ALFA International
THE GLOBAL LEGAL NETWORK

2026 International Client Seminar

March 5-7, 2026

The Privacy Balancing Act – Practical Compliance in a Fragmented Legal Landscape

Dana Howard, CIPP/US, AIGP, Patent Attorney
Moderator
STOLL KEENON OGDEN PLLC
Lexington, Kentucky
dana.howard@skofirm.com

Stacy Cole, CIPP/US, CIPP/E, CIPM
KEATING MUETHING & KLEKAMP, PLL
Cincinnati, Ohio
SCole@KMKlaw.com

©2026 ALFA International Global Legal Network, Inc. | All Rights Reserved.

Fragmented Landscape of U.S. Privacy Law

Publicity is no longer left to the discretion of a newspaper editor or television producer. Any detail about anyone, no matter how minor, can be distributed anywhere in seconds. From printing presses to pixels, technology has changed privacy expectations. In this hyper-connected world, every digital interaction leaves a trail, and as the law continues to determine its place on this trail, businesses must adapt their processes and practices to comply with changing privacy requirements.

The U.S. legal landscape for data privacy is often described as "fragmented." Unlike many countries, the United States does not have a single, comprehensive law that covers all personal data. Instead, U.S. privacy law consists of a patchwork of rules that change depending on the state and industry in which a business operates. For businesses, this means there is no "one-size-fits-all" compliance strategy. Mapping the overlapping requirements of the various statutes is a constant challenge, requiring organizations to be proactive in managing the various regulatory risks across different jurisdictions.

This U.S. privacy law overview examines how, and by whom, data privacy obligations are enforced in the U.S., a summary of those obligations, and current compliance issues, including state-specific laws and AI-specific concerns.

Sectoral Approach to Federal Privacy Law

There is no express right to privacy in the U.S. Constitution. While privacy is often perceived as a fundamental American right, the word itself does not appear in the text. Instead, the right to privacy has been inferred by courts from various amendments, such as the Fourth Amendment's protection against unreasonable searches. The lack of an explicit constitutional anchor is one of the primary reasons why privacy protection in the U.S. remains a patchwork of different laws rather than one single, unified mandate.

While other nations have a single law covering all data, the U.S. follows a sectoral approach. Federal laws have been enacted to cover certain industries, like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare or the Gramm-Leach-Bliley Act (GLBA) for financial data. Other federal laws have been enacted in response to specific issues. For example, recently, on May 19, 2025, President Trump signed the Federal Take It Down Act, which prohibits the nonconsensual online publication of pornographic digital forgeries (or deepfakes).[i] The law addresses concerns regarding the use of an identifiable individual's image in AI-enabled sexual exploitation. Among other things, the Act requires certain covered, public-facing, user generated content platforms to remove prohibited content within forty-eight (48) hours of notification. Other issue-specific federal privacy laws include the Children's Online Privacy Protection Act (COPPA), which imposes certain requirements on operators of websites or online services directed to children under 13 years of age.[ii]

US Privacy Law Enforcers

For businesses not covered by a federal statutory scheme, like HIPAA or GLBA, the Federal Trade Commission, or FTC, is likely the primary enforcer of their privacy obligations at the federal level. The FTC does not have a specific privacy law to enforce, but instead relies on its Section 5 powers under the FTC Act to regulate companies for unfair or deceptive acts or practices.[iii] Basically, if businesses tell consumers they are protecting their data and do not, or collect and use their customer's data in misleading ways, the FTC can step in and force complaince. The FTC has used this power in the past to settle major cases against tech and retail giants, effectively filling the gap left by a lack of legislation.

Beyond the federal level, state attorney generals and dedicated privacy agencies are becoming increasingly active. In states like California, specific agencies have been created just to handle privacy enforcement. These state-level actors are often the first to investigate data breaches or deceptive data practices. They have the power to bring lawsuits, seek injunctions, and levy heavy fines. This means businesses may have to answer to regulators in every state where they have customers, making compliance a multi-front effort across jurisdictions.

