial institution;
- disclosing non-public personal information to affiliates and non-affiliated third parties;
- disclosing non-public personal information of persons who have ceased to be customers of the financial institution; and
- protecting the confidentiality and security of the non-public personal information of consumers.

In 2009, a group of federal financial regulators issued a model privacy form. Financial institutions may rely on the model privacy form as a safe harbour to provide disclosures under the GLBA Privacy Rule.

A financial institution must, in its notice to consumers, give the consumer the opportunity to direct that non-public personal information not be disclosed to third parties, and must give the consumer an explanation of how the consumer can exercise that non-disclosure option. A financial institution also may not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

Nevertheless, a financial institution may provide non-public personal information to a non-affiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the Regulations prescribed under the GLBA, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information. A non-affiliated third party that receives such non-public personal information from a financial institution is prohibited from disclosing the information to any other non-affiliated third party.

A financial institution may disclose non-public personal information under a variety of other circumstances, including:

- as necessary to effect, administer, or enforce a transaction requested or authorised by the consumer, or in connection with servicing or processing a financial product or service requested or authorised by the consumer;
- maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card programme or other extension of credit on behalf of such entity;

- a proposed or actual securitisation, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;
- with the consent or at the direction of the consumer;
- to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein;
- to protect against or prevent actual or potential fraud, unauthorised transactions, claims, or other liability;
- for required institutional risk control, or for resolving customer disputes or inquiries;
- to persons holding a legal or beneficial interest relating to the consumer;
- to persons acting in a fiduciary or representative capacity on behalf of the consumer;
- to provide information to insurance rate advisory organisations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;
- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act, to law enforcement agencies, self-regulatory organisations, or for an investigation on a matter related to public safety;
- to a consumer reporting agency in accordance with the FCRA, or from a consumer report reported by a consumer reporting agency;
- in connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of non-public personal information concerns solely consumers of such business or unit;
- to comply with federal, state or local laws, rules and other applicable legal requirements;
- to comply with a properly authorised civil, criminal or regulatory investigation or subpoena or summons by federal, state or local authorities; or
- to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorised by law.

The GLBA Safeguards Rule requires each financial institution to develop a written information security programme to protect the confidentiality and integrity of personal consumer information that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. Each of the federal agencies responsible for adopting rules pursuant to the GLBA has promulgated its own Safeguards Rule, as have state insurance regulators.

The GLBA is clear that a state statute, regulation, order or interpretation is not inconsistent with the provisions of the GLBA if the protection such statute, regulation, order or interpretation affords any person is greater than the protection provided under the GLBA. Certain states, such as California and Vermont, do impose more stringent sharing requirements that, with certain exceptions, require explicit opt-in before non-public personal information may be shared with a non-affiliated third party. The CalFIPA also purports to restrict the sharing of consumer information with affiliates, stating that "[a] financial institution shall not disclose to, or share a consumer's non-public personal information with, an affiliate unless the financial institution has clearly and conspicuously notified the consumer annually in writing… that the non-public personal information may be disclosed to an affiliate of the financial institution and the consumer has not directed that the non-public personal information not be disclosed." (This affiliate-sharing restriction has been the subject of litigation and is at least partially pre-empted by the FCRA.)

The FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), regulates the collection, use, disclosure and disposal of personal information by consumer reporting agencies and the users of consumer reports (including financial institutions). The FCRA prohibits an organisation from using or obtaining a consumer report for any purpose unless the report is obtained for a purpose for which it is authorised to be furnished under the FCRA and the purpose is certified as required under the statute by a prospective user of the report. The FCRA also includes an affiliate sharing rule and an affiliate marketing rule that impose certain restrictions on affiliate sharing of certain types of information for a variety of purposes.

Health data

HIPAA regulates the handling of protected health information (PHI) by health plans, healthcare clearing-houses and healthcare providers who transmit health information in electronic form in connection with certain transactions. It also directly regulates service providers of such covered entities, known as business associates, who process PHI on behalf of a covered entity or otherwise have access to it. The Privacy Rule standards address the use and disclosure of PHI as well as standards for individuals' privacy rights to understand and control how their health information is used. The HIPAA Security Rule establishes national standards to protect individuals' electronic PHI that is created, received, used or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI. Covered Entities and Business Associates must enter into specific forms of agreements known as Business Associate Agreements as part of HIPAA's requirements.

