GIR KNOW HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

USA

Lisa Madigan, Sunil Shenoi
and Maureen Gallagher
Kirkland & Ellis LLP

JANUARY 2024

GIR

SCOPE OF DATA PROTECTION LAWS RELEVANT TO CROSS-BORDER INVESTIGATIONS

1. What laws and regulations in your jurisdiction regulate the collection and processing of personal data? Are there any aspects of those laws that have specific relevance to cross-border investigations?

Unlike Europe, the United States does not have a generally applicable and comprehensive privacy regime. Instead, certain laws may apply depending on the type, size and industry of the data and company involved. Some privacy provisions are found in laws that are not fundamentally about privacy, such as autonomous car testing regulations or anti-discrimination laws.

In the absence of a comprehensive, federal privacy law, states are filling the gap. Currently 13 states – California, Colorado, Connecticut, Delaware, Florida, Iowa, Indiana, Montana, Oregon, Tennessee, Texas, Utah and Virginia – have enacted comprehensive data privacy laws, with eight of those laws scheduled to take effect in 2024 or 2025. By the end of 2023, such laws will only be effective in five of those states – California, Colorado, Connecticut, Utah and Virginia. More state-level privacy laws are likely to follow as states seek to protect consumers from privacy and cyber risks and stay competitive with international data regulation.

Lawyers involved in investigations should keep in mind that certain federal laws relating to privacy regularly arise in investigations: the Graham-Leach Bliley Act and the HIPAA Privacy Rule. However, both laws share a common characteristic: they focus on the privacy of consumers rather than a company's employees or its counterparties' employees. Since many internal investigations focus on the behaviour of employees, investigations' lawyers should be sure to note this distinction. Whether an investigation pertains to a company's employees or its interaction with customers will influence what set of privacy laws applies.

State privacy laws

Currently, the most influential general-purpose privacy law in the United States is the California Consumer Privacy Act, as modified by the California Privacy Rights Act (the CCPA), which governs data relating to California residents and applies across all industries, subject to some important caveats discussed below. Practitioners should stay apprised of all relevant state privacy laws when conducting an investigation.

GLB

The federal Gramm-Leach-Bliley Act (GLB) governs the treatment of nonpublic personal information about consumers by financial institutions. Because GLB defines 'financial institutions' broadly, it may come into play for investigations of companies in the financial sector and potentially other businesses.

HIPAA

The Privacy Rule, issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA), governs patient confidentiality and applies to most healthcare providers, health insurers and healthcare information clearinghouses (called 'covered entities' under the statute) – plus anyone who provides certain services to companies in these categories (called 'business associates'). HIPAA considerations may arise in healthcare fraud, antitrust or other investigations in the healthcare space.

Aside from state privacy laws, GLB and HIPAA, a few others occasionally come into play, but will not be the focus of this chapter. These include the following.

Recording laws

Where an investigation's lawyer needs to record a conversation, federal and state laws impact their conduct. In general, the laws may require a lawyer to obtain the consent of one or all parties to a conversation before recording. Before an investigations lawyer records a conversation, he or she should either announce to all participants that it will be recorded and give them an opportunity to end the conversation, or should ensure that the laws of the states for participants in the conversation allow 'one-party' consent for recording.

Wiretapping and hacking law

Various criminal laws prohibit the unauthorised interception of or access to telephone conversations, electronic communications or other electronic content. In particular, the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act (ECPA) – and their state law counterparts – prohibit anyone from accessing computers or communications systems without authorisation, or from intercepting communications generally. For purposes of conducting investigations, these laws usually will not prohibit a company from reviewing its own communications systems (such as its email systems), but usually will prohibit a company from surreptitiously looking into the personal communications systems of its employees or others (such as an employee's personal email account). Whether an employer can review its own communications systems depends on, among other things, whether it is reviewing communications sitting on a server rather than in transit (in 'real time'), whether and how it has given notice to employees about surveillance and investigations, and which state laws apply. Whether an employer can look at an employee's personal communications sent over an employer's network (eg, when an employee looks at a personal email account on a bring your own device connected to the office wireless system), or whether employers can demand access to an employee's personal accounts, similarly demands a more complex analysis.