Global View

Beyond the U.S. borders, the global picture is quite different. At least 144 countries have enacted their own national data privacy laws. This global movement toward regulation means that companies doing business internationally must juggle different, and sometimes conflicting, data protection requirements that can significantly impact their global data transfer strategies and operations.

The European Union's General Data Protection Regulation, or GDPR, is widely considered the "gold standard" for privacy law. It's a comprehensive, borderless law that applies to any company handling the data of EU residents, regardless of where that company is located.[iv] The GDPR's influence is so significant that it has triggered what's known as the 'Brussels Effect,' where its standards are adopted by companies and other governments around the world just to simplify global operations. It also serves as the primary inspiration for many emerging state laws. The GDPR requires a lawful basis for processing any personal data, meaning you are unable simply to mine or collect data on a whim. It also emphasizes transparency and purpose limitation, requiring businesses to tell users exactly why they are collecting data and only using it for that specific reason. Data minimization and storage limitation requirements force companies to collect only what they need and delete it when it's no longer necessary.

Similar to the GDPR, China passed the Personal Information Protection law (PIPL) in 2021, which applies to companies that handle the personal information of individuals in China regardless of whether those companies conduct business in China.[v] Concepts from these global laws now are being mirrored in the new wave of state laws across the United States, representing a fundamental shift toward more responsible data management practices.

Wave of State Comprehensive Data Privacy Laws

As of 2026, nineteen (19) states will have their own comprehensive acts in effect.[vi] This wave started in California, but has quickly spread across the country. While many of these laws are similar, they are not identical. This creates the potential for a compliance headache for national businesses, who must decide whether to follow the strictest state law for everyone or attempt to manage different rules for different residents. This "patchwork" is the primary driver for the current push by some for federal legislation to establish more consistent, national standards.

Central to these laws is the definition of "personal data," which encompasses a broader category of information than what has been legally considered "personally identifiable information" for purposes of data breach notification. Generally, "personal data" includes any information that is linked or reasonably linkable to an identified or identifiable individual. This goes far beyond an individual's name or social security number; it can include IP addresses and geolocation data. However, there are exceptions. Most laws do not cover 'de-identified' data—information that has been stripped of its personal links—or aggregate data that shows broad trends. Publicly available information, like government records, is also sometimes exempt. Knowing exactly what data is being collected and how it fits these definitions is the first, most critical step in any privacy compliance program and requires companies to employ systems for identifying the collection points for potential "personal data" of consumers and tracking how that information enters, moves through, and is stored their systems.

Under these state comprehensive privacy laws, consumers are granted a potentially powerful suite of rights over

their data. These include the *right to access* what a company knows about them and the *right to correct* any inaccurate information. There also is the *right to delete* allowing users to ask a company to wipe their data entirely. Another key right is *data portability*, which allows consumers to take data from one service provider and move it to another easily. These rights give individuals more control over their personal identities and digital footprints, creating a new standard for how companies interact with their consumers.

In addition, many states require that consumers have the *right to opt-out* of the sale of personal data or its use for targeted advertising. Some laws go even further, requiring *opt-in consent* before a company collects sensitive information. For many businesses, responding to "Consumer Rights Requests" will require having automated systems and dedicated teams in place to meet strict timelines and verification requirements mandated by various state statutes, some of which include providing consumers with a response to their requests within forty-five (45) days and rights to appeal.

In addition to consumer rights, comprehensive privacy laws obligate businesses to provide clear and transparent privacy notices that explain their data practices in plain language. They must also practice data use minimization, ensuring they are not collecting more data than they actually need to provide a service. Protecting "sensitive information" requires heightened security measures and limited access within the organization. These obligations are not just suggestions; they are legal requirements that, if ignored, could lead to enforcement actions

For certain data collection, some state laws now require data protection assessments, which are documented audits of any high-risk data processing activities. This includes things like selling data to third parties, using it for targeted ads, or using AI for profiling. These laws also require businesses to ensure they have reasonable security measures and solid vendor contracts in place that obligate vendors to protect data in the same manner. These internal controls and documented assessments may provide helpful evidence businesses if a regulator conducts an audit or if your practices are challenged in court.

