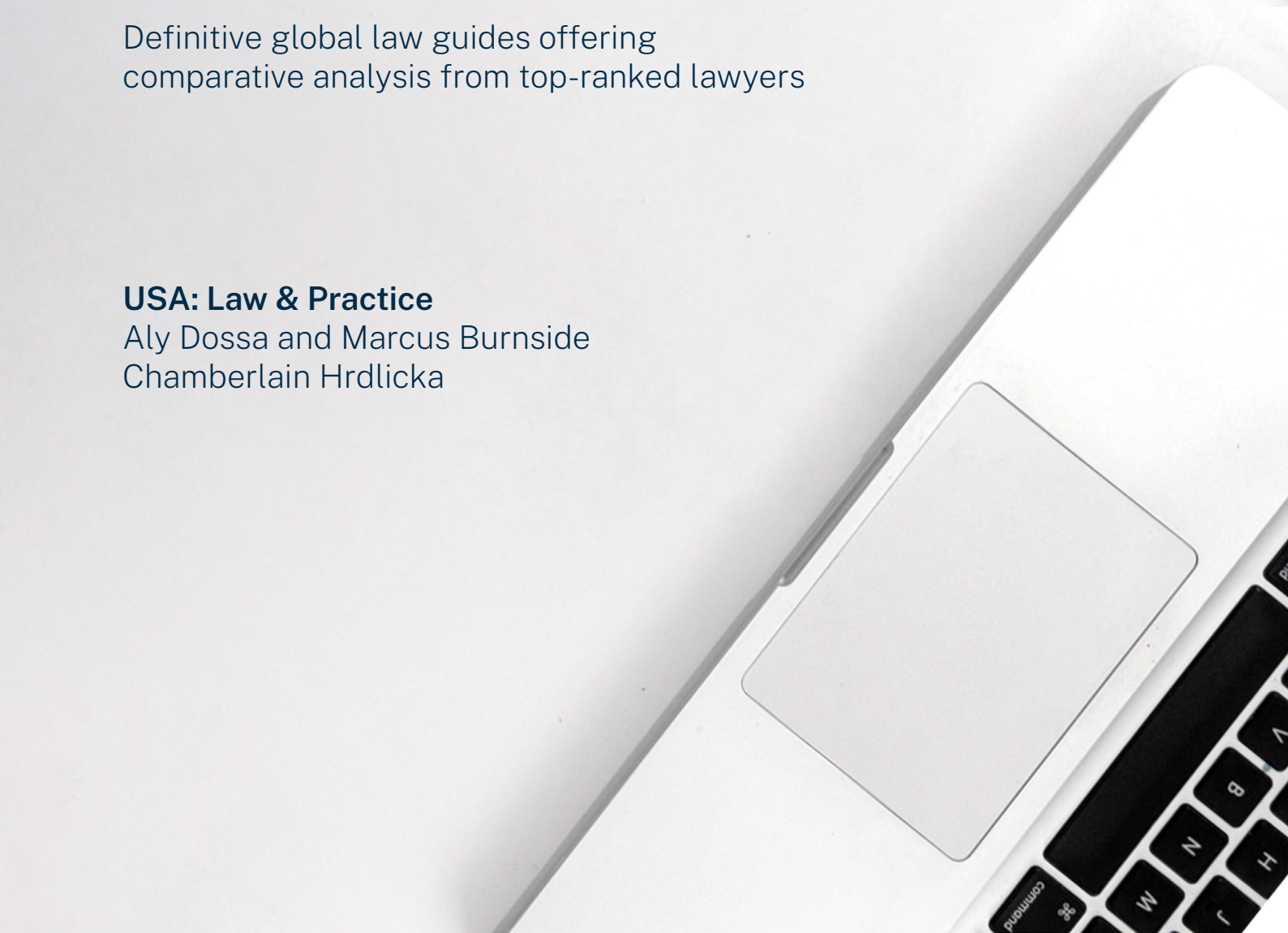
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers



USA: Law & Practice

Aly Dossa and Marcus Burnside
Chamberlain Hrdlicka

USA

Law and Practice

Contributed by:
Aly Dossa and Marcus Burnside
Chamberlain Hrdlicka

Contents

Chamberlain Hrdlicka is a nationally recognised law firm offering a full suite of legal services to businesses and individuals across a wide range of industries. With offices in Houston, Atlanta, Philadelphia and San Antonio, it combines the experience of a large firm with the personal attention of a boutique practice. In respect of data security and privacy, the firm understands how data is captured, stored, transferred and monetised, with experience spanning Fortune 100 companies, leading internet firms, communications providers, mid-size businesses and emerging start-ups. It is well-versed in legal issues and possesses deep technical knowledge of data flows, system interfaces and technology implementation. It navigates complex federal and state laws, each requiring immediate, compliant breach responses and subsequent obligations. Leveraging its comprehensive, multidisciplinary legal and industry experience, it identifies trends and anticipates risks across industries, providing forward-thinking, customised legal strategies to help clients succeed.

Authors

Aly Dossa is intellectual property and technology practice group chair at Chamberlain Hrdlicka. For over 23 years, he has focused on intellectual property counselling and litigation for software, hardware, medical device and consumer device companies, from start-ups to Fortune 100 firms. Aly helps clients navigate the dynamic regulatory landscape, advising on data privacy, cross-border transfers, compliance, breach response and M&A due diligence. He develops global IP strategies, handles patent and trade mark prosecution, negotiates licences and provides legal opinions. He holds certifications as a Certified Information Privacy Professional (CIPP/US), Certified Information Privacy Manager (CIPM), and Artificial Intelligence Governance Professional (AIGP) through IAPP.

Marcus Burnside is senior counsel at Chamberlain Hrdlicka. He focuses his practice on intellectual property for domestic and foreign clients. With mechanical and electrical engineering knowledge, he assists clients across technologies including computer hardware, oil and gas, automation, robotics, communication systems, data storage and green energy. Marcus drafts patent applications, office action responses and appeal briefs. He counsels on IP matters including licence negotiation, non-infringement and invalidity opinions, and due diligence. His practice supports AI companies with strategic IP protection, machine learning data procurement, AI integration and regulatory compliance. Marcus holds certifications as a Certified Information Privacy Professional (CIPP/US) and Artificial Intelligence Governance Professional (AIGP) through IAPP.