Public-sector and telecommunications privacy laws

Providers of computing and telecommunications services to the public will sometimes be called upon to help with law enforcement, national security or foreign intelligence investigations. In these cases, 'public sector' privacy laws such as the ECPA or the Foreign Intelligence Surveillance Act may come into play. Moreover, other public-sector laws such as the Privacy Act of 1974 may govern what the government itself does with personal data. Though they contain various privacy implications, these laws are beyond the scope of this chapter.

Corporate privacy commitments

Finally, all companies need to be mindful of privacy commitments they have made. For example, if a company has transferred certain personal data from Europe by promising to comply with 'Standard Contractual Clauses' or the EU-US Data Privacy Framework, or if the company made promises in privacy policies it has made publicly available, the company will need to assess whether those commitments allow it to use particular data in an investigation.

Consumer protection laws

There are other laws that could impact investigatory considerations. Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive trade practices. The Federal Trade Commission has interpreted its provisions to prohibit certain practices around personal data.

Many states have similar consumer protection laws, as well as previously mentioned special-purpose privacy laws, such as those relating to health and insurance. While these laws may have implications for data management, they are unlikely to bear upon reviews of personal data in an internal investigation or situations in which companies are turning data over to authorities. In addition, the federal Fair Credit Reporting Act is another privacy law to consider, but it fundamentally concerns how companies share information about creditworthiness. The federal Children's Online Privacy Protection Act

imposes obligations on companies that know or should know that they are collecting data online for persons under 13 years of age. Investigations lawyers should keep these laws in the backs of their minds, but they are atypical considerations.

Biometric privacy laws

States such as Illinois, Texas and Washington have laws governing the collection and disclosure of biometric information, which are measurements related to a person's unique physical characteristics, including fingerprints, palmprints, voiceprints, facial, retinal or iris measurements and more. The first such law, Illinois's Biometric Information Privacy Act, requires companies to develop a public written policy establishing a retention schedule and destruction guidelines for biometric information, and provides guidance regarding the collection, selling, disclosing and storing biometric information. Though disclosure of biometric information is permitted to comply with government investigations, such laws should be considered when undertaking an investigation.

2. What other laws and regulations, besides data protection laws, may prevent data sharing in the context of an investigation?

In the USA, laws typically do not prevent data sharing in an investigation. However, some laws may require companies to keep such data sharing confidential. For example, anti-money laundering (AML) and anti-terrorism financing laws may require certain entities to report suspicious financial activity; when they do, they ordinarily need to keep the reports and surrounding circumstances secret. Similarly, where companies receive requests from law enforcement, they may be obligated to keep the requests (or their responses) secret when the process is issued pursuant to the Bank Secrecy Act, accompanied by non-disclosure orders issued pursuant to the Stored Communications Act. In both cases, the purpose is to prevent tipping off persons under investigation.

Certain government inquiries made pursuant to the Foreign Intelligence Surveillance Act and national security letters issued pursuant to a range of statutes may also have confidentiality requirements that restrict the ability to share information pertaining to them. To the extent an investigation calls for certain information about technology relevant to national defence to be transferred to a party outside the US, such as a foreign regulator, export control laws may prevent the transfer of certain information.

3. What constitutes personal data for the purposes of data protection laws?

Because the US does not have a comprehensive privacy law, there is not an overarching definition of personal data in the US as exists under the European General Data Protection Regulation (GDPR) regime. Personal data, therefore, varies based on the particular law at issue.

Importantly, personal data does not necessarily remain subject to special treatment indefinitely. Under state privacy laws, GLB and HIPAA, there are various ways to 'anonymise' or 'de-identify' personal data so that it falls outside the scope of these laws. Practitioners should keep this option in mind when dealing with tricky investigation issues, particularly around disclosure of information to authorities.

