Use this button to switch between dark and light mode.

Latest Blogs

September 24, 2024

Learn About New Practical Guidance Content and Resources

Review this exciting guide to some of the recent content additions to Practical Guidance, designed to help you find the tools and insights you need to work more efficiently and effectively. Practical Guidance...

September 24, 2024

ERISA at 50: Pre-ERISA and the Need for Pension Protections

By: Jeffrey D. Mamorsky , COHEN & BUCKMANN, P.C. THIS VIDEO SERIES CELEBRATES THE ENACTMENT of the Employee Retirement Income Security Act (ERISA), signed by President Gerald Ford on September 2...

By: Kirk A. Sigmon , BANNER WITCOFF THIS CHECKLIST OUTLINES KEY CONSIDERATIONS THAT ATTORNEYS should review when advising whether and how to copyright artificial intelligence (AI) and machine learning...

September 24, 2024

Artificial Intelligence (AI) Considerations in Acquisition A...

By: Erin Hanson , Arlene Arin Hahn , Sahra Nizipli , and Jordan Hill , WHITE & CASE LLP THIS ARTICLE SUMMARIZES VARIOUS INTELLECTUAL PROPERTY AND TECHNOLOGY (IP/IT) PROVISIONS, including sample definitions...

September 24, 2024

AI in Employment Decisions and Performance Management

By: Damon W. Silver , Gregory C. Brown, Jr. , and Cindy Huang , JACKSON LEWIS P.C. Overview of Artificial Intelligence (AI) in Employment Decisions AI tools are fundamentally changing how people work...

More

Privacy Regulation in the United States

March 19, 2024 (18 min read)

By: **Kirk Nahra**, **Arianna Evers**, **Ali Jessani**, **Genesis Ruano**, and **Samuel Kane**, WILMERHALE

This article is intended to give privacy officers and other privacy professionals an overview of how commercial privacy issues are regulated in the United States.

While this article is not intended to be exhaustive in terms of all potentially applicable U.S. privacy laws, it should provide privacy

The United States generally regulates privacy through four main approaches: sector-specific laws, use case-specific laws, laws applicable to certain types of data (data-specific laws), and comprehensive privacy laws (at the state level). We have used this framework to summarize the laws, regulations, and issues that privacy professionals are most likely to come across in their work.

Recent trends in U.S. privacy law can help privacy professionals understand where the law may be going. While change in U.S. privacy law at the federal level continues to remain a possibility, state legislatures continue to be at the forefront of new privacy regulations. Iowa, Tennessee, Indiana, Texas, Oregon, Delaware, and Montana have joined early adopters of comprehensive privacy laws (California, Virginia, Colorado, Utah, and Connecticut) as of 2023. In addition to comprehensive state privacy laws, many states have also passed sector, industry, and data-specific laws as states race to replicate successful statutes and address data issues that have emerged in the wake of the COVID-19-driven shift towards remote work and school. As a result, there has been a strong recent focus on data brokers and more sensitive categories of data, such as health information and genetic data. Regulators have increased attention on issues relating to Adtech and targeted advertising more generally, and many of the laws and regulatory trends discussed in this article are driven by that focus.

While many of these statutes share similar principles—indeed, newer bills frequently draw inspiration from the text and implementation issues of prior statutes—they vary in definitions, scope, and enforcement rights. The complexity created by this web of statutes has been further magnified by the creation of nontraditional privacy obligations and the cross-industry digital transformation that occurred in the wake of COVID-19. In this developing privacy landscape, more companies risk failing to understand the scope of their privacy compliance obligations. Companies that handle sensitive information or engage in practices that would constitute a heightened risk, such as automated decision-making, should be particularly on guard as many

Notably, companies and privacy professionals must consider the abundance of laws that implicate privacy considerations, such as information security laws, laws that regulate government data use, additional data-specific laws like those governing health status, among others, which are not covered in this article. In addition, not all of these laws will be applicable to every company.

Sector-Specific Privacy Laws

Privacy laws at the federal level have primarily focused on regulating privacy in specific sectors, such as healthcare, education, and financial institutions. While still important for practitioners to consider, federal privacy regulations have thus far remained largely unchanged by the recent wave of privacy and data regulation activity—although there are pending rulemaking changes that may lead to some change in these rules in 2024. The three major federal privacy laws that regulate specific types of entities—the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Family Educational Rights and Privacy Act (FERPA)—have remained stable since at least the last wave of amendments made between 2013 and 2015. All three of these statutes draw heavily on the Fair Information Practice Principles,[1] a set of widely accepted guidelines surrounding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personal data. They include, in part:

- Transparency and choice (notice and consent)
- Consumer rights to access and amend their personal information
- Limitations on data collection and use, such as non-disclosure requirements and collection limitation
- Information security safeguards or other breach mitigation procedures

These are not the only statutes that impose requirements on the processing of health, financial, and education data. Many statutes have

Disabilities Act, the FDA's confidentiality rules during clinical trials, and the Individuals with Disabilities Education Act's medical information confidentiality requirements (in addition to a wide range of state laws that impact the privacy and confidentiality of health data). While practitioners should remain vigilant for developments in the privacy implications of sector-specific statutes that do not directly regulate privacy, the below sections highlight the key considerations in the three most prominent sector-specific privacy laws.

Further, it is important to consider that although federal level legislation has primarily remained unchanged, federