

# Data Security & Cybercrime

## Jurisdiction snapshot

Trends and climate

**Would you consider your national data protection laws to be ahead or behind of the international curve?**

USA

**Sidley Austin LLP**

The US legal regime is considered one of the most established regimes for modern privacy and data protection rights. It has been a leader in the formulation of fair information practice principles and has some of the most robust legal protections and obligations, such as those for data breach notifications and the significant consequences for certain privacy violations. The Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), Federal Communications Commission (FCC), Department of Health and Human Services/Office for Civil Rights, Securities and Exchange Commission (SEC) and several other federal agencies have enforcement jurisdiction, as do the state attorneys general and insurance commissioners. Private parties have long been able to hold companies accountable through class actions, and some statutes specify statutory damages (eg, \$500 fines per text for unauthorised use of text messaging for marketing purposes under the Telephone Consumer Protection Act).

However, many of the international data protection law trends are modelled on the more omnibus EU data protection legal regime based on the EU Data Protection Directive (95/46/EC). The US system is not identical to the EU system because, as a common law country, the United States has developed a multidimensional, sector-sensitive system of federal and state laws and jurisprudence, rather than a single omnibus law comparable to the EU Data Protection Directive (read in light of the EU Charter of Fundamental Rights).

Nevertheless, the US body of laws is consistent with the international curve. For example, it ensures that government access to data for law enforcement and intelligence purposes is limited to what is necessary and proportionate. In addition, it governs the private sector and impels it to adopt strong privacy practices that – particularly when reinforced by legally binding commitments – correspond to the principles of the EU Data Protection Directive. Taken together, the practical effect of these laws and practices is to provide a level of data protection that is essentially equivalent to the legal order in the European Union, although the United States has yet to be granted an equivalency status from the European Union.

One difference that merits mention is the robust sense in which the Constitution protects privacy by limiting governmental intrusions. The Fourth Amendment protects citizens from unreasonable governmental searches and seizures since the ratification of the Constitution. Similarly, the First Amendment robustly protects free speech in the United States, which includes speech through the processing of data. Certain governmental restrictions on private free speech are allowed in particular circumstances; however, these restrictions must often be tied to significant governmental interests and tailored to advance these interests.

[Back to top](#)

**Are any changes to existing data protection legislation proposed or expected in the near future?**

USA

**Sidley Austin LLP**

Privacy and data protection legislation is constantly and frequently debated and pending in both state and federal legislatures. Reform of the Electronic Communications Privacy Act is likely to be adopted in 2016. This proposed law, which has passed one chamber of Congress, would require a search warrant for emails and stored electronic communications – regardless of how long the electronic material has been stored. The FCC has proposed extensive and strict new privacy regulations for internet service providers, which are currently the subject of a notice and comment period before any final adoption. Far-reaching reforms to the structure of US privacy law, such as a consumer privacy bill of rights proposed by the Obama administration in 2014, has yet to gain much momentum. However, the states have historically served as a testing ground for and source of policy evolution, particularly for privacy and data protection laws. Some jurisdictions are more influential in this area than others (eg, California, Connecticut, Florida, Illinois and Massachusetts). For instance, state laws already address aspects of data from the Internet of Things. However, state and federal legislation, as well as regulation and policy statements from federal regulators including the FTC, FCC, SEC, CFPB and several others, drive the evolution of data protection obligations in the United States and should be regularly

## Contributors

USA



**Alan Charles Raul**  
Sidley Austin LLP

[Legal updates](#)

USA



**Anna L. Spencer**  
Sidley Austin LLP

[Legal updates](#)

USA



**Colleen Theresa Brown**  
Sidley Austin LLP

[Legal updates](#)

USA



**Edward R. McNicholas**  
Sidley Austin LLP

[Legal updates](#)

# Legal framework

## Legislation

### What legislation governs the collection, storage and use of personal data?

USA

#### Sidley Austin LLP

US federal and state privacy laws, regulations, common law and privacy practices establish a comprehensive privacy regime that governs the collection, storage and use of personal data. The most sensitive data – such as financial, medical, health, electronic communications and children’s information – are protected by nearly two dozen federal sector-specific laws and numerous state laws, resulting in a reinforcing web of hundreds of potentially relevant statutes, not to mention regulations and sometimes binding industry standards.

This complex body of law includes:

- the Electronic Communications Privacy Act – governs electronic communications (18 USC § 2510 and following);
- the privacy provisions of the Communications Act – govern personal information maintained by telecoms providers (47 USC § 222);
- the Computer Fraud and Abuse Act – protects against computer crimes;
- the Children’s Online Privacy Protection Act (COPPA) – governs the collection of personal data from children online and parental notice and consent (47 USC § 227 and following);
- the Family Educational Rights and Privacy Act – governs educational records;
- the Fair Credit Reporting Act – governs consumer reports, including those used to make critical eligibility determinations (15 USC § 1681, and following);
- the privacy and security provisions (Title V) of the Gramm-Leach-Bliley Act – govern financial information (15 USC §§ 6801–6809);
- the privacy and security provisions of and regulations issued pursuant to the Health Insurance Portability and Accountability Act – govern health and insurance information (Pub L 104–19 §§ 262, 264; 42 USC §§ 1320d–1320d-9; 45 CFR Parts 160 and 164); and
- the Genetic Information Non-Discrimination Act – governs genetic information (Pub L 110–233, 122 Stat 881 (2008) codified at 42 USC § 2000ff).

In addition, 47 of the 50 US states, plus several non-state entities, enforce varied broad data security and data breach notification laws that affect the storage of sensitive personal data.

These specific laws are backstopped by the broad reach of the Federal Trade Commission (FTC), which is the lead privacy enforcement agency in the United States. The FTC protects consumers from unfair and deceptive acts and regulates a broad range of activity involving data processing. State attorneys general act in a similar function.

Enforcement by the FTC and by other public and private actors is authorised by:

- Section 5 of the Federal Trade Commission Act (prohibits unfair or deceptive business practices and enforces principles of notice and choice and reasonable information security practices);
- state ‘little FTC acts’; or
- state unfair, deceptive or abusive acts and practices statutes (prohibits unfair or deceptive acts and practices).

Finally, negligence or privacy torts under state law (including causes of action to recover for public disclosures of private facts and intrusions on seclusion) serve as additional legal considerations for the collection, storage and use of personal data in the United States. Although it is difficult to categorise the effect of these statutes, the potential for their enforcement by class actions and the assessment of punitive damages, above and beyond any actual damages, can prove to be a significant deterrent.

## Scope and jurisdiction

### Who falls within the scope of the legislation?

USA

#### Sidley Austin LLP

Generally, privacy and data protection obligations can apply to any entity that collects, processes or otherwise maintains personal information in any context. The sectoral approach of many privacy and data protection laws within the United

States means that there are specific categories of entities and sensitive information subject to those sector specific laws – although these often extend to other entities that receive information from those specific entities. For example, privacy and data protection obligations for protected health information under the Health Insurance Portability and Accountability Act (HIPAA) apply to HIPAA-covered entities and their business associates. Privacy and data protection obligations for non-public personal financial information under the Gramm-Leach-Bliley Act apply to financial institutions. Some laws apply depending on the activity entities are engaged in, such as COPPA, which applies to the collection of personal information online from children under 13 years old.

[Back to top](#)

**What kind of data falls within the scope of the legislation?**

USA

**Sidley Austin LLP**

The types of personal information covered by various privacy and data protection laws in the United States is more specific and driven by categories and context than the more amorphous definition of ‘personal data’ in the European Union. For example, under state data breach notification laws, ‘personal information’ is defined as a name, plus an additional category of information that may subject an individual to fraud or similar harms, such as:

- social security numbers;
- financial account information;
- drivers’ licence numbers;
- medical or health information;
- biometric data; and
- increasingly, online account credentials.

The sector-specific privacy laws cover personal information when collected in a specific context. For example, the Gramm-Leach-Bliley Act covers non-public personal financial information collected in the context of providing financial services. HIPAA covers individually identifiable health information held or transmitted by a covered entity (eg, a healthcare provider or healthcare plan or healthcare clearinghouse) or its business associates, in any form or medium, whether electronic, on paper or oral. However, there are also areas of law in the United States that cover personal (or otherwise private) information in a much broader way, such as where individuals have a reasonable expectation of privacy that can be vindicated through tort law or data subject to consumer privacy protections enforced by the FTC or state attorneys general.

[Back to top](#)

**Are data owners required to register with the relevant authority before processing data?**

USA

**Sidley Austin LLP**

There are no general data processing registration requirements; indeed, a blanket requirement for registration with the government before collecting or processing personal data would be at least constitutionally suspect.

[Back to top](#)

**Is information regarding registered data owners publicly available?**

USA

**Sidley Austin LLP**

Not in general. Several voluntary privacy or data protection-related certifications, frameworks or industry standards contribute to the US legal order for data protection and many of these provide public lists of participating companies. One such framework includes the safe harbour programme through the US Department of Commerce. A list of participating companies is available at <https://safeharbor.export.gov/list.aspx>. While the safe harbour programme was invalidated as a means to legitimise data transfers from the European Union to the United States, it is still a valid framework under US law and any successor programme would likely include a publically searchable database to identify participating companies.

[Back to top](#)

**Is there a requirement to appoint a data protection officer?**

USA

**Sidley Austin LLP**

Not in general. However, HIPAA-covered entities and business associates must appoint both a privacy and security officer for HIPAA compliance, and some other similar appointment requirements exist in particular areas.

[Back to top](#)

Enforcement

Which body is responsible for enforcing data protection legislation and what are its powers?

USA

Sidley Austin LLP

Companies that disregard the US privacy and data protection regime will face penalties on multiple, simultaneous fronts. US privacy and data protection laws are enforced by federal regulatory agencies, federal prosecutors, state attorneys general and other state regulators. In addition to the Federal Trade Commission (FTC), federal enforcers are found in an expanding network of agencies with sector-specific expertise, as well as in the Department of Justice. Beyond federal powers, state law may afford data subjects regulatory protection and causes of action for legal redress. Many states have created formal units charged with privacy oversight. State attorneys general often cooperate in joint enforcement actions against companies that experience data breaches or violate consumer privacy rights. Class action suits also form a significant enforcement mechanism. Coordinated and comprehensive privacy regulations combined with active enforcement and sizable fines establish a strong deterrent to motivate compliance with US privacy and security requirements.

[Back to top](#)

Collection and storage of data

Collection and management

In what circumstances can personal data be collected, stored and processed?

USA

Sidley Austin LLP

The standards for data collection, storage and processing vary between the many privacy and data protection laws. That said, a common theme is that personal data can be collected, stored and processed as long as the data subject has adequate notice of the collection, storage and processing, as appropriate to the sensitivity of the data.

[Back to top](#)

Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?

USA

Sidley Austin LLP

Although record retention obligations arise from other sources of law, no general limitations or restrictions on data retention from US privacy or data protection laws exist. However, guidance on fair information practices provides that the retention should be appropriate to the purposes for which the data was collected or otherwise harmonious with the notice provided to data subjects. At a minimum, if retention would violate privacy commitments made to data subjects (eg, from a privacy policy) that would be a deceptive business practice and thus prohibited.

[Back to top](#)

Do individuals have a right to access personal information about them that is held by an organisation?

USA

Sidley Austin LLP

Generally, the right to access and correct personal information is encouraged as a fair information principle, but there is no general legal obligation to provide a right of access. However, a number of sector-specific data protection laws (eg, the Fair Credit Reporting Act, the Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA)) include such a right. The rights of access in the Fair Credit Reporting Act are particularly robust and likely inspired other international access rights.

[Back to top](#)

Do individuals have a right to request deletion of their data?

USA

Sidley Austin LLP

The Fair Credit Reporting Act and certain state laws that are similar to the act provide a right to dispute inaccurate or out of date information, and certain types of information (eg, late payments) must be removed from consumer credit reports after specified periods. COPPA permits parents to request the deletion of data regarding their children under 13 years old, and a California state law for minor’s online data (Cal Bus and Prof Code 22580-81) provides a right to request the removal of content or information posted online by a minor. Outside these limited contexts, no general right to request deletion or to be forgotten exists for accurate data in the United States. Indeed, a general governmental obligation to require someone to delete accurate records would likely raise First Amendment free speech issues under the federal and state constitutions.

[Back to top](#)

Consent obligations

Is consent required before processing personal data?

USA

Sidley Austin LLP

Depending on the sensitivity of the data, or prior data protection commitments made to data subjects, consent may be required before processing personal data. For example, in its March 2012 report Protecting Consumer Privacy in an Era of Rapid Change, the Federal Trade Commission (FTC) stated that “Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes”. In this report, the FTC provided examples of sensitive data such as:

- children’s data;
- financial and health information;
- social security numbers; and
- certain geolocation data.

In addition, sector-specific privacy and data protection laws may have specific consent requirements. For instance, under HIPAA, patient authorisation is required to process protected health information except as specifically permitted or required by HIPAA. For example, only with consent can covered healthcare providers use and disclose protected health information to treat an individual or seek payment for the provision of healthcare services. Other exceptions that further important public policy objectives (eg, public health activities) allow the processing of protected health information in the absence of consent only if certain safeguards are present or requirements are met. Consent may be required to share certain non-public personal financial information with unaffiliated third parties under the Gramm-Leach-Bliley Act. Parental consent is required before collecting and processing personal information online from children under COPPA. Consent is also required for some uses of customer data under the Communications Act. That said, no general requirement to obtain consent exists.

[Back to top](#)

If consent is not provided, are there other circumstances in which data processing is permitted?

USA

Sidley Austin LLP

No general statute requires data subjects’ consent before processing personal data, and so data processing is permitted whenever it is not restricted. The FTC has recognised that even where explicit consent is unnecessary, it might still be required under the circumstances. In general, privacy policies are used in the United States as a form of implied consent, particularly in the online context, as policies frequently make access and use of a website or online service constitute acceptance of an online privacy policy. Certain data processing may also be performed even without the data subject’s consent – for example, in order to comply with legal requirements or processes such as a subpoena, court order or regulatory reporting process.

[Back to top](#)

What information must be provided to individuals when personal data is collected?

USA

Sidley Austin LLP

When notice is required, content may be specified under certain sector-specific privacy and data protection laws. For example, HIPAA regulates the content of privacy practices notices in the healthcare context. The Gramm-Leach-Bliley Act requires regular notice of privacy practices, and certain regulators have issued model form notices. State laws may also specify the content of privacy policies, in particular for online or mobile privacy policies such as under the California Online Privacy Protection Act (Cal Bus and Prof Code § 22575 and following) or the more recent Delaware Online Privacy and Protection Act at Title 6 of the Delaware Code.

[Back to top](#)

## Data security and breach notification

### Security obligations

#### Are there specific security obligations that must be complied with?

USA

#### Sidley Austin LLP

Several sector-specific privacy and data protection laws provide for information security obligations. Almost all US states enforce broad data security and data breach notification laws that apply to sensitive personal data. About two-thirds of the states have legislation that requires companies to implement reasonable information security measures, at least in the disposal context. Data security laws also generally require companies holding certain personal information about state residents to:

- implement and maintain reasonable security procedures and practices in order to protect information from unauthorised access, destruction, use, modification or disclosure;
- take reasonable steps to destroy personal information that is no longer to be retained or to make it otherwise unreadable or undecipherable; and
- contractually require third parties to which the company discloses personal information to maintain reasonable security procedures (see, for example, Cal Civ Code § 1798.81.5 (2007); Md Code Ann, Com Law § 14-3503).