Moreover, US privacy laws generally apply only to information pertaining to natural persons, but not necessarily all natural persons: the CCPA, for example, applies only to persons resident in California, GLB applies only to financial consumers and HIPAA applies only to healthcare patients. More information about definitions of personal information is below.

State privacy laws

State privacy laws generally define personal data as any information that can be linked to a person. For example, the CCPA covers 'personal information', which is information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly

or indirectly, with a particular consumer or household. In other words, personal information can be anything related to a person, such as name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints and inferences from other personal information that could create a profile about your preferences and characteristics. It also includes information that a company both collects and creates about a person. Note that the CCPA's definition of personal information closely tracks GDPR's definition of 'personal data'. While certain states exclude public information from the definition of personal information, the CCPA's narrow 'public information' exception applies only to information made available in official government records.

There are some exceptions to state privacy laws' broad definitions of personal information, including that many state privacy laws exclude from their scope any personal information covered by other privacy laws such as GLB, HIPAA or other laws, such as the Drivers' Privacy Protection Act. Certain state privacy laws also exclude employee information from their scope, though as of 1 January 2023, the CCPA includes employee data. However, the CCPA provides exemptions for data used solely for internal use or to comply with a legal obligation. Exemptions to the definition of personal information should be examined carefully in the context of an investigation.

GLB

GLB protects consumers' non-public personal information (NPI). NPI is any personally identifiable information that a financial institution collects about an individual in connection with providing a financial product or service unless that information is otherwise publicly available. However, not all information that can be used to identify an individual falls under GLB. The key distinction is the connection between the information and the underlying financial services. For example, a car dealership may be a financial institution because it leases vehicles or provides loans, but the mere fact that a person bought a car from the dealership, without any information about whether the person obtained financing, is not NPI.

HIPAA

HIPAA covers 'protected health information' (PHI), which means personal information combined with individually identifiable health information (broadly including information about past, present or future medical diagnoses, treatment and payment for the same) that is held or transmitted by entities subject to HIPAA (called 'covered entities' and 'business associates', which are discussed later in this chapter). Practically, HIPAA will cover almost all information that a healthcare provider, insurer or clearinghouse, or a business associate of those covered entities, holds about a patient.

4. What is the scope of application of data protection laws in your jurisdiction? What activities trigger the application of data protection laws, to whom do they apply and what is their territorial extent?

US privacy laws apply, in some form or another, both to companies that collect and hold data – roughly, what might be called a 'controller' by many global privacy regimes – and those that do things with data on another's behalf – roughly, what might be called a 'processor' under those regimes. Not all US privacy laws use the terms 'controller' or 'processor', but many new state privacy laws, such as those in Colorado, Connecticut and Delaware, adopt the terms. Often, the laws apply only to certain controllers active in a particular industry or jurisdiction.

State privacy laws

Under state privacy laws, data controllers and processors, often referred to by other analogous terms, such as businesses and services providers, are limited to those doing business or residing in the state. State privacy laws also usually place revenue, customer or personal information thresholds on controllers. For example, the CCPA applies to any for-profit entity that 'do[es] business in California'

and that meets one or more thresholds: (i) has gross annual revenue of over US$25 million; (ii) buys, sells or shares the personal information of 100,000 or more California consumers or households; or (iii) derives 50 per cent or more of their annual revenue from selling California residents' personal information.

State privacy laws may also apply to service providers, or data processors, that maintain or provide services involving personal data on behalf of covered businesses. Under certain state privacy laws, if a processor were to begin exercising decision-making authority with respect to the purposes and means of personal data processing, it would become a controller with respect to that processing and subject to the obligations imposed on controllers.

GLB

GLB directly applies to 'financial institutions', defined as institutions that are significantly engaged in financial activities,and businesses that are adjacent to those institutions. For example, the GLB can apply to car dealers who arrange for financing or leasing of cars or even to career counsellors in the financial industry. It also applies to service providers and certain other entities that receive NPI from a financial institution.