Chamberlain Hrdlicka

1200 Smith Street
Suite 1400
Houston, TX 77002
USA

Tel: +1 713 654 9672
Fax: +1 713 658 2553
Email: aly.dossa@chamberlainlaw.com
Web: www.chamberlainlaw.com

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Constitutional Foundations

The US Constitution does not explicitly guarantee a right to privacy, but courts have recognised certain privacy protections through constitutional interpretation. The Fourth Amendment protects against unreasonable searches and seizures, establishing limits on government surveillance and data collection. Various Supreme Court decisions have recognised implicit privacy rights in specific contexts; however, these rights do not apply to non-governmental actions.

Statutory Framework

The United States lacks a comprehensive federal data privacy law comparable to the Europe's GDPR. Instead, privacy and data laws operate through a combination of state and federal laws. In this patchwork, the federal laws operate through a domain-specific approach that applies to certain data types being used within certain contexts. Meanwhile, some states have enacted general data privacy laws and additional domain-specific laws, but these state laws often have exemptions for data protected by particular federal laws. While many of these laws are less onerous than GDPR, the fractured approach requires a broader base of knowledge, both from legal and technical perspectives.

Federal Laws

The following provides a list of the most commonly applicable federal laws that apply to data and privacy. However, it should be appreciated that there are several, rarely applicable laws (including ones that have never been enforced).

- Health Insurance Portability and Accountability Act (HIPAA) – governs the use and disclosure of protected health information by covered entities and their business associates.
- Gramm-Leach-Bliley Act (GLBA) – regulates financial institutions' collection, use and disclosure of consumers' personal financial information.
- Children's Online Privacy Protection Act (COPPA) – requires parental consent for collection of personal information from children under 13. An updated version of COPPA, known as COPPA 2.0, is currently working through Congress and may be passed this year.
- Family Educational Rights and Privacy Act (FERPA) – protects the privacy of student education records.
- Fair Credit Reporting Act (FCRA) – regulates the collection, dissemination and use of consumer credit information.
- Electronic Communications Privacy Act (ECPA) – governs law enforcement access to electronic communications and associated data.
- Video Privacy Protection Act (VPPA) – restricts disclosure of personally identifiable rental records for video materials.
- Cable Communications Policy Act – protects subscriber privacy for cable television services.
- Telephone Consumer Protection Act (TCPA) – restricts telemarketing calls, auto-dialed calls and text messages.
- CAN-SPAM Act – establishes requirements for commercial email messages.
- Genetic Information Nondiscrimination Act (GINA) – prohibits discrimination based on genetic information in health insurance and employment.

Enforcement of these laws is distributed across different federal agencies, and, in some cases, enforcement can be deferred to state attorneys general.

In addition to the above laws that specifically address data privacy, other federal laws can be used to enforce data collection and use. The most prominent of these laws is The Federal Trade Commission Act that empowers the FTC to bring enforcement actions against unfair or deceptive trade practices, which has become a significant source of privacy regulation through enforcement actions and consent decrees.

State-Level Comprehensive Privacy Laws

19 states have enacted comprehensive consumer privacy laws as of early 2026, with more legislation pending. Each state law contains different obligations, exemptions, scope provisions and enforcement mechanisms. Notable examples include:

- Texas Data Privacy and Security Act (TDPSA);

- California's Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA);
- Virginia's Consumer Data Protection Act (VCPA);
- Colorado Privacy Act;
- Connecticut Data Privacy Act; and
- Utah Consumer Privacy Act.

These laws generally share common features including consumer rights (access, deletion, correction, portability), business obligations (transparency, purpose limitation, data security) and opt-out rights for certain data uses, but differ significantly in their thresholds for applicability, definitions, exemptions, private rights of action and enforcement authority.

Between 30–35 states have enacted more limited sectoral privacy laws addressing specific technologies or data types, such as biometric data, genetic information, insurance data or financial data.

In addition, many states have older laws that did not contemplate data collection but are now being applied to data collection practices. The most notable type of these laws is recording consent laws that were originally intended to apply to the recording of phone calls, but have now been applied to online interactions, and most notably to data collection on websites.

Interaction Between Federal and State Laws

Federal sectoral laws generally pre-empt conflicting state laws within their specific domains. For example, HIPAA pre-empts state health privacy laws that provide less stringent protections but allows states to maintain more protective standards. GLBA similarly pre-empts state financial privacy laws to a significant extent.

State comprehensive privacy laws typically contain exemptions for data and entities already regulated under federal sectoral laws, creating a complex patchwork where different rules apply depending on the type of data, the entity collecting it, the context of collection and the use of the data. Organisations handling multiple data types must comply with overlapping federal sectoral requirements, state comprehensive laws and additional state-specific sectoral requirements.

This fragmented approach creates significant compliance complexity, as organisations must navigate which law applies to which data processing activity, with potential gaps where certain data or activities fall outside all regulatory frameworks.

Extraterritorial Reach

Several state privacy laws have extraterritorial application. California's CCPA/CPRA applies to businesses that collect personal information of California residents, regardless of where the business is located, if the business meets certain revenue or data processing thresholds. Similarly, Virginia, Colorado, Connecticut and other states apply their laws to controllers and processors that conduct business in the state or produce products or services targeted to state residents.

These extraterritorial provisions are triggered by factors such as targeting residents of the state, conducting business in the state or meeting quantitative thresholds related to the number of residents whose data is processed. The various state laws use different threshold tests, creating additional complexity for multi-state operations.

Federal sectoral laws generally apply based on the nature of the regulated entity or activity rather than geographic considerations, though they apply throughout US jurisdictions.

Interplay With Non-Personal Data, Cybersecurity and AI Regulation

Cybersecurity

The distinction between privacy and cybersecurity regulation is often blurred. All 50 states have enacted data breach notification laws with varying requirements for timing, content and triggers. Federal sectoral laws like HIPAA and GLBA include security requirements alongside privacy provisions. The Cybersecurity and Infrastructure Security Agency (CISA) plays a role in critical infrastructure protection, which also have additional cybersecurity requirements. Several states have enacted cybersecurity frameworks requiring reasonable security measures, with some specifically addressing ransomware and incident response.

Non-personal data

US law focuses primarily on personally identifiable information, with less regulation of anonymised or aggregate data. However, the boundaries are increasingly contested as re-identification techniques improve (ie, using a collection of non-identifying data to identify an individual). State privacy laws vary in how they define personal information and whether they regulate pseudonymised or de-identified data. Trade secret and intellectual property laws may govern certain business data.