Communications data

The Federal Communications Act and the rules of the Federal Communications Commission (FCC) require telecom-

munications carriers and interconnected providers of Voice over Internet Protocol (VoIP) services to protect customer proprietary network information (CPNI). CPNI includes, among other things, phone numbers called, the frequency, duration and timing of such calls, and any services purchased by the consumer, such as call waiting. FCC rules require the filing of annual reports to certify their compliance with the CPNI rules.

Other categories of sensitive data
Union membership, sexual orientation, political or philosophical beliefs and similar information are not currently treated as sensitive information under US privacy or data security law. However, the CCPA defines personal information to include any 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, including, but not limited to, characteristics of protected classifications under California or federal law (such as race, gender and sexual orientation).

Voice Telephony
See above discussion of communications data.

Text Messaging
As noted above, text messaging is strictly regulated under the TCPA, which prohibits text messaging without prior affirmative express consent (which must be in writing in the case of marketing text messages).

Internet
As noted above, California, Delaware and Nevada require online privacy policies that include disclosures regarding how information is collected, used and shared. When the CCPA takes effect, it will add much more specific requirements for online privacy policy disclosures. The CCPA requires that a business that collects personal information about a consumer disclose:

- the categories of personal information it has collected about that consumer;
- the categories of sources from which the personal information is collected;
- the business or commercial purpose for collecting or selling personal information;
- the categories of third parties with whom the business shares personal information; and
- the specific pieces of personal information the business has collected about that consumer.

A business that sells consumers' personal information to third parties must provide notice to consumers that the information may be sold and that consumers have the right to opt out of the sale of their personal information. The CCPA also requires that a business that collects a consumer's personal information inform consumers at or before the point of collection as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.

Use of cookies, beacons, tracking technology
See discussion above regarding advertising industry self-regulatory initiatives that allow a consumer to opt out of online behavioural advertising and FTC principles regarding online behavioural advertising and cross-device tracking.

"Do not track" considerations
The state of California amended CalOPPA several years ago to require that companies disclose whether they respond to browser 'do not track' signals. There is no legal requirement that companies actually respect such signals.

Consent required for behavioural advertising
There is no affirmative consent required by existing US state or federal laws for behavioural advertising.

Video and Television
As discussed above, the VPPA restricts the sharing of personally identifiable video viewing information in the absence of prior affirmative consent.

In the last couple of years, the FTC has taken action against smart TV manufacturers under its Section 5 authority to limit what it believes are unfair or deceptive practices. As part of its recent focus on the Internet of Things (IoT) and smart devices, in February 2017 the FTC, in conjunction with the Office of the New Jersey Attorney General, announced a settlement with Vizio, including payment of USD1.5 million to the FTC and USD1 million to the New Jersey Division of Consumer Affairs, with USD300,000 of that amount suspended, over claims that Vizio's smart TVs collected information about consumers' video-viewing behaviour and shared that data with third parties without sufficient notice or consent.

In 2018, California passed another new law that will require that a manufacturer of a 'connected device' equip the device with a defined minimum amount of security. 'Connected device' encompasses "any device, or other physical object" with an IP address or a Bluetooth address that can connect to the internet "directly or indirectly."

Social Media, Search Engines, Large Online Platforms
Regulatory Obligations
Please see above discussions regarding the FTC's 2014 data broker report.

Right to Be Forgotten (or of Erasure)
There is no right to be forgotten under US law. That being said, the CCPA introduces a right to deletion for California residents. A business that collects personal information about consumers must disclose the consumer's rights

to request the deletion of their personal information, and a business that receives a verifiable consumer request from a consumer to delete the consumer's personal information must delete their personal information from its records and direct any service providers to delete the personal information from their records.

A business or a service-provider is not required to comply with a consumer's request to delete their personal information if it is necessary for the business or service-provider to maintain the information in order to:

- complete the transaction for which the personal information was collected, provide goods or services requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity, or prosecute those responsible for that activity;
- debug to identify and repair errors that impair existing intended functionality;
- exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- comply with the California Electronic Communications Privacy Act;
- engage in public or peer-reviewed scientific, historical or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
- enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- comply with a legal obligation; or
- otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Addressing Hate Speech, Disinformation, Abusive Material, Political Manipulation, etc

There is little in US federal or state privacy law that addresses hate speech, disinformation, abusive material or political manipulation. These matters are usually largely addressed in the context of free speech and First Amendment law, beyond the scope of this chapter. These issues have emerged more prominently following alleged Russian interference with the 2016 presidential election, including through the use of social platforms such as Facebook.

Data portability

The CCPA is the first US law to introduce what appears to be a data portability right. It provides that a business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information. The information may be delivered by mail or electronically, and if provided electronically, the information must be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit the information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide it more than twice in a 12-month period.

Children's Privacy

COPPA requires operators of websites and online services that knowingly collect, use or disclose personal information of children under the age of 13 to allow parents the opportunity to review or restrict the personal information being collected and used. Violations of COPPA can carry hefty fines of in excess of USD40,000 per violation.

Educational or school data

The federal Family Educational Rights and Privacy Act (FERPA) protects educational records that contain information directly related to an individual student and maintained by an educational agency or institution or by a party acting for the agency or institution. There are also state student privacy laws that protect a broader scope of 'student personal information' and data that is collected and used via education technology products and services.

2.3 Online Marketing

The federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) bans false or misleading header information and prohibits deceptive subject lines. It requires that unsolicited commercial email be identified as advertising and provide recipients with a method for opting out of receiving any such email in the future.

Most states also have email subject line labelling laws and laws prohibiting false or misleading practices, which are not pre-empted by CAN-SPAM.

Please see in **1.5 Major NGOs and Self-Regulatory Organisations** discussion of advertising industry self-regulatory initiatives and FTC principles with respect to online behavioural advertising.

As discussed above, the FTC considers precise geolocation information to be sensitive information that requires affirmative express consent prior to collection. State Attorney Generals have also pushed for mobile app platforms to provide a consistent mechanism for users to consent to tracking of geolocation information. More recently, some State Attorney Generals have taken enforcement action to stop 'geo-fencing' advertising designed to target users enter-

ing a particular location of a medical office that suggests they have a particular medical condition.

2.4 Workplace Privacy

There are numerous federal and state laws that impact workplace privacy. These include:

- the FCRA and state laws that restrict the use of background checks and give individuals certain rights with respect to such checks;
- state laws that restrict the use of E-Verify;
- the federal Genetic Information Non-discrimination Act, which prohibits acquiring genetic information except in limited circumstances, and state laws that restrict collection of genetic information and testing;
- state laws that restrict or prohibit enquiry into arrest records and certain conviction records;
- state laws restricting enquiries regarding salary history;
- state laws that restrict collection of social media account credentials;
- the federal Occupational Health and Safety Act and state laws that address access to and protection of personnel files;
- HIPAA, which covers employer-sponsored health plans;
- state laws that restrict the printing of social security numbers on pay stubs;
- state laws that protect employee medical information and information about alcohol and drug rehabilitation; and
- state laws that prohibit any employer requirement to have a microchip containing a radio frequency identification device implanted in an employee's body.

US laws, including the federal Electronic Communications Privacy Act (ECPA) and Computer Fraud and Abuse Act (CFAA), generally permit monitoring of workplace communications if an employer has provided sufficient and explicit notice to individuals and made them aware that there is no right to privacy when using the employer's electronic systems. There is significant litigation under the CFAA regarding under what circumstance an employee exceeds authorised access to employer systems (sometimes in connection with that employee leaving the company).

Some states have two-party consent laws for recording of telephone conversations, which means that employees must be provided with advance notice and provide consent to such monitoring. Some states impose restrictions on audio or video recording of certain areas such as restrooms, locker rooms and other rooms designated for changing clothes.

Employees, even those who are not unionised, who post on social media, compose emails or blog about working conditions or their employer may be protected under the National Labor Relations Act. The National Labor Relations Board has taken action against employers with policies that appear to restrict this kind of activity.