HIPAA

As noted above, HIPAA applies to 'covered entities', which is roughly analogous to 'controllers' and 'business associates', which is roughly analogous to 'processors'. A 'covered entity' is limited to: (i) a health plan; (ii) a health information clearinghouse; or (iii) most healthcare providers. 'Business Associate' means a person who on behalf of such a covered entity processes PHI for business functions or provides services to a covered entity involving the processing of PHI.

5. What are the principal requirements under data protection laws that are relevant in the context of investigations?

As there is no overarching US privacy law, data protection requirements will vary based on the type of information collected and the use for which that information is collected. See also the response to question 12 for requirements relevant to parties assisting with an investigation.

State privacy laws

State privacy laws generally contain an exception for compliance with demands from law enforcement or to investigate, establish, exercise, prepare for or defend legal claims or respond to security incidents. For example, the CCPA has exceptions for compliance with regulatory investigations by federal, state and local authorities, cooperating with law enforcement agencies, and for engaging in communications that are privileged under California law. Companies should consider whether such exceptions are applicable to internal investigations.

Companies should also consider whether their 'collection notice' indicates that they might use personal data for legal or compliance purposes, including investigations. For example, under the CCPA, a business can use personal information only for the purposes listed in the 'collection notice' that it provided when it collected the personal information, and if a business wants to use the information for a purpose that is 'materially different' from the purposes it listed, it must go back to the consumer for consent. Given that the scope of the statutory exceptions described above might vary by state, collection notices should be considered when conducting internal investigations.

GLB

GLB regulates how companies disclose NPI. Generally speaking, a financial institution can disclose NPI to a non-affiliated third party only if it has given notice of that disclosure and a reasonable opportunity for the consumer to opt out. One exception is for disclosures to service providers. To use this

exception, the financial institution needs to have entered into a contractual agreement prohibiting the third party from disclosing or using the information other than to carry out the purposes for which the financial institution discloses the information. The financial institution also needs to have told consumers that it might share information with service providers in its initial privacy notice to consumers or in a revised notice.

Other exceptions exist for risk and compliance activities. A company can disclose NPI to, among other reasons, protect against fraud, comply with federal or state law, comply with an investigation by or subpoena from federal or state authorities, or to respond to judicial process or government regulatory authorities.

HIPAA

HIPAA establishes several categories for which a covered entity might use PHI and assigns different requirements to each: for some purposes a covered entity or business associate can use PHI without specific requirements; for other purposes, a covered entity must obtain the patient's affirmative authorisation or give a patient an opportunity to object. One of the most important purposes for which entities can use PHI outright is 'healthcare operations', a relatively broad term that includes 'conducting or arranging for [...] legal services [...] and auditing functions including fraud and abuse detection and compliance programs'. This will, in most cases, cover investigations, but a best practice is to make this explicit in a privacy policy disclosure to patients.

In addition, HIPAA governs disclosures in a few ways. First, the 'business associate' provisions govern how covered entities share information with their service providers. A covered entity needs to take various steps to ensure that its business associates are processing PHI properly and safely; chief among them is entering into a compliant 'business associate agreement' with the service providers. The Department of Health and Human Services has provided sample clauses here. Second, HIPAA has separate provisions governing how covered entities or business associates share information with various government authorities. Generally, these provisions allow disclosures when required by law, to health oversight agencies, in judicial and administrative proceedings, and to law enforcement. Certain limitations apply in each case.

Finally, HIPAA contains an overarching principle of minimisation. That means that a covered entity needs to consider whether it is using or disclosing PHI more than needed to achieve whatever purpose it has for processing the PHI.

6. Identify the data protection requirements relevant to a company carrying out an internal investigation and to a party assisting with an investigation.

State privacy laws

As noted in response to question 5, state privacy laws generally contain an exception for compliance with demands from law enforcement or to investigate, establish, exercise, prepare for or defend legal claims or respond to security incidents. Companies should consider whether such exceptions are applicable to internal investigations.