Some states impose more rigorous information security requirements. For instance, Massachusetts requires entities to develop and implement a written comprehensive information security programme (see 201 Mass Code Regs § 17.02). The regulation requires employee training, adoption of encryption standards and regular monitoring and establishes requirements for securing computer systems (*id* §§ 17.03–17.04). These requirements are passed through to third-party vendors engaging in business with entities subject to the regulation (*id* § 17.03(2)(f)). These requirements include:

- taking reasonable steps to select and retain third-party service providers capable of maintaining appropriate security measures; and
- requiring that the third-party service providers implement and maintain appropriate security measures by contract for any personal information or data.

[Back to top](#)

### Breach notification

#### Are data owners/processors required to notify individuals in the event of a breach?

USA

#### Sidley Austin LLP

Data breach notification laws in 47 states require corporate and government entities to take particular actions in the event of a data security breach or suspected breach (see, for example, 815 Ill Comp Stat 530/5, 530/10; NY Gen Bus Law § 899-AA; Tenn Code Ann § 47-18-2107; Tex Bus and Com Code § 521.053). Once the notification threshold has been met, which varies by state, entities must notify state residents whose personal information has been affected by the breach. Some states require notification of any unauthorised access to or acquisition of covered personal data, although most require such notifications only when there is risk of a harm, such as identity theft. As a rule, notification must be provided by the entity that owns the data, which is generally the entity that collected the data from the data subject. The breach laws generally require service providers (or data processors) that merely process data on another entities' behalf to provide notice to the data owner, and for the data owner to then fulfil the notification obligations under state law. As state data breach notification laws apply based on the state of residence of the affected data subject, it is not unusual for a data breach to implicate multiple and varying state data breach notification standards and requirements.

[Back to top](#)

Are data owners/processors required to notify the regulator in the event of a breach?

USA

Sidley Austin LLP

Notice to law enforcement, consumer reporting agencies, and the state attorney general or other regulators also may be required where the state data breach notification law has been triggered. A small minority of states, including Florida, also require notification to a regulator in the event of a breach when the entity determines that notification of a data breach to the data subjects is not required under the law pursuant to an analysis that the incident has not exceeded a risk of harm threshold.

[Back to top](#)

Electronic marketing and internet use

Electronic marketing

Are there rules specifically governing unsolicited electronic marketing (spam)?

USA

Sidley Austin LLP

Yes. The Controlling the Assault of Non-Solicited Pornography and Marketing Act protects individuals against unsolicited commercial electronic communications and includes specific requirements for commercial emails (15 USC §§ 7701–7713). Beyond spam emails, the Telephone Consumer Protection Act is a critical law, as it protects against unwanted marketing and guards individuals against unwanted or harassing telemarketing and other communications made by autodialers, pre-recorded messages, text messages or faxes (47 USC § 227 and following). The Telephone Consumer Protection Act, which has a private right of action, is the source of many class actions and significant potential liability because its damages are set by statute on a per call, fax or text basis.

[Back to top](#)

Cookies

Are there rules governing the use of cookies?

USA

Sidley Austin LLP

Online tracking must be properly disclosed pursuant to California tracking disclosure requirements. Likewise, general privacy standards for notice and prohibitions on deceptive or unfair business practices forbid unfair or deceptive use of cookies. Generally, however, no specific regulations govern the use of cookies.

[Back to top](#)

Data transfer and third parties

Cross-border data transfer

What rules govern the transfer of data outside your jurisdiction?