The US does not have works councils.

The US does not have privacy laws that address whistleblower hotlines and anonymous reporting.

2.5 Enforcement and Litigation

Please see in **1.2 Regulators** discussions regarding the FTC's authority to take action under Section 5 and to enforce COPPA, and regarding the State Attorney General's enforcement efforts under the 'little FTC Acts.'

As discussed above, State Attorneys General have assessed penalties ranging from none or a few thousand dollars up to hundreds of millions of dollars. Where it has authority to seek fines and penalties, the FTC has assessed anywhere from zero to more than USD20 million. There is speculation that the FTC may assess a record-breaking penalty against Facebook in 2019.

In December 2018, the New York State Attorney General announced a USD4.95 million settlement with Oath Inc, the largest penalty as of that date assessed under COPPA. The NY AG found that Oath's ad exchanges transferred persistent identifiers and geolocation from website users to demand-side platform (DSP) bidders in its automated auction process. Oath did not seek verifiable parental consent, instead treating all websites (and therefore all user information) the same, despite knowledge that some website inventory on its exchange was directed to children under 13. Oath's ad exchanges also allowed advertisers to collect information on children and display ads on sites targeting children.

Over the course of 2018, the FTC entered into consent agreements with several companies for alleged misrepresentations regarding Privacy Shield certification.

The FTC entered into a consent decree with Uber Technologies, Inc over allegations that the company failed to monitor employee access to consumers' personal information on an ongoing basis and to render reasonably secure sensitive consumer data, resulting in two data security breaches. Under the final settlement, Uber could be subject to civil penalties if it fails to notify the FTC of certain future data security breaches and is prohibited from misrepresenting how it monitors internal access to consumers' personal information and the extent to which it protects the privacy, confidentiality, security and integrity of personal information. Uber, like most companies subject to an FTC consent decree, must also implement a comprehensive privacy programme and for 20 years obtain biennial independent, third-party assessments certifying that it has a privacy programme in place that meets or exceeds the requirements of the FTC order.

In September 2018, Uber reached a USD148 million nationwide settlement with the Attorney Generals of all 50 states

and the District of Columbia to resolve claims that it violated state laws protecting consumers and personal information.

Because the US has so many different federal and state laws that provide a private right of action, as discussed above, and because each statute differs as to whether it allows for statutory damages, and the amount of such statutory damages, or whether plaintiffs are limited to actual damages suffered, there is no consistent legal standard that applies to authorise private litigation. As discussed above, there is significant litigation at the federal Circuit and Supreme Court level as to what allegations of harm are necessary to establish standing in data breach cases.

Class actions are allowed in the United States if they meet the requirements of the applicable federal or state rules for class actions, beyond the scope of this chapter.

In January 2019, the Illinois Supreme Court ruled against Six Flags in a fingerprinting suit challenging the state's controversial biometric privacy law, the BIPA, discussed above. The court found that an individual need not allege actual injury or adverse effect beyond violation of rights under the BIPA in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief. The ruling may impact pending litigation under the BIPA against Google and Facebook related to facial recognition technology.

In June, the United States Supreme Court held in Carpenter v United States that a warrant is required for police to access cell site location information, ie, the detailed geolocation information generated by a cell phone's communication with cell towers.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

In the United States, the Fourth Amendment to the Constitution restrains the government when it seizes or searches persons or property. It also provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." There is a huge body of case law in the country addressing the question of what is a 'search' and when a warrant is required.

ECPA provides for certain law enforcement access to data. Under the Stored Communications Act portion of ECPA, the government is able to access many kinds of stored communications without a warrant. Emails in transit or in storage on a home computer, and emails in remote storage that are unopened for fewer than 180 days, require a warrant, but opened emails in remote storage and emails in remote storage, unopened for more than 180 days, require only a subpoena.

The government can also serve a National Security Letter (NSL) on a communications company to obtain basic subscriber information. The information sought will determine whether a court order is required. The standard for a court order is less than the probable cause required for a warrant.

ECPA also allows a service-provider to share customer records in an emergency involving immediate danger of death or serious physical injury to any person.