As also noted in response to question 5, Companies should also consider whether their 'collection notice' indicates that they might use personal data for legal or compliance purposes, including investigations.

GLB

As noted in response to question 5, GLB regulates how companies disclose NPI. If, as part of an internal investigation a financial institution needs to disclose NPI to a non-affiliated third party, it may do so only if it has given notice of that disclosure and a reasonable opportunity for the consumer to opt out. One exception is for disclosures related to risk and compliance activities. A company can disclose NPI to, among other reasons, protect against fraud. An appropriate disclosure under this exception includes those made to attorneys or auditors.

HIPAA

HIPAA generally allows covered entities to use PHI in internal investigations, so the need to obtain consent of the data subject should be rare and primarily relevant where disclosure is needed to an entity outside a privileged relationship.

As noted in question 5, HIPAA contains an overarching principle of minimisation. In the context of an internal investigation, companies should seek to limit the use or disclosure of PHI to what is needed to achieve whatever purpose it has for processing the PHI.

RIGHTS OF INDIVIDUALS

7. Is the consent of the data subject mandatory for the processing of personal data as part of an investigation?

As discussed below, personal data may be used as part of an investigation without consent due to broad exemptions for investigations purposes. Further, personal data may also be used in connection with responding to subpoenas in connection with a government investigation.

State privacy laws

As noted above, state privacy laws generally contain an exception for compliance with demands from US law enforcement or to investigate, establish, exercise, prepare for or defend legal claims or respond to security incidents. For example, under the CCPA, consent would be necessary for the disclosure of personal information to lawyers or third parties if the privileged-communications exception does not apply, the company cannot disclose the information within the confines of a service-provider relationship, and no other exceptions apply.

GLB

Gramm-Leach-Bliley notices typically state that NPI may be provided to service providers, such as lawyers or other third parties for investigation purposes, so the need to obtain consumer consent should be rare. However, if a financial institution has not delivered the required Gramm-Leach-Bliley notice to the consumer, or the notice does not state that NPI may be provided to service providers, then the financial institution may need to obtain consent from the consumer.

HIPAA

As noted in question 6, HIPAA generally allows covered entities to use PHI in internal investigations, so the need to obtain consent should be rare and primarily relevant where disclosure is needed to an entity outside a privileged relationship, where the disclosure is not covered by one of the exceptions for legally required disclosures.

8. If not mandatory, should consent still be considered when planning and carrying out an investigation?

Given the sensitive and non-public nature of investigations, unless required by law, companies usually do not seek consent due to the potential adverse impact on the outcome of an investigation. In addition, company HR policies, such as acceptable use policies, that cover use of employee data.

9. Is consent given by employees likely to be valid in an investigation carried out by their employer?

As discussed, US privacy laws generally do not require consent before processing personal data as part of an investigation subject to narrow exceptions (see responses to questions 7 and 8).

10. How can consent be given by a data subject? Is it possible for data subjects to give their consent to processing in advance?

The method through which a data subject can provide consent varies based on the applicable law.

State privacy laws

Methods of securing consent will vary by state. For example, the CCPA defines consent as 'any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose'. The Connecticut Data Privacy Act has a substantively similar, but shorter, definition.

Some state laws also specify what does not constitute consent. As an example, the Colorado Privacy Act states that '(a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (b) hovering over, muting, pausing, or closing a given piece of content; and (c) agreement obtained through dark patterns' do not qualify as consent. The Connecticut Data Privacy Act has a nearly verbatim provision.

GLB

As noted above, the annual privacy notice requirements of GLB should address scenarios where disclosures need to be made to lawyers or third parties assisting with an investigation. To the degree that such notices have not been made and in the rare circumstances where a conclusion is reached that exceptions to the requirements are inapplicable, the regulations permit a party to consent to the sharing. The exact form depends on the particular facts and circumstances and further counsel is advisable in such situations.