AI regulation

AI-specific privacy regulation is emerging but remains limited. The federal government continues to change and evolve its stance on AI use and regulation but has largely used existing laws and regulations to enforce AI-related use. Colorado has enacted requirements for high-risk AI systems. Several states have proposed AI-specific legislation addressing algorithmic discrimination, automated decision-making, and transparency. Federal sectoral regulators (FTC, EEOC, CFPB) have issued guidance on AI applications within their domains. The interplay typically involves applying existing privacy principles (transparency, fairness, purpose limitation) to AI-driven processing, with questions about whether automated decision-making requires heightened protections.

Regulatory enforcement and trends

Enforcement authority varies significantly. Federal laws are typically enforced by designated agencies (FTC, HHS, FCC, etc). State comprehensive privacy laws grant enforcement authority to state attorneys general. However, some states provide a limited private right of action under certain statutes. This creates a multi-regulator environment where various authorities may have overlapping jurisdiction.

The trend is toward increased state-level activity given federal legislative gridlock; however, both state and federal enforcement has adjusted to view data privacy as a subset of consumer protection. Meanwhile, the plaintiff's bar continues to use older laws applied to new technologies to drive compliance in highly specific domains or use cases of data.

1.2 Rights and Obligations

General Principles for Processing Personal Data

As discussed in **1.1 Overview of Data and Privacy-Related Laws**, US privacy laws operate through a complex patchwork that have been enacted across decades and meant to accomplish divergent goals. Despite this complexity, a common theme throughout most US privacy laws is that organisations should provide clarity. As such, there is very limited ability to provide generally applicable guidance on rights and obligations for personal data. Instead, the following serves as a framework for the practical steps of achieving compliance with US privacy laws.

Practical Implementation Checklist

Organisations should approach compliance in phases.

- Assessment phase – determine applicable laws, conduct gap analysis, identify high-risk activities and prioritise based on legal risk and enforcement patterns.
- Foundation phase – create data inventory, map data flows, inventory systems and vendors, and establish data governance.
- Operational phase – draft policies, implement rights management systems, configure consent mechanisms, execute vendor contracts, deploy security controls and establish training programmes.
- Ongoing phase – monitor regulatory developments, conduct periodic compliance reviews, update processes as business changes, and maintain records of requests, assessments and compliance decisions.

Critical elements vary by applicable law. Examples of some of the most commonly applicable privacy laws include:

- HIPAA requires designated officers, workforce sanctions, Business Associate Agreements and Security Rule safeguards;
- COPPA requires age-screening, verifiable parental consent and limited collection;
- GLBA requires annual privacy notices, opt-out mechanisms and information security programmes; and

- state comprehensive privacy laws often require "Do Not Sell" links, universal opt-out signal recognition, data protection assessments and authenticated consumer portals in some jurisdictions.

Organisations should prioritise compliance efforts based on legal risk (laws with private rights of action or active enforcement), data sensitivity (health, financial, biometric, children's data), scale of processing, reputational exposure and business criticality, recognising that compliance is an ongoing process requiring continuous monitoring and adaptation.

1.3 Special Categories of Personal Data

Because US federal law addresses special categories of data primarily through sectoral regulation rather than comprehensive frameworks, each category of data governed by a federal law could be considered a special category. Some example statutes are provided in **1.1 Overview of Data and Privacy-Related Laws**.

At the state level, state comprehensive privacy laws typically classify as "sensitive personal information" requiring enhanced protections: health data, biometric data (with approximately 15 states having specific biometric privacy statutes requiring informed consent), genetic information, precise geolocation data, citizenship or immigration status, data revealing racial or ethnic origin, religious beliefs, sexual orientation, social security numbers, financial account credentials, and in some states, union membership or communications content.

Processing sensitive data under state laws generally requires either affirmative opt-in consent or at minimum providing consumers with the right to opt out of such processing, along with heightened security measures, purpose limitations and more stringent vendor oversight. Several states prohibit processing that results in unlawful discrimination based on protected characteristics and restrict certain automated decision-making using sensitive categories.

Data Relating to Minors and Criminal Convictions

COPPA applies to operators of websites or online services directed to children under 13, or operators with actual knowledge they are collecting personal information from children under 13, requiring operators to post clear privacy policies, provide direct notice to parents, obtain verifiable parental consent before collecting information, honour parental rights to review and delete children's information, maintain confidentiality and security of children's data, and limit collection to what is reasonably necessary for participation in the activity.

Some state laws extend protections beyond age 13, with California's Age-Appropriate Design Code Act (currently subject to litigation) imposing obligations for likely child users under 18, and several states enacting restrictions on social media platforms' use of minors' data for targeted advertising or requiring parental consent for minors' accounts.

Regarding criminal conviction data, FCRA restricts consumer reporting agencies from including arrests over seven years old, paid tax liens over seven years old, and most other adverse information over seven years old in consumer reports, while the Equal Employment Opportunity Commission (EEOC) provides guidance limiting employers' use of arrest and conviction records to avoid discriminatory impact under Title VII.

State comprehensive privacy laws generally do not create special categories for criminal history data separate from general personal information protections, though state-specific "ban the box" laws, fair chance hiring statutes, and criminal record sealing/expungement laws limit when and how employers, landlords and others may request, consider or retain criminal history information.

1.4 Processing of Personal Data for Research and Development Purposes

Anonymisation for Product Development and Scientific Research

The first step is to determine which laws apply to the data. In the US, HIPAA commonly applies to personal health information (PHI), but there are many circumstances under which HIPAA does not apply to PHI, and other laws, including various federal and state laws, may apply. In addition, there are different exemptions for the use of PHI for research purposes under most privacy laws. Further, anonymising or de-identifying can cause PHI to no longer be considered PHI under US laws, and thus the various laws gov-

erning PHI would not apply. However, as described above, advances in technology can make de-identified data become identifiable data. Thus, even if data is not governed by current laws and the laws do not change, technology changes can cause some of these laws to start applying, causing de-identification to be a moving target requiring ongoing compliance review.