Whether agencies can authorise unilaterally or will require independent judicial or approval and what safeguards protect privacy by law and in practice must be determined according to the above discussions.

3.2 Laws and Standards for Access to Data for National Security Purposes

The Foreign Intelligence Surveillance Act (FISA), reauthorised in early 2018, allows the government to obtain access to communications of non-US persons outside the US without a court order or warrant, but only with the approval of a FISA court.

In March 2018, the President signed the CLOUD Act, which requires internet companies to hand over personal data to US law enforcement agencies regardless of where the data is stored. The Act also allows the executive branch of the US government to create agreements with foreign countries to provide direct access to personal data stored in the US.

Whether agencies can authorise unilaterally or require independent judicial or approval and what safeguards protect privacy by law and in practice are decided on the basis of the above discussion of FISA and the Cloud Act.

3.3 Invoking a Foreign Government

Whether a foreign government may lawfully seek personal information from a US company will depend on the legal process used and whether that foreign government has jurisdiction over the US company by virtue of the company's operations vis-à-vis the country in question.

3.4 Key Privacy Issues, Conflicts and Public Debates

Government access to personal information has been a highly controversial and hotly litigated topic for many years, but especially since the Edward Snowden revelations in 2013. Government access to data has also heightened tensions with Europe and created compliance challenges for organisations seeking to transfer personal information from the EU to the US.

4. International Considerations

4.1 Restrictions on International Data Issues
As discussed above, the US is considered an inadequate country by the European Union for purposes of privacy protection.

4.2 Mechanisms That Apply to International Data Transfers
As discussed, organisations may self-certify to the Privacy Shield Framework in order to transfer HR or non-HR personal information from the EU to the US.

4.3 Government Notifications and Approvals
See above discussion of the Privacy Shield. There are no laws restricting the transfer of personal information of individuals located in the US outside of the US.

4.4 Data Localisation Requirements
The US does not have any data localisation requirements.

4.5 Sharing Technical Details
There are no laws that require an organisation to share software code, algorithms or similar technical details with the government in the absence of limited circumstances involving investigation of crimes or national security issues. There is ongoing litigation under the Fourth and Fifth Amendments as to whether a court can compel an individual to turn over passwords or even encryption keys in connection with a search in the absence of a warrant. It may depend on whether a search is conducted at the border.

4.6 Limitations and Considerations
The US does not have blocking statutes. Whether an organisation is compelled to turn over information to a foreign government will depend on the legal process used and whether the foreign government has jurisdiction over the company.

4.7 "Blocking" Statutes
The US does not have any blocking statutes.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law
For Big Data analytics, automated decision-making, profiling, facial recognition, and biometric privacy laws, discussions of the advertising industry's self-regulatory initiatives and FTC principles for online behavioural advertising, see section **2. Fundamental Laws**.

Artificial intelligence (including machine learning) is regulated, if at all, only to the extent it is covered by laws addressed elsewhere in this chapter, either by virtue of being covered by a sectoral law, a state law or one that covers a particular type of information (eg, children) or technology (eg, IoT), in particular the new California law.

Autonomous decision-making (including autonomous vehicles) and related privacy issues have been the subject of Congressional inquiry, but are not specifically regulated at this time beyond the other IoT and related Big Data guidance and laws described above. The CCPA, also discussed above, will also likely have implications for autonomous vehicles.

Drones
California prohibits, among other things, using a drone to capture pictures or video, even if the drone does not physically trespass on property. It is also a violation for a person to transmit, publish or broadcast footage, if the person knows the content was created in violation of the law. Under Texas law, it is an offence to use a drone to capture an image of an individual or privately owned real property "with the intent to conduct surveillance" without the consent of the individual or the owner/occupant. There are similar laws in Florida.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators
Laws that apply to data, systems, infrastructure, etc
There are a number of federal and state laws that require organisations to implement certain physical, administrative and technical safeguards to protect personal information. These include the GLBA and the New York Department of Financial Services (NYDFS) Cybersecurity Regulations for financial institutions, and HIPAA for covered healthcare entities. They also include state laws that broadly cover all industries such as the Massachusetts Standards for the Protection of Personal Information, the Nevada law requiring encryption of electronic transmissions outside of the secure system of the business and on portable devices, Ohio's Data Protection Act and Oregon law.