HIPAA

HIPAA requires an 'authorization' for uses and disclosures of protected health information not otherwise allowed by the Privacy Rule. Where the Privacy Rule requires patient authorisation, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorisation. An authorisation is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment or healthcare operations, or to disclose protected health information to a third party specified by the individual.

An authorisation must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorised to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorisation.

11. What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

Though certain state privacy laws and HIPAA permit data subject access rights, usually such rights cannot be used to access or verify their personal data or influence or resist the processing of their personal data, as part of a government or internal investigation. However, as noted above, the federal Fair Credit Reporting Act may need to be considered, but it fundamentally concerns how companies share information about creditworthiness.

State privacy laws

While some state laws permit a consumer to request what information a business holds on the consumer or to delete such information, such laws often contain exemptions that will justify most refusals to fulfil such requests in connection with an investigation. For example, under the CCPA, if a consumer demands deletion of his or her information, the business can refuse if, among other things, keeping the data is necessary to comply with a legal obligation or to use the information for internal purposes, in a 'manner that is compatible with the context in which the consumer provided the information'. Other exemptions allow a business to refuse if the personal data is needed to 'detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity', or 'enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business'.

State privacy laws also generally do not require a business to provide the information to third parties or the government if doing so would reveal the contents of communications privileged under state law.

HIPAA

Under HIPAA, patients can request that their PHI be disclosed to them; however, a covered entity may refuse to provide information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. The patients' right to amend or delete information has the same limitation. However, under HIPAA a patient has a right to demand that a covered entity limit disclosures of PHI. The only exception to the requirement to limit disclosures is where a disclosure is affirmatively required by law.

EXTRACTION, LEGAL REVIEW AND ANALYSIS BY THIRD PARTIES, INTERNATIONAL TRANSFER

12. Are there specific requirements to consider where third parties are appointed to process personal data in connection with an investigation?

Third parties processing personal data in connection with an investigation will generally do so as a service provider pursuant to an agreement. Any engagement with a third party should clearly indicate that the third party's processing is in support of obtaining legal services and bind the third party to process the data only for the purposes of the services.

State privacy laws

Under state privacy laws, lawyers and third parties may generally process personal data in connection with an investigation in two main ways: first, under the privileged-communication exception, or second, as a service provider (see also response to question 5). Any engagement with a third party should clearly indicate that the third party's processing is in support of obtaining legal services and bind the third party to process the data only for the purposes of the services.

GLB and HIPAA

Under Gramm-Leach-Bliley and HIPAA, lawyers and third parties processing personal information will generally be service providers or business associates, respectively, so the company disclosing the personal data should ensure that the proper service-provider and business-associate contracts are in place, as described in question 5.

13. Is it permitted to share personal data with law firms or legal process outsourcing firms for the purpose of providing legal advice?

See response to question 11.

14. Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

No.

15. What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

As noted above, US privacy laws do not restrict cross-border data transfers out of the United States. But companies may face lingering obligations as a result of data they previously transferred into the United States. For example, if a company imported personal data into the United States from Europe pursuant to the adequacy decision for the EU-US Data Privacy Framework, it may be committed to comply with a detailed set of privacy obligations, such as the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties.

Companies also need to consider laws other than privacy laws. In particular, US export controls law may prevent certain exports of information relevant to US national security. If your investigation involves documents that might contain export-controlled information – particularly in the defence and technology sectors – you may need to take steps to search for that information before shipping data abroad.

16. Are there specific exemptions, derogations or mechanisms to enable international transfers of personal data in connection with investigations?

No.

TRANSFER TO REGULATORS OR ENFORCEMENT AUTHORITIES

17. Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

US privacy laws tend to have broad carve-outs for compliance with regulatory and law enforcement demands coming from US authorities. See also question 5.

State privacy laws

State privacy laws often expressly permit businesses to comply with any civil, criminal or regulatory inquiry, investigation, subpoena or summons by US authorities.