Not every small business is subject to these complex laws. Most state statutes have applicability thresholds. A state's law might only apply to a business if it is doing business in that state and meets certain other criteria, such as collecting personal data from a certain number of that state's residents (typically 25,000 or 100,000 depending upon the state) or deriving over fifty percent (50%) of revenue from the sale of personal data. There also are exemptions for small businesses with low revenue, non-profits, higher education institutions, or businesses subject to HIPAA and GLBA. Likewise, many laws do not apply to data collected from employees or business-to-business interactions. However, the trend is toward lower thresholds and broader application. Some states, like Montana and Connecticut, have amended or proposed amendments to remove exemptions for businesses subject to GLBA, meaning that those businesses will be subject to the additional requirements under state laws. Accordingly, more companies may find themselves under the spotlight of privacy regulation in the future.

Keeping Up with Opting Out

One of the most innovative compliance requirements is the "Universal Opt-Out Mechanism." Instead of making consumers find a "Do Not Sell" link on every single website requiring consumers to manually opt-out of having their personal data sold, many states now require businesses to honor a browser-level signal, like the Global Privacy Control. This machine-readable signal tells the website operator automatically: "do not track me" or "do not use my data for ads." For businesses, this means their websites must be technically capable of recognizing and respecting these signals in real-time. It's a shift toward automated privacy that makes it much easier for consumers to protect their information across the entire internet. These requirements are being made part of some states' comprehensive privacy acts as well as being made requirements under separate, issue-specific state laws, like California's Opt Me Out Act, which was signed by Governor Newsom on October 8, 2025.[vii]

Heightened Scrutiny for Sensitive Data

Within the broader category of personal data, "sensitive data" gets special attention. This includes things like race, ethnicity, religious beliefs, health data, and precise geolocation. It also covers immigration status, children's data, and biometric or genetic information. Because the risk of harm is higher if this data is misused, most state laws require explicit "opt-in" consent before it can be collected. Companies must adhere to much stricter security and retention rules for this type of information. For businesses handling sensitive data, their compliance roadmaps need to be significantly more robust to avoid potential legal liabilities.

Biometrics, like facial geometry, fingerprints, and iris scans, are a major focus for some state regulators. Colorado recently amended its comprehensive privacy law to impose new obligations on the collection of biometric data from both consumers and employees. Other states have stricter, issue-specific laws, like Illinois's Biometric Information Privacy Act (BIPA)[viii] that have led to multi-million dollar class-action settlements for unauthorized collection. Just recently, in October of 2025, an Illinois federal judge approved a $12.1 million class action settlement in a dispute between Speedway LLC and a group of employees over the use and collection of finger-scan timeclocks.[ix]

Whether using biometrics for identity verification, smart cameras, or simple workplace security, the legal risk is something to note. Organizations must ensure they have clear, written consent and provide users with easy ways to opt-out or delete their biometric records to stay ahead of these aggressive enforcement trends.

Cybersecurity and Data Breach Notification

Regardless of how well a business protects its data, a breach is always a possibility. In the U.S., every state has a data breach notification law.[x] These laws require notifications to individuals—and sometimes state regulators—whenever their "personally identifiable information" (pii) is accessed without authorization. While the requirement is universal, the details vary significantly by state. Different states have different definitions of what counts as a breach and different timeframes for how quickly notifications must be sent. Most definitions of pii include a combination of an individual's name and a government id number or financial account number. Unlike many comprehensive privacy acts, data breach notification acts apply to pii that has been collected by businesses, regardless of whether the individual is a consumer or employee. This means a single national data breach may potentially trigger various sets of requirements and reporting timelines, making incident response a large undertaking and making data retention policies a critical part of any business's data privacy compliance program.