Impact of Health Data Space Regulations

Unlike the European Union's Health Data Space Regulation, which creates a comprehensive framework for secondary use of health data for research, innovation and policymaking with centralised data access bodies and standardised procedures, the United States has no comparable federal initiative establishing a unified health data infrastructure or streamlined access mechanisms for research and product development. The absence of a centralised health data access framework means companies must negotiate individual data use agreements with healthcare systems, navigate varying institutional policies, address inconsistent state law requirements across jurisdictions, and manage complex consent requirements when combining data from multiple sources, thus creating significantly higher transaction costs and longer timelines compared to the streamlined mechanisms envisioned in European health data space initiatives, though potentially offering greater flexibility in commercial applications once data access is secured. Further, as with any other data type, US-based organisations should ensure that any data originating from Europe is obtained and used in a manner that is in compliance with European data privacy laws.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

AI-Specific Requirements and Guidance

The US lacks comprehensive federal AI legislation comparable to the EU AI Act, and instead largely relies on the application of existing laws to AI usage. One complication that arises from this is that users of AI systems often cannot specify what caused an AI tool to create the output that it created. One common issue is the use of AI tools in decision-making where a protected class (eg, race, religion, national origin, etc) could affect a decision, such as hiring. This creates an extra oversight step when implementing an AI tool because these tools can use secondary information to infer protected class information and generate outputs on that basis.

Several states have introduced legislation specifically governing the use of AI, particularly in relation to decisions that are considered significant life decisions, such as hiring, financial decisions, legal decisions, etc. However, the trend in the US is that regulators are relying on the application of existing laws to AI usage to avoid over-regulating the usage of AI.

1.6 Data Breach Requirement

Notification Requirements

All 50 states have enacted data breach notification laws with varying requirements for timing, triggers, content and scope, creating a complex patchwork that organisations must navigate following a security incident. Generally, organisations must provide notice to affected individuals when there has been unauthorised acquisition of computerised personal information that compromises the security, confidentiality or integrity of the information and creates a risk of harm.

Federal sectoral laws impose additional requirements: HIPAA requires covered entities and business associates to notify affected individuals within 60 days of breach discovery, notify HHS within 60 days (for breaches affecting 500+ individuals, immediate notice; for smaller breaches, annual reporting), and notify media for breaches affecting 500+ individuals in a state or jurisdiction. GLBA requires financial institutions to notify customers as soon as possible when sensitive customer information has been misused, with notification to primary federal regulators. The FTC has authority to bring enforcement actions against organisations that fail to provide reasonable security or that make deceptive statements about their security practices, even absent specific breach notification violations.

Organisational Action Items and Authority Investigations

Prior to any data breach, organisations should obtain cyber insurance so that breach response resources will be made very quickly available, at controlled costs, and using vendors pre-approved by their insurance. Regardless of whether an organisation has cyber

insurance, upon discovering a potential data breach, organisations should:

- immediately activate incident response plans and assemble response teams (legal, IT, security, communications, executive leadership);
- contain the incident and preserve evidence for forensic investigation;
- engage in communications with a threat actor using a threat actor communications expert;
- conduct preliminary assessment to determine scope, nature and cause of the breach;
- assess what personal data was accessed or acquired and which individuals are affected; and
- evaluate risk of harm to individuals considering data sensitivity, likelihood of misuse and any actual misuse.

There are many other additional actions that will likely need to be taken depending on the details surrounding the incident, including, for example, the type of incident, type of data implicated, which laws are applicable, etc.

Often, in the wake of an incident, competent authorities including state attorneys general, the FTC, HHS Office for Civil Rights, state regulators and sector-specific federal regulators initiate investigations based on breach notifications, consumer complaints or their own monitoring. Further, as information about the incident is made public, often following the required notifications, mass data privacy litigation follows, with plaintiffs filing class actions alleging negligence, breach of contract, breach of implied contract, unjust enrichment, violations of state consumer protection statutes and violations of state data breach notification laws, though standing requirements and damages theories remain contested and are addressed in detail in **2. Privacy Litigation**.

1.7 Regulators

Investigations

The specific regulator having jurisdiction over investigations is highly fact specific and can include a number of different federal agencies, state agencies and state attorneys general. However, regardless of the regulator, the investigation workflow is largely the same. Generally, the regulating authorities have monitors in place to identify organisations which have suffered an incident and will do a preliminary fact-finding action to determine the scope and severity of the incident, which may be based on their own research (eg, of activity on the dark web), notifications made directly to them, notifications made to affected individuals, complaints from the general public, or from other regulators who may not have jurisdiction, but did discover the incident.

In most instances, an incident will give rise to overlapping jurisdiction amongst the regulators. This gives the regulators, who are often resource constrained, the ability to work together to allocate those resources. As such, many incident investigations are conducted by a consortium of regulators.

Guidance

Regulators often give guidance on privacy issues under their jurisdiction. Whether this guidance is binding depends on the regulator and through which mechanism the guidance was provided. This guidance often provides "safe harbour" rules in terms of which, if followed, the regulator will not pursue any actions. Further, regardless of the enforceability of the guidance, it can provide insight into what that particular regulator reviews when making enforcement decisions.

1.8 Enforcement Proceedings and Fines

Investigation and Enforcement Procedures

Data privacy investigations in the US are initiated and conducted by multiple authorities with varying procedures depending on jurisdiction and applicable law. Enforcement proceedings vary greatly based on the regulator bringing the enforcement action. Most enforcements are resolved as the result of an agreement made between a regulator and the affected organisation.

However, if no agreement is reached, the resulting actions differ between federal enforcement and state enforcement. At the federal level, most federal agencies have procedures internal to the agency to handle enforcement actions, causing federal court actions to be rare and arise only when an organisation appeals a decision made within the agency or if the agency refers a case to the Department of Justice. At the

state level, there are fewer agency bodies available and most actions are taken in lawsuits between the state and the affected organisation.

Due to the patchwork framework of the US, the procedural rules vary greatly based on which regulator is initiating an action. However, privacy laws are usually civil in nature, and thus these actions usually align with the local procedural rules. In addition, the penalties vary greatly by regulator, and review of a particular regulator is required to better understand what types of penalties are enacted, often including an agreement to remedy prior violations, take actions to prevent future harm, make recurring disclosures to regulators and payment of fines.

1.9 Enforcement Trends

Significant Enforcement Actions (2023-2025)

Recent enforcement activity has intensified and monetary damages have significantly increased. The FTC has aggressively pursued cases involving health and children's data, including a USD10 million proposed settlement with Disney over COPPA violations, settlements with Cerebral (USD7 million) and GoodRx (USD1.5 million) for issues affecting health information with advertising platforms, and actions against Rite Aid for using facial recognition technology without adequate safeguards and accuracy testing. Biometric privacy enforcement has intensified under state laws, with BNSF settling a class action litigation under Illinois' Biometric Information Privacy Act (BIPA) for USD75 million. State attorneys general have increased co-ordinated multi-state investigations and enforcement, with major actions including a USD391.5 million settlement with Google (40 states) for deceptive location-tracking practices. In addition, Texas has emerged as one of the strictest enforcers with the Texas Attorney General securing a USD1.4 billion settlement with Meta in 2024 and a USD1.375 billion settlement with Google, each for unlawful capture and use of biometric data through facial recognition features without proper consent.