GLB

Similarly, GLB allows disclosure to comply with US law, or with any properly authorised civil, criminal or regulatory investigation, or subpoena or summons by US authorities. GLB could, perhaps, be clearer about whether it covers voluntary and informal requests from authorities. In such circumstances, practitioners sometimes choose to negotiate a 'friendly subpoena' with law enforcement to remove any doubt.

HIPAA

Under HIPAA, there are three main provisions relevant to disclosures to authorities. First, covered entities can disclose protected health information in judicial proceedings. Disclosure is permitted in response to an actual court order. Before responding to subpoenas or discovery requests, covered entities must attempt to notify the patients involved or seek a compliant protective order. Additionally, covered entities can disclose protected health information in response to certain law enforcement requests. When facing an administrative request or investigative demand, a covered entity also needs to ensure that the information is relevant and material to a legitimate inquiry, appropriately limited in scope, and that it is not possible to de-identify the information. Finally, there is a broad carve-out for disclosing information to an agency involved in health oversight activities provided by law.

CCPA

For example, the CCPA expressly permits businesses to comply with any civil, criminal, or regulatory inquiry, investigation, subpoena or summons by US authorities.

GLB

Similarly, GLB allows disclosure to comply with US law, or with any properly authorised civil, criminal or regulatory investigation, or subpoena or summons by US authorities. GLB could, perhaps, be clearer about whether it covers voluntary and informal requests from authorities. In such circumstances, practitioners sometimes choose to negotiate a 'friendly subpoena' with law enforcement to remove any doubt.

HIPAA

Under HIPAA, there are three main provisions relevant to disclosures to authorities. First, covered entities can disclose protected health information in judicial proceedings. Disclosure is permitted in response to an actual court order. Before responding to subpoenas or discovery requests, covered entities must attempt to notify the patients involved or seek a compliant protective order. Additionally, covered entities can disclose protected health information in response to certain law enforcement requests. When facing an administrative request or investigative demand, a covered entity also needs to ensure that the information is relevant and material to a legitimate inquiry, appropriately limited in scope, and that it is not possible to de-identify the information. Finally, there is a broad carve-out for disclosing information to an agency involved in health oversight activities provided by law.

18. Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

US privacy laws tend focus on compliance with US regulatory and law enforcement demands, rather than foreign authorities.

State privacy laws

State law carveouts for complying with legal demands are usually specifically limited to demands from US authorities or investigations relating to US law. Businesses facing foreign demands, therefore, would have to rely on another rationale provided by such laws to justify a transfer.

GLB

GLB is slightly more permissive. It allows disclosures:

[t]o comply with Federal, State, or local laws, rules and other applicable legal requirements; [t]o comply with a properly authorized 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 you for examination, compliance, or other purposes as authorized by law.

The first two provisions are limited on their face to US laws and authorities, whereas the third provision is not, and so it arguably includes foreign authorities.

HIPAA

HIPAA. unlike the CCPA and GLB, allows disclosure to 'authorities', 'courts', etc. However, certain other provisions in HIPAA distinguish between 'authorities' and 'foreign authorities'. Some argue that this suggests that when the HIPAA regulations refer to authorities, courts, etc, without qualification, they mean domestic authorities, courts, etc; others take a different view. Covered entities and business associates will therefore need to take an approach to this problem in line with their risk tolerances.

19. What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

Companies can take several steps to determine an appropriate response to requests for personal information. First, determine whether any privacy laws, regulations or other restrictions exist that would limit your ability to respond to the request, and also whether any exemptions trump such laws, regulations or restrictions. Also consider whether the company has made any commitments regarding personal data, such as whether notices provided to data subjects state that personal data might be provided to a regulator. Another option involves explaining your privacy concerns to the regulator and working with them to drop or narrow the scope of the request. Discussing the issue with a regulator might also cause the regulator to realise that they do not need personal data and that anonymised or de-identified information would be acceptable. In unusual circumstances, getting the data subject's consent might be needed.