The threats causing these breaches are constantly evolving. Ransomware remains a top concern, often involving sophisticated attackers who may be on the government's "blocked persons" list—making it a crime to even pay the ransom. Phishing scams and unwise internal practices, like sending sensitive financial information through unencrypted email remain a source of vulnerability. Preventing these attacks requires more than just good software; it requires a culture of security within the organization. Limiting failed login attempts, requiring multifactor authentication, and training employees to spot phishing attempts are now essential components of a legally defensible cybersecurity strategy.

The standing of consumers to sue for harm or anticipated harm from data breaches continues to be an intensely litigated issue with many courts having previously decided that a showing of some actual misuse of data is required to sue under a state's data breach notification statute. In June of 2025, an Indiana Court of Appeals determined that former employees of an Indiana bakery had standing to sue based upon a cybersecurity breach that resulted in the employees' full names and social security numbers being taken.[xi] The bakery had stored the employees' pii unencrypted. In reversing the lower court's dismissal, the Indiana Court of Appeals distinguished the case from

other cases based exclusively on enforcing a statutory right stating that the asserted claims involved common law claims of negligence and breach of contract. The Indiana Court of Appeals further found that the likelihood that the information may be sold on the dark web and the time spent by the named-plaintiff to mitigate potential future harm from identity theft constituted a sufficient showing of harm for purposes of standing.

AI-Specific Data Privacy Issues

The intersection of AI and data privacy is one of the most complex areas of law today. AI models require large amounts of data to "learn," including personal data. As companies rush to integrate AI into their operations, they must grapple with the fact that many existing privacy laws were written before these technologies became mainstream, leading to potentially significant legal and ethical gray areas.

The Office of Economic Cooperation and Development's definition of AI, which many regulators use, describe AI as a machine-based system that, for explicit or implicit objectives, infers from the input it receives how to generate outputs like predictions, content, or decisions.[xii] These systems vary widely in their levels of autonomy and how they adapt after deployment. From a privacy perspective, the most important part of this definition is the "input" it receives. If that input is personal data, all the data privacy principles—like transparency, purpose limitation, and the right to delete—suddenly apply to the AI training process itself, creating a whole new layer of compliance obligations for developers and users alike.

Consider a common AI use case: training a marketing model on customers' personal data to find "look-alike" prospects. This raises immediate privacy questions. Is this use consistent with the original reason the data was collected? Did the user have a chance to opt-out of this specific type of profiling? How do businesses properly gain consumer consent under existing privacy laws to use previously collected data in this new way? "Dynamic Consent"[xiii]—a self-service dashboard where users can update their preferences in real-time—might be one possible solution. Regardless of the technical fix, businesses must ensure that their use of AI does not violate the core promises contained in their privacy notices or risk facing enforcement actions for deceptive practices under state privacy laws, consumer protection laws, or the FTC.

AI raises other ethical issues, particularly around surveillance. Facial recognition technology is a prime example. The FTC has instituted enforcement actions against a retail store chain that used face scanning technology and AI to identify potential shoplifters where consumers' images were collected without consent, and the AI technology was often inaccurate leading to many mismatches.[xiv] Other issues include using AI to make "deep fakes" or incorporate an individual's voice and likeness without their authorization. These ethical dilemmas are already leading to states, such as California, Colorado, Utah, Tennessee, and Illinois adopting AI-specific laws prohibiting such acts or requiring transparency.[xv]

Putting the Pieces Together

Compliance with this patchwork of U.S. data privacy obligations requires a comprehensive assessment of a businesses' data collection practices and purposes. Privacy enforcement is not just about the government, though. A business's primary privacy obligations may arise from a data processing agreement with a vendor or a cybersecurity insurance policy long before a government statute ever applies. Mergers and acquisitions also now involve intense scrutiny of a company's data practices by acquiring entities or their insurers. In the modern business world, a privacy policy may be viewed as a contract with website users or customers. In many ways, the private sector creates its own ecosystem of strict privacy enforcement. By staying informed and proactive, businesses are able to navigate this complex landscape and build the proper data privacy infrastructure to ensure their longevity in the digital world.