Emerging Trends

In the past, US privacy law enforcement was largely left to federal agencies tasked with their domain-specific enforcement. However, recently, state level enforcement, beginning with California, and reaching new highs in Texas, has significantly increased the breadth and scope of enforcement in the US. In addition, many of these regulators are seeking more onerous operational penalties on organisations, restricting types of data they can collect and what they can do with certain data that exceed the statutory requirements.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Dispute Trends

Litigation between private parties most often results from a data breach, which, as discussed in **1.6 Data Breach Requirement**, includes plaintiffs filing class actions alleging negligence, breach of contract, breach of implied contract, unjust enrichment, violations of state consumer protection statutes and violations of state data breach notification laws. Other common lawsuits include: actions under the California Invasion of Privacy Act (CIPA) resulting from the use of certain online tracking tools on websites; and lawsuits in response to a Business Email Compromise (BEC) in which an attacker gains access to an email account and tricks customers or employees into sending money or sensitive information, often by changing payment details or sending fake invoices.

The potential damage model for each dispute is highly dependent on the underlying law and facts. For example, in a class action lawsuit resulting from a data breach, the damages are often a relatively small amount per person, but that amount is multiplied potentially millions of times, creating significant risk. In contrast, laws like CIPA provide statutory damages (ie, a set amount of damages per violation), which can also be multiplied many times to create significant risk. Further, suits based on a BEC are dependent solely on the amount of money wrongly sent.

2.2 Recent Case Law

The patchwork system of the US means that the case law is highly specific to the particular governing law. In addition, most actions, particularly those brought by regulators, are settled before a case is even filed. As such, there is often a small body of case law, and

review of the enforcement actions and trends of a regulator is required.

For state-level actions, there exists some case law but, due to the recent nature of these cases, many of them have not advanced far enough through the court systems to become precedential. For example, most CIPA litigation has not reached an appeals court that can release precedential opinions and, as such, the current case law is viewed more similar to enforcement trends rather than precedential case law.

2.3 Collective Redress Mechanisms

In the US, collective redress mechanisms are referred to as class action lawsuits, which have been discussed above. These lawsuits often last years and are commonly settled after key decisions are made by the presiding judge.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

The United States does not have an overarching federal framework comparable to the EU Data Act for governing non-personal data or mandating cross-sector data access. Instead, US law relies on a patchwork of federal and state laws that that prioritise cybersecurity, consumer protection and national security concerns over structured data-sharing rights. As a result, companies do not have statutory entitlements to access or reuse non-personal data; these arrangements are left largely to private contract.

Federal statutes such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act protect systems and communications against unauthorised access (including access to non-personal data); these statues do not address any form of lawful sharing. Similarly, federal policies related to cloud computing and data collected by IoT devices focus on security standards and not on allocating control, access or portability of non-personal data generated by connected products or services.

Currently, the Federal Trade Commission (FTC) and various state Attorneys General (AGs) are taking the lead in shaping non-personal data handling, using its authority over "unfair or deceptive practices" to police inadequate security and harmful data uses. Enforcement actions increasingly address aggregated datasets, location data, and inferred attributes when their downstream use creates meaningful risk to individuals.

While regulators (at the FTC and the state AGs) may demand reasonable security and truthful representations, they cannot (and do not) impose openended governance frameworks or compel broad data sharing absent clear statutory authority. For in-house counsel, this means enforcement exposure turns heavily on reasonable safeguards, precise disclosures and demonstrable risk management, rather than on compliance with a single, unified data-governance statute.

At present, there is not a clear path to a federal data protection law in the US. In response to the lack of federal legislation, various states have expanded their regulatory regimes to start addressing data sharing and access. Keeping tracking of the various changes in state data protection laws, of which there are currently 19, will be key to managing legal risk.

3.2 Interaction of Data Regulation and Data Protection

In the US, intellectual property rights for non-personal data primarily arise in the context of trade secrets, with access governed by contract, including confidentiality clauses. Data privacy frameworks operate independently and do not overlap with intellectual property rights.

3.3 Rights and Obligations Under Applicable Data Regulation

Non-Personal Data

The access to, use of and sharing of non-personal data is primarily governed by contract. Accordingly, parties' rights and obligations must be determined on a contract-by-contract basis.

Personal Data

The United States lacks comprehensive federal data protection legislation. Instead, personal data is regulated through 19 state privacy laws and various sector-specific federal statutes.

Given this fragmented regulatory landscape, organisations should adopt the following practical approach:

- identify what personal data they collect and process;
- determine which state and federal laws apply to that data; and
- implement a data governance programme that addresses all obligations under the identified laws

Where applicable laws impose overlapping or conflicting requirements, best practice is to adopt the most stringent obligation across all relevant statutes. This "highest common denominator" approach ensures compliance while simplifying operational processes.

3.4 Regulators and Enforcement

The Federal Trade Commission and state AGs serve as the primary enforcers of privacy laws in the United States.

The FTC enforces privacy requirements under Section 5 of the FTC Act, which prohibits unfair or deceptive practices. This authority enables the agency to pursue companies that misrepresent their privacy practices or fail to implement reasonable data security measures.

State AGs enforce privacy requirements under state-specific privacy laws, sector-specific federal laws and state consumer protection statutes.

While there is some co-ordination between the FTC and state AGs, significantly more collaboration occurs among the states themselves. State AGs frequently form coalitions – such as the recent "Consortium of Privacy Regulators" comprising California, Colorado, Connecticut, Delaware, Indiana, New Jersey and Oregon – to conduct multi-state investigations, share technical expertise and address cross-border data issues. This collaborative approach creates a more unified enforcement front and ensures more consistent consumer protection across jurisdictions.

4. Sectoral Topics

4.1 Use of Cookies

The US regulates online tracking technologies – including cookies, pixels, SDKs, mobile advertising IDs, device identifiers, fingerprinting and session replay tools – through a fragmented framework of federal and state laws.

Federal Framework

At the federal level, the regulation of tracking technologies are primarily governed by the following statutes and regulatory bodies.