USA

Sidley Austin LLP

Consistent with the national commitment to free and fair trade, no specific rules govern the transfer of data outside of the United States, beyond the basic fair information principles for notice and prohibitions on deceptive or unfair business practices that may apply to any processing or disclosures of data inside or outside of the country.

[Back to top](#)

Are there restrictions on the geographic transfer of data?

USA

Sidley Austin LLP



Generally, no.

[Back to top](#)

Third parties

**Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?**

USA

**Sidley Austin LLP**

On a practical level, written agreements with third-party vendors are either required or highly recommended. Depending on the context and nature of the data, data owners may be required to execute agreements (eg, a business associate agreement under the Health Insurance Portability and Accountability Act) or otherwise exercise oversight for third parties to which they transfer personal data for processing. For example, under the Massachusetts information security regulations (201 Mass Code Regs § 17.02), requirements must be passed to third-party vendors engaging in business with entities subject to the regulation (*id* § 17.03(2)(f)). Similarly, banking institutions regulated under the Gramm-Leach-Bliley Act must impose contractual data security obligations on their vendors and service providers. Moreover, companies must take reasonable steps to select and retain third-party service providers capable of maintaining appropriate security measures, and must contractually require that the third-party service providers implement and maintain appropriate security measures for any personal information or data. Further, companies are often held responsible for the information practices and, in particular, the information security practices of the service providers or vendors which they select to process personal information.

[Back to top](#)

Penalties and compensation

Penalties

**What are the potential penalties for non-compliance with data protection provisions?**

USA

**Sidley Austin LLP**

Potential penalties can be significant. Federal and state privacy laws are enforced by an expanding network of federal regulatory agencies, federal prosecutors, state attorneys general, other state regulators and private plaintiffs. Many states have created formal units charged with privacy oversight, and state attorneys general often cooperate in joint enforcement actions against companies that experience data breaches or privacy violations. In the United States, coordinated and comprehensive privacy regulation combined with active enforcement and sizable fines establish a strong deterrent to motivate compliance with US privacy and security requirements.

[Back to top](#)

Compensation

**Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with data protection provisions by the data owner?**

USA

**Sidley Austin LLP**

The availability of a private cause of action to enforce rights is a question that can be answered only with respect to each statute. That said, class actions in the wake of data breaches are common in the United States. The theories of liability vary widely, although they are generally based on common law theories of negligence and occasional contractual claims. One common challenge for data breach plaintiffs is that federal constitutional law allows courts to exercise their jurisdiction only when plaintiffs have standing based on concrete injury. Therefore, in litigation that does not involve specific demonstrable pecuniary or other concrete harm, plaintiffs may not be able to pursue their speculative claims. However, some courts have been willing to recognise standing for data breach class actions.

[Back to top](#)



# Cybersecurity

## Cybersecurity legislation, regulation and enforcement

### Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

USA

#### Sidley Austin LLP

The federal Computer Fraud and Abuse Act (18 USC § 1030 and following), the federal Identity Theft and Assumption Deterrence Act 1988 (*id* §§ 1028, 1028A), the Cybersecurity Act 2015 and multiple state laws criminalise unauthorised access of computer systems and identity theft (eg, Cal Penal Code § 368, Crimes against elders, dependent adults and persons with disabilities). These laws impose punishments such as incarceration, forfeiture, restitution and payment of attorneys' fees to the victim. The Cybersecurity Information Sharing Act, adopted in 2015, facilitates the sharing of cyberthreat indicators between the government and private companies and also enhances companies' ability to engage in network monitoring and other defensive measures.

Multiple laws cover general cybersecurity requirements.

[Back to top](#)

### What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?

USA

#### Sidley Austin LLP

A cybersecurity framework developed by the National Institute of Standards and Technology has become a significant consideration for US companies developing information security programmes. Additionally, for entities involved in payment processing, the Payment Card Industry Data Security Standards are a significant source of particular information security requirements and are generally enforced through contractual obligations. Compliance with the standards is required by some state laws.