Outside of the regulated industries, the FTC and the State Attorneys General are the lead regulators enforcing cybersecurity laws.

At the federal level, for non-regulated entities, the FTC is the primary enforcement agency with respect to cybersecurity.

There is no distinction in the United States between data protection authorities and privacy regulators, on the one hand, and cybersecurity regulators on the other.

The CFPB and the FTC are the GLBA regulators for data security, and the NYDFS regulates entities under its jurisdiction.

6.2 Key Frameworks

Numerous security frameworks have been adopted by the private sector. Most prevalent is the Payment Card Industry Data Security Standard (PCI-DSS), a contractual standard to which any merchants that process payment card information must adhere or risk losing the ability to process cards and penalties.

Other commonly adopted frameworks include the ISO 27000 series and NIST. These standards are not incorporated into US legal requirements. However, the California Attorney General cited the Center for Internet Security (CIS) 20 Controls as a baseline for what constitutes 'reasonable security' in her 2016 annual data breach report.

6.3 Legal Requirements

As previously discussed, the GLBA and the Massachusetts Information Security Regulations require the implementation and maintenance of a written information security programme. In addition, the new Vermont data broker law requires the development, implementation and maintenance of a written, comprehensive information security programme that contains appropriate physical, technical and administrative safeguards designed to protect consumers' personal information. The NYDFS Regulations have similar requirements.

While incident response plans are not mandated by law, they are highly recommended as best practice across industries and largely required by cyber-insurance carriers of their policyholders. They also greatly assist in risk-mitigation with respect to application of data security breach notification laws.

HIPAA and the NYDFS Regulations are the only laws that currently require the appointment of a chief information security officer (CISO) or equivalent. However, most large US organisations have a CISO or equivalent to help mitigate risk and address incident response.

The NYDFS Cyber Regulations require implementation and maintenance of a written policy approved by a senior officer or the covered entity's board of directors, and require that the CISO report in writing at least annually to the covered entity's board of directors or equivalent governing body.

The Securities and Exchange Commission (SEC) has started to investigate cybersecurity matters actively as well, heightening the need for Board education and involvement.

6.4 Key Affirmative Security Requirements

The laws and regulations previously described generally require organisations to implement certain physical, administrative and technical safeguards to protect personal information. Some regulations, like those of Massachusetts and Nevada, are more specific in requiring controls such as encryption for certain kinds of personal information in transit over the public internet or wi-fi or stored on mobile or portable media or devices.

US federal and state privacy laws do not address business data. The requirements for securing business networks and systems are all connected to the protection of personal information.

In 2013, President Obama issued Presidential Policy Directive 21 encouraging measures to strengthen the cybersecurity of critical infrastructure. NIST has issued guidelines and the energy industry has engaged in self-regulatory initiatives.

US federal and state privacy and data security laws do not specifically address denial of service attacks or similar attacks on system or data availability or integrity that do not impact personal information.

6.5 Data Breach Reporting and Notification

Defining a potentially reportable data security incident or breach

Under many of the 50 state laws, notice must be sent to individuals whose unencrypted personal information (some states limit this to computerised information, others cover data in all forms) was, or is reasonably believed to have been, acquired by an unauthorised person when the security of unencrypted consumer information has been compromised. Some states, however, have a risk-of-harm threshold for determining whether notification of affected individuals and/or regulators is required. In the US, the risk-of-harm test is often whether a reasonable or good faith investigation determines that the misuse of personal information has occurred or is reasonably likely to occur. Thus, in those states, notice obligations are not triggered unless there is, at a minimum, a reasonable basis for believing that misuse is likely to occur.

Under HIPAA, acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under HIPAA is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised, based on a risk assessment considering, at least:

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- the unauthorised person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.