- FTC Act Section 5 – the Federal Trade Commission prohibits unfair or deceptive practices related to tracking technologies.
- COPPA (Children's Online Privacy Protection Act) – requires verifiable parental consent (opt-in) before collecting personal information, including persistent identifiers used for tracking, from children under 13 years of age. Enhanced data-retention requirements became effective in June 2025.

State Comprehensive Privacy Laws (State Laws Impose Varying Consent Models)

- California (CCPA/CPRA) – requires businesses to provide opt-out mechanisms for the sale or sharing of personal information, including browsing history and online activity. Enhanced protections apply to minors under 16, requiring affirmative opt-in consent from the consumer (ages 13–15) or parent/guardian (under 13). Businesses must honour Global Privacy Control (GPC) signals as valid opt-out requests.
- Virginia (VCDPA) – requires opt-out mechanisms for targeted advertising and data sales, and mandates opt-in consent for processing sensitive data and data from identified children.
- Colorado (CPA) – defines consent as a "clear, affirmative act" and prohibits dark patterns. Provides detailed technical specifications for universal opt-out mechanisms.
- Connecticut (CTDPA) – permits technology-based opt-out mechanisms and prohibits geofencing for tracking purposes within 1,750 feet of mental health or reproductive health facilities. Opt-in con-

sent is required before the sale of consumer health data.
- Texas (TDPSA) – requires clear, affirmative consent for processing sensitive data and mandates that universal opt-out mechanisms enable consumers to make unambiguous choices to opt out.

Summary of Consent Models

- Opt-in consent required for children under 13 (federal), minors under 16 (California), sensitive data processing (Virginia, Texas) and health data sales (Connecticut)
- Opt-out models apply to targeted advertising and data sales under most state comprehensive privacy statutes, including those in California, Virginia, Colorado, Connecticut and Texas.

Practical Compliance Requirements

Organisations must provide clear, conspicuous notice about tracking practices, implement effective opt-out mechanisms where required, honour universal opt-out signals like GPC in applicable states, ensure consent banners are properly configured and avoid misleading interfaces, establish vendor management processes with contractual protections for third-party tracking providers, and implement data minimisation practices aligned with state law requirements.

Given the complexity of the regulatory landscape, organisations should determine which state and federal laws govern their tracking practices and implement compliance programmes that satisfy the most stringent requirements across all applicable jurisdictions.

4.2 Personalised Advertising and Other Online Marketing Practices

Personalised and Targeted Advertising Regulation in the United States

The United States regulates personalised and targeted advertising through a patchwork of federal and state laws. At the federal level, the FTC prohibits deceptive advertising practices and has imposed significant penalties for misrepresenting data collection and use. COPPA essentially bans behavioural advertising to children under 13, requiring verifiable parental consent before collecting any personal information including cookies and device identifiers. HIPAA restricts healthcare providers from using health information for marketing without authorisation, while GLBA limits financial institutions' ability to share customer data for marketing purposes.

Multiple states – including California, Colorado, Virginia, Connecticut, Utah and Texas – have enacted comprehensive privacy laws governing targeted advertising. These laws generally require businesses to provide opt-out mechanisms for targeted advertising and data sales, often through "Do Not Sell My Personal Information" links on websites. California's law is the strictest, requiring opt-in consent for minors under 16 and mandating recognition of Global Privacy Control signals. All state laws impose heightened protections for sensitive data (health information, precise location, biometric data, race, ethnicity, religion or sexual orientation), requiring affirmative opt-in consent before using such data for advertising. States also prohibit "dark patterns" – manipulative design tricks to obtain consent – and some require risk assessments for profiling activities that could cause unfair treatment or harm.

To comply, companies must:

- post clear privacy notices explaining data collection for advertising;
- provide easy opt-out options for targeted advertising and data sales;
- obtain affirmative opt-in consent for children's data and sensitive information;
- honour universal opt-out signals (like Global Privacy Control) where required;
- avoid manipulative consent interfaces ("dark patterns"); and
- conduct risk assessments for high-risk profiling activities.

Enforcement comes from the FTC and state AGs, with penalties ranging from thousands of dollars per violation to billions for major violations. Given this fragmented landscape, best practice is to identify applicable laws and implement the strictest requirements across all jurisdictions where the business operates.

4.3 Employment Privacy Law

The United States regulates employment privacy through a patchwork of federal and state laws with no single comprehensive federal employment privacy statute. At the federal level, the Electronic Communications Privacy Act (ECPA) generally prohibits intercepting communications but allows businesses to monitor their own systems when clear policies reserve that right. The Stored Communications Act protects against unauthorised access to stored electronic communications. The Computer Fraud and Abuse Act criminalises unauthorised access to computers, creating liability when employers access employee devices without authorisation. The Fair Credit Reporting Act (FCRA) establishes strict requirements for background checks, requiring standalone written disclosure, written authorisation, pre-adverse action notices and certification of compliance with equal employment laws.

State laws vary significantly and often impose stricter requirements than federal law. Wiretapping consent requirements differ by state: California, Illinois and Pennsylvania require all-party consent to record conversations, while many other states operate under one-party consent frameworks. Biometric privacy laws create substantial compliance obligations – Illinois BIPA is the most comprehensive, requiring written notice, disclosure of purpose and retention period and written consent before collecting biometric data like fingerprints or facial scans, with statutory damages of USD1,000–USD5,000 per violation creating significant class action exposure. California's CCPA employment exemptions became inoperative on 1 January 2023, subjecting employee data to notice requirements, access rights, deletion rights and opt-out mechanisms. Virginia, Colorado, Connecticut and Utah generally maintain employment data exemptions from their privacy laws, though this may change.

Workplace monitoring is governed by reasonable expectation of privacy standards, with courts generally finding that clear employer policies reserving monitoring rights eliminate privacy expectations in company-owned systems. However, employees may retain privacy expectations in personal web-based email accounts, attorney-client communications and certain private communications even on company devices. Remote work monitoring raises enhanced privacy concerns due to home environments where employees have heightened expectations. BYOD (Bring Your Own Device) policies must clearly define employer access rights, specify when device wiping may occur, address data segregation between personal and work information, obtain specific consent for geolocation tracking and implement mobile device management solutions that protect employer data while respecting employee privacy. Processing applicant data requires clear privacy notices, necessary consents (particularly for background checks and biometric screening), FCRA compliance, and in California, CCPA compliance for applicant information.