[Back to top](#)

### Which cyber activities are criminalised in your jurisdiction?

USA

#### Sidley Austin LLP

Generally, computer crimes that cause damage to protected networks or computers may violate computer crime laws (eg, the Computer Fraud and Abuse Act). Cyber activities that implicate identity theft, theft of trade secrets or other similar prohibited activities are subject to similar criminal penalties.

[Back to top](#)

### Which authorities are responsible for enforcing cybersecurity rules?

USA

#### Sidley Austin LLP

Multiple regulatory authorities are taking ownership over cybersecurity matters within their sector-specific or otherwise jurisdictional expertise, including the Federal Trade Commission, the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau, the Commodities Futures Trade Commission, the Department of Homeland Security, the Department of Defence, the Department of Health and Human Services, the Food and Drug Administration, the Commerce Department, the Department of Transportation and state authorities, including state attorneys general and state insurance commissions.

[Back to top](#)

## Cybersecurity best practice and reporting

### Can companies obtain insurance for cybersecurity breaches and is it common to do so?

**Sidley Austin LLP**

Cybersecurity insurance is becoming increasingly favoured as one piece in a company's larger cybersecurity preparedness, although the insurance and re-insurance markets for such coverage are still developing. It is common to see companies with coverage, although many – and perhaps most – companies do not have such coverage.

[Back to top](#)**Are companies required to keep records of cybercrime threats, attacks and breaches?****Sidley Austin LLP**

Adequate recordkeeping could be considered an indirect legal requirement. Reasonable information security practices incentivise industry standard logging of cyberthreats and intrusions. Further, incident response plans should ideally provide for recordkeeping of information security incidents. Finally, considering that many data breaches can result in litigation against the company, many data breaches represent an event that is worthy of an internal litigation hold to preserve potentially relevant evidence for the resolution of legal claims.

[Back to top](#)**Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?****Sidley Austin LLP**

State data breach laws, and certain federal breach standards, require reporting of cybercrimes affecting personal information to certain state and federal regulators. Cooperation with law enforcement is also generally favoured in the wake of a data breach. Further, legislation passed in December 2015 provides incentives for private-public sharing of cyberthreat indicators and other information sharing (Cybersecurity Act 2015, Pub L No 114–113, Division N, § 104(d)).

[Back to top](#)**Are companies required to report cybercrime threats, attacks and breaches publicly?****Sidley Austin LLP**

No general requirement to report cybercrime exists outside of cybersecurity events that impact personal information or in certain sectors (eg, certain national defence systems or under certain government contracts). With respect to crimes involving personal data, multiple data breach notification requirements exist but vary from state breach notification laws to sector-specific notification laws that require notification to affected data subjects or state or federal regulators. These notifications frequently result in public reports of cybersecurity incidents.

[Back to top](#)**Criminal sanctions and penalties****What are the potential criminal sanctions for cybercrime?****Sidley Austin LLP**

The federal Computer Fraud and Abuse Act (18 USC § 1030 and following), the federal Identity Theft and Assumption Deterrence Act 1988 (*id* §§ 1028, 1028A) and multiple state laws criminalise unauthorised access of computer systems and identity theft (eg, Cal Penal Code § 368, Crimes against elders, dependent adults and persons with disabilities). These laws impose punishments such as incarceration, forfeiture, restitution and payment of attorneys' fees to the victim.

[Back to top](#)**What penalties may be imposed for failure to comply with cybersecurity regulations?****Sidley Austin LLP**

Penalties may be specified in sector-specific data protection laws. In addition, cybersecurity failures may result in class actions, regulator enforcement or even contractual penalties.

[Back to top](#)

## Law stated date

Correct as of

Please state the date of which the law stated here is accurate.

USA

Sidley Austin LLP

May 3 2016.

[Back to top](#)