Data elements covered
Depending on the state or territory involved, certain data elements may, alone or in combination, trigger a notification requirement, including:

- a user name, unique identifier or number, email address, or routing code, in combination with a password or security question and answer, that would permit access to an online account;
- even without a user name or email address, a password, security code, other access code, account number or any other number or code or combination of numbers or codes, shared secrets or security tokens, or other information, that allow access to financial accounts, credit accounts and/or other kinds of accounts;
- a standalone PIN;
- a financial account number;
- a credit or debit card number;
- a social security number (even a partial number if more than four digits in some states);
- information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional;
- a medical identification number;
- a health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records;
- a unique identification number created or collected by a government body or regulatory entity, including driver's licence numbers or authorisation numbers or cards, passport numbers, taxpayer identification numbers, voter's identification, tribal identification numbers or cards, alien registration numbers, and identity protection personal identification numbers issued by the IRS;
- data from measurements or analysis of a consumer's physical characteristics or human body characteristics, sometimes called unique biometric data (such as fingerprint, voice print, retina or iris image);
- DNA profile;
- digitised or other electronic signature;
- information or data collected through the use or operation of an automated licence plate recognition system;
- birth or marriage certificate;
- date of birth;
- mother's maiden name;
- employer-assigned ID in combination with any required security code, access code or password;
- tax information; and/or
- work-related evaluations.

Under HIPAA, PHI is notice-triggering.

Systems covered
The laws are not specific as to the kinds of systems covered. Some cover electronic only, while others cover paper.

Security requirements that apply to medical devices
The federal Food and Drug Administration (FDA) has issued guidelines for manufacturers to consider cybersecurity risks as part of their medical device design and development.

Security requirements that apply to Industrial Control Systems (and SCADA) and IoT
NIST has issued standards for the security of industrial control systems and SCADA. There are also self-regulatory initiatives. For IoT, see discussion of the new California IoT law above.

Criteria that trigger reporting to government authorities
Many states now require notification to government regulators in the event that notification must be made to individuals. Some states only require notification to government regulators if a security breach impacts more than a certain number of individuals. States and territories that now require regulator notice for non-regulated private entities reporting a data security breach include Alabama, Arizona, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Puerto Rico, Rhode Island, South Carolina, South Dakota, Vermont, Virginia, and Washington.

HIPAA requires notification to the HHS and potentially other federal health regulators.

Criteria that trigger reporting to individuals
See discussion above regarding the general test for triggering a breach notification obligation to individuals.

Criteria that trigger reporting to other companies or organisations
Companies that maintain information on behalf of a data owner must generally notify the data owner. Similarly, under HIPAA, business associates must notify covered entities.

HIPAA requires media notice for data security breaches involving more than 500 individuals.

6.6 Ability to Monitor Networks for Cybersecurity
US law does not specifically address permitted or restricted practices and tools for network monitoring and other cybersecurity defensive measures, provided that those measures do not violate other laws such as the CFAA or criminal laws. Law enforcement has warned the private sector against attempts to 'hack back.'

6.7 Cyberthreat Information Sharing Arrangements

See discussion of required disclosures to state regulators and the HHS in **6.5 Data Breach Reporting and Notification**.

The Federal Bureau of Investigation (FBI) strongly encourages any company that is the victim of a cybersecurity incident to share information with it to assist in its efforts to apprehend those that hack or otherwise compromise corporate systems.

6.8 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

Significant audits, investigations or penalties imposed for alleged cybersecurity violations or data security incidents or breaches

See above discussion of the FTC's Uber investigation and consent decree and of Uber's settlement for USD148 million with the State Attorney General. In addition, in June, Equifax entered into a consent order with eight state banking regulators related to the company's 2017 data breach involving 143 million consumers.

HHS continues to investigate actively breaches reported under HIPAA.

For significant private litigation involving cybersecurity allegations or data security incident or breaches, see above discussion of the split in federal Circuit Court authority on standings in data-breach class actions, and the pending Zappos petition for a writ of certiorari.

Frankfurt Kurnit Klein & Selz

2029 Century Park East,
Suite 1060,
Los Angeles,
CA 90067

Frankfurt Kurnit Klein + Selz PC

Tel: +1 310 579 9615
Fax: +1 347 438 2092
Email: tforsheit@fkks.com
Web: www.fkks.com