[i] The TAKE IT DOWN ACT: A Federal Law Prohibiting the Nonconsensual Publication of Intimate Images, S. 146, https://www.congress.gov/crs-product/LSB11314

[ii] https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-not-just-kids-sites

[iii] 15 U.S.C. §§ 41-58; https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act

[iv] https://gdpr.eu/what-is-gdpr/

[v] Chiang Ling Li, "First case on PIPL's extraterritorial scope highlights key compliance priorities" (February 27, 2025). https://iapp.org/news/a/first-case-on-pipl-s-extraterritorial-scope-highlights-key-compliance-priorities

[vi] California Consumer Privacy Act (2018), Cal. Civ. Code § 1798.100, et seq., as amended by The California Privacy Rights Act of 2020; Colorado Privacy Act (2021), Colo. Rev. Stat. § 6-1-1301, *et seq*., as amended by SB 25-276; Connecticut Data Privacy Act (2022), Conn. Gen Stat. § 42-515, *et seq*., as amended by SB 1295; Delaware Personal Data Privacy Act, (2023), Del. Code Titl. 6 § 12D-101; Indiana Consumer Data Protection Act (2023), Ind. Code §§ 24-15-1-1, *et seq*.; Iowa Consumer Data Protection Act (2023), Iowa Code §§ 715D.1, *et seq.*; Kentucky Consumer Data Protection Act (2024), Ken. Rev. Stat. § 367.3611, *et seq.*, as amended by HB 473; Maryland Online Data Privacy Act (2024), SB 541; Minnesota Consumer Data Privacy Act (2024), HF 4757; Montana Consumer Data Privacy Act (2023), Mont. Code §§ 30-14-2801, *et seq.*, as amended by SB 297; Nebraska Data Privacy Act (2024), LB 1074; New Hampshire Data Privacy Act (2023), SB 255; New Jersey Data Privacy Law Act (2024), SB 332; Oregon Consumer Privacy Act (2022), Oregon SB 619 as amended by HB 2008 and HB 3875; Rhode Island Data Transparency and Privacy Protection Act (2024), H7787; Tennessee Information Protection Act (2023), Tenn. Pub. Ch. No. 408 §§ 47-18-3201; Texas Data Privacy and Security Act (2023), Tex. Bus. & Com. Code §§ 541.001, *et seq.*; Utah Consumer Privacy Act (2022) Utah Code § 13-61-101, *et seq.,* as amended by HB 418; Virginia Consumer Data Protection Act (2021), VA. Dode § 59.1-575, *et seq.*, as amended by SB 854.

[vii] Governor Signs Groundbreaking Privacy Bill Making It Easier for Californians to Protect Their Personal Data, October 8, 2025. https://cppa.ca.gov/announcements/2025/20251008_2.html

[viii] Illinois's Biometric Information Privacy Act, 740 ILCA 14/1, *et seq.*

[ix] *Howe v. Speedway LLC*, Case. No. 1:19-CV-01374, 2024 U.S. Dist. LEXIS 176263, (N.D. Ill. September 24, 2024) (certifying class action for violations of Illinois's Biometric Information Privacy Act or BIPA).

[x] National Conference of State Legislatures, https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

[xi] *Hensley v. Lewis Bros. Bakeries, Inc*, 263 N.E.3d 199 (Ind. App. 2025).

[xii] OECD AI Prinples overview. https://oecd.ai/en/ai-principles.

[xiii] Tracy Tuten, "Expanding informed consent in the age of synthetic data and digital twins," *Quirk's Media* (November 1, 2025). https://www.quirks.com/articles/expanding-informed-consent-in-the-age-of-synthetic-data-and-digital-twins

[xiv] FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens, https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance; FTC v. Rite Aid, https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v; Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

[xv] California AI Transparency Act (2025), AB-853; The Texas Responsible Artificial Intelligence Governance Act (TRAIGA) (2025), HB 149; Utah Artificial Intelligence Policy Act (2024), A.B. 149; Tennessee Ensuring Likeness, Voice and Image Security Act of 2024, SB 2096 (Johnson), HB 2091 (Lamberth)