To comply with employment privacy laws, employers should:

- implement clear monitoring policies notifying employees of surveillance activities and reserving employer monitoring rights;
- obtain appropriate consents for biometric data collection, background checks, and monitoring activities where required by state law;
- provide required notices about data collection, use, and employee rights under applicable privacy laws;
- conduct data protection assessments for high-risk processing activities;
- address multi-state compliance by identifying and applying the most restrictive applicable laws across all jurisdictions;
- manage vendor agreements to ensure third-party service providers meet privacy obligations;
- implement data segregation in BYOD environments to protect both employer and employee interests; and
- maintain detailed records of processing activities, consents and compliance measures

Enforcement comes from the FTC, state AGs, private lawsuits (especially under Illinois BIPA), FCRA class actions and the National Labor Relations Board. Given this complex landscape, employers should assess which laws apply to their operations and implement comprehensive privacy programmes addressing the strictest requirements across all applicable jurisdictions.

4.4 Data Protection in M&A

Given the absence of comprehensive US data privacy requirements, M&A deals require deal-by-deal determinations of applicable data privacy obligations across the transaction lifecycle.

Due Diligence

Buyers should conduct privacy-focused due diligence to assess the target's compliance with applicable state and federal privacy laws, evaluate existing privacy policies and practices, review data processing agreements with third parties, and identify potential liabilities or ongoing investigations.

Representations and Warranties

Asset purchase agreements and equity purchase agreements typically include standard representations and warranties stating that the seller is in compliance with all applicable privacy laws. The onus is on the parties to determine which laws apply to the particular transaction.

Change-of-Control Notifications

Notification requirements for changes of control depend on:

- contractual obligations – many data processing agreements and vendor contracts require notice to customers or data subjects before a change of ownership;
- state privacy laws – some state laws (such as the CCPA) may require updated privacy notices if data practices will materially change post-transaction; and
- sector-specific laws – certain regulated industries (such as healthcare under HIPAA) have specific change-of-control notification requirements.

Post-Closing Integration

Post-closing obligations are determined on a deal-by-deal basis, focusing on which privacy laws apply (state or federal) and what actions the buyer must take under those laws, including updating privacy policies, integrating data governance programmes, harmonising consent mechanisms, and ensuring ongoing compliance with all representations and warranties made during the transaction.

5. International Considerations

5.1 Restrictions on International Data Transfers

The United States regulates cross-border data transfers through a fragmented framework of federal sectoral laws, export controls, national security restrictions and state privacy laws rather than a single comprehensive statute. A "transfer" is defined broadly to include physical movement of data across borders, remote access from abroad, hosting data on foreign servers, disclosure to foreign affiliates or vendors, and granting administrative access to foreign personnel – meaning even allowing an overseas employee to access a US-based database constitutes a transfer. The regulatory landscape encompasses sector-specific federal laws like HIPAA (healthcare data) and GLBA (financial data), which require the same contractual safeguards for international service providers as for domestic ones. Export controls under ITAR prohibit transferring defence-related technical data abroad or to foreign persons within the US without licences. National security frameworks include CFIUS oversight of foreign investments involving sensitive US data and the DOJ Bulk Data Rule effective April 2025, which prohibits data brokers from transferring bulk sensitive personal data to countries of concern (China, Russia, Iran, North Korea, Cuba and Venezuela). State privacy laws in California, Virginia, Colorado, Connecticut, Utah and Texas impose contractual requirements on international processors regardless of data location.

For lawful cross-border transfers, organisations must implement multiple compliance mechanisms depending on applicable laws. Under HIPAA, covered entities must enter into Business Associate Agreements with international third parties handling protected health information, requiring contractual safeguards and application of the "minimum necessary" standard limiting cross-border access. GLBA requires financial institutions to provide privacy notices and opt-out rights before disclosing non-public personal information internationally. State comprehensive privacy laws require written agreements with international processors containing confidentiality obligations, purpose limitations, restrictions on onward transfers without authorisation and compliance assistance requirements. Organisations must conduct risk assessments

evaluating security risks, foreign government access risks and potential data subject impacts before transferring, plus perform vendor due diligence assessing international service provider security controls and compliance capabilities. Contractual agreements must include flow-down provisions ensuring sub-processors receive identical protections. Exceptions exist for consent from individuals (though requirements vary by jurisdiction), necessity for legal proceedings or defending legal rights, law enforcement and national security purposes, and specific business carve-outs in the DOJ Bulk Data Rule.

Cross-Border Transfer Compliance Checklist

- Identify applicable frameworks – determine which federal sectoral laws (HIPAA, GLBA), export controls (ITAR), national security restrictions (CFIUS, DOJ Bulk Data Rule) and state privacy laws apply to transfers.
- Define the transfer – document whether data is being physically moved internationally, allowing remote access from abroad, using foreign hosting, or granting access to foreign personnel.
- Conduct risk assessments – evaluate security risks, foreign government access risks and data subject impacts before making cross-border transfers.
- Perform vendor due diligence – assess international service provider security controls, establish audit rights and verify compliance capabilities.
- Implement contractual safeguards – execute written agreements with foreign processors containing confidentiality provisions, purpose limitations, onward transfer restrictions and security requirements.
- Establish onward transfer controls – include flow-down provisions requiring foreign sub-processors to maintain equivalent protections and notification before engaging new international sub-processors.
- Document legal basis – identify applicable exceptions (consent, legal necessity, law enforcement or business carve-outs) and maintain supporting records.
- Maintain compliance records – keep documentation of risk assessments, international contracts, consent mechanisms and transfer authorisations for regulatory inquiries.

5.2 Government Notifications and Approvals

The United States generally does not require governmental registrations, filings or approvals for routine cross-border transfers of personal data or commercial business data. Federal law imposes no overarching data-export authorisation regime, and state privacy laws (such as the CPRA and VCDPA) require only contractual safeguards – not government permission. Likewise, sector-specific privacy laws (HIPAA, GLBA, FERPA) may restrict disclosure but do not impose approval requirements for international transfers. As a result, typical business and personal-data transfers from the US may proceed without filing.

However, three regulatory regimes – EAR, ITAR, and OFAC – do require licences for exports of certain technology, technical data and software. The Export Administration Regulations (EAR) regulate controlled software and technology and cover electronic, cloud-based and deemed exports, with licensing dependent on ECCN classification, country destination, end-user and end-use. The International Traffic in Arms Regulations (ITAR) require prior authorisation for all exports of defence articles and technical data on the US Munitions List, including deemed exports, and mandate registration with DDTC. The OFAC sanctions regime restricts transfers to sanctioned countries, entities and individuals, with licences required unless a general licence applies. Before any cross-border transfer of data or technology, organisations should classify the item, screen the destination and recipient, assess end-use and determine whether a licence or exception applies; non-controlled business or personal data may be transferred without government involvement.