ENFORCEMENT AND SANCTIONS

20. What are the sanctions and penalties for non-compliance with data protection laws?

State privacy laws

As an example, CCPA fines are up to US$2,500 for unintentional violations and US$7,500 for intentional violations or violations involving children under 16. In contrast, the Virginia Consumer Data Protection Act does not distinguish between intentional and unintentional violations. Instead, the statute allows for fines of up to US$7,500 for any violation.

GLB

Gramm-Leach-Bliley fines can be serious. Violations can give rise to civil fines of US$100,000 for financial institutions and up to US$10,000 for officers or directors. In addition, violations may result in criminal charges against officers and directors, with a maximum of five years' imprisonment.

HIPAA

HIPAA penalties are divided into two major categories: 'Reasonable cause' fines range from US$100 to US$50,000 per incident. 'Willful neglect' fines range from US$10,000 to US$50,000 per incident and may result in criminal charges.

RELEVANT MATERIALS

21. Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

CCPA, as amended by the CPRA
CCPA regulations
Colorado Privacy Act
Connecticut Data Privacy Act
Virginia Consumer Data Protection Act
Utah Consumer Privacy Act
GLB privacy provisions
GLB FTC regulations
HIPAA Privacy Rule
The Fair Credit Reporting Act (FCRA) , 15 U.S.C. § 1681 et seq
Illinois's Biometric Information Privacy Act (BIPA)
TEX. BUS. & COM. CODE ANN. § 503.001
WASH. REV. CODE §§ 19.375.010 et seq
Computer Fraud and Abuse Act
Electronic Communications Privacy Act (ECPA)

Lisa Madigan

Kirkland & Ellis LLP

Lisa Madigan is a partner in Kirkland & Ellis LLP's government, regulatory and internal investigations group. The former Illinois Attorney General, Lisa has more than 25 years of experience handling a range of issues including data security and privacy, consumer protection, healthcare, the environment and sexual assault and harassment. Lisa was the first female Attorney General in Illinois and held the post for 16 years, becoming the longest-serving Attorney General in the state's history.

Sunil Shenoi

Kirkland & Ellis LLP

Sunil Shenoi is a partner in Kirkland & Ellis LLP's government, regulatory and internal investigations group. He focuses his practice on advising clients on data security and data privacy matters, with a particular focus on responding to data breaches and defending against government investigations into data breaches. Sunil regularly advises clients on compliance with laws and regulatory guidance relating to data security and data privacy issues. Sunil also represents multinational organisations in DOJ and SEC investigations.

Maureen Gallagher

Kirkland & Ellis LLP

Maureen Gallagher is an associate in Kirkland & Ellis LLP's government, regulatory and internal investigations group. Her practice focuses on government, congressional and internal investigations, as well as compliance matters, white-collar defence, and other enforcement actions and regulatory proceedings.

Kirkland & Ellis LLP

Kirkland & Ellis has one of the largest Government, Regulatory & Internal Investigation (GR&II) groups in the world, with over 190 attorneys who work on securities and futures enforcement, securities advisory and compliance, and white-collar criminal defense matters. Our team includes more than 35 former senior enforcement professionals from the SEC, DOJ, FTC, DHS, US Senate and SFO. Our team represents and counsels clients in SEC, DOJ and other market regulators' investigations and in internal investigations involving various securities and commodities laws, including allegations of financial and accounting fraud, disclosure issues, FCPA, auditor liability, private fund examinations and enforcement actions, offering fraud, insider trading, market manipulation, money laundering and other broker-dealer and investment adviser violations. We represent financial services organisations, public companies, fund advisers, accounting firms and other major market participants, as well as individuals.

1301 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
United States
Tel: +1 202 389 5000

www.kirkland.com

Lisa Madigan
lisa.madigan@kirkland.com

Sunil Shenoi
sunil.shenoi@kirkland.com

Maureen Gallagher
maureen.gallagher@kirkland.com