5.3 Data Localisation Requirements

Data Localisation

The United States has no general requirement that data be stored domestically. Most companies may store data abroad or use foreign cloud providers without seeking government approval. Exceptions primarily arise in government and defence contexts: federal contractors subject to FedRAMP or DFARS/CMMC often must store data on US servers and limit access to US persons, and ITAR-controlled defence technical data cannot be stored overseas or accessed by

foreign nationals without State Department authorisation.

Regulated industries such as banking, healthcare and education may use offshore storage but must maintain strong contractual protections to ensure privacy, security and regulatory access. A 2024 executive order is expected to impose new restrictions on transferring sensitive personal data (such as geolocation, biometrics, genetic data and certain health or financial information) to specific countries of concern, but final rules are still pending. CFIUS may also require US-based storage when foreign investors acquire US companies holding sensitive data. In practice, most commercial data may be stored globally, while government, defence and some categories of sensitive personal information face stricter controls.

Remote Access

For ordinary business and personal data, remote access from outside the United States is generally allowed without government filings. The requirements mirror offshore storage – appropriate contracts, encryption and access controls – but no licensing. However, remote access to controlled technology, such as encryption source code or defence-related technical data, is treated as an export and may require authorisation from BIS (under the EAR) or DDTC (under ITAR) unless an exception applies. Organisations must determine whether the data is controlled, the nationality of the person accessing it, and whether they or their country appear on restricted party lists.

Remote access by persons located in or connected to sanctioned countries such as Cuba, Iran, North Korea, Syria or certain sectors in Russia requires OFAC approval. For federal and defence contractors, remote access from outside the US or by non-US persons is typically prohibited unless explicitly permitted under the contract. Overall, remote access is freely allowed for routine business data but restricted or subject to licensing when involving controlled technology, sanctioned individuals or countries, or federal and defence information.

5.4 Blocking Statutes

No US Blocking Statutes; Courts Retain Discovery Power Despite Foreign Laws

The United States does not have blocking statutes like those found in Europe that categorically prohibit compliance with foreign discovery orders or restrict cross-border disclosures. Unlike many countries that have enacted laws to prevent their citizens and companies from responding to foreign court requests, US law generally facilitates rather than restricts international information sharing and foreign judgment enforcement. States have adopted laws (Uniform Foreign-Country Money Judgments Recognition Acts) that make it easier to recognise and enforce foreign court judgments in the US, not harder. These laws create a presumption in favour of honouring foreign judgments and place the burden on anyone resisting enforcement to prove specific problems with the foreign court's decision.

However, US federal law does create some targeted restrictions. The most significant are Treasury Department sanctions administered by the Office of Foreign Assets Control (OFAC), which prohibit transactions with specially designated nationals and blocked persons from countries like Iran, North Korea, Russia and others. These sanctions can restrict sharing information with sanctioned entities or individuals. Additionally, export control laws (including the International Traffic in Arms Regulations for defence items and Export Administration Regulations for dual-use technology) restrict disclosure of technical data, source code and defence-related information to foreign nationals or entities without proper authorisation. Courts handle these restrictions by issuing specialised protective orders that limit who can access sensitive materials and require compliance with federal export rules.

How US Courts Handle Foreign Blocking Statutes and Privacy Laws

When foreign blocking statutes or privacy laws (like the EU's General Data Protection Regulation) conflict with US court discovery orders, American courts do not simply defer to foreign law. The Supreme Court established in the 1987 *Aerospatiale* case that foreign blocking statutes do not deprive US courts of power to order parties under their jurisdiction to produce evidence, even if doing so violates foreign law. Instead,

courts perform a balancing test (called "comity analysis") weighing factors like the importance of the evidence to the case, how specific the request is, where the information is located, whether there are alternative ways to get it and the strength of the foreign country's interest in blocking disclosure.

The modern judicial trend holds that foreign blocking statutes and privacy laws cannot be used to circumvent US discovery rules. Courts have consistently found that the mere existence of foreign laws restricting data disclosure does not prevent American judges from ordering discovery, though these laws may influence whether sanctions are imposed if someone disobeys the order. For example, courts have ruled that even strict privacy laws like the GDPR, which carry significant penalties for violations, cannot be used as an automatic excuse to refuse discovery in US litigation. However, courts recognise genuine conflicts and often use procedural tools to manage them: protective orders limiting who can see sensitive information, requiring the requesting party to pay compliance costs (including costs of meeting foreign privacy law requirements) and demanding indemnification against foreign penalties. Courts also require parties claiming foreign law prevents compliance to provide detailed proof of the specific legal restrictions and show they made good faith efforts to obtain waivers or clarification under foreign law. The bottom line: US courts maintain their authority to order discovery even when foreign laws say otherwise, but they consider foreign legal restrictions when deciding how to structure discovery and whether to penalise non-compliance.

5.5 Recent Developments

The Shift Toward National Security-Driven Restrictions

The United States is moving away from its traditional hands-off approach to data transfers and implementing significant new restrictions based on national security concerns, particularly targeting data flows to China, Russia, Iran, North Korea, Cuba and Venezuela. The most important change is Executive Order 14117 (issued 28 February 2024), which directs the Justice Department to restrict or prohibit American companies from sharing sensitive personal data in bulk – including precise location tracking, biometric data (fingerprints, face scans), genetic information, health records and financial data – with businesses or individuals connected to adversary nations. The Justice Department released a draft framework in April 2024 and is expected to issue proposed regulations in early 2025 with final rules by mid-2025. Once in effect, companies using foreign vendors, cloud providers or employees from these countries who can access large amounts of sensitive US customer data will likely need to implement security programmes (encryption, access controls, auditing) or obtain government approval for certain transactions – the first time the US will require permission or registration for routine data transfers. This represents a fundamental shift: data is now viewed as a strategic national security asset that must be protected from foreign adversaries, not just a consumer privacy issue. Congress has reinforced this approach by passing the TikTok divestiture law (April 2024), which requires ByteDance to sell TikTok or face a US ban because of concerns that the Chinese government could access Americans' data. The federal government also banned TikTok from all federal devices in late 2022, and over 38 states have done the same. The clear trend is toward more government oversight and restrictions on data flows to geopolitical rivals, driven by concerns about espionage, tracking of Americans and threats to national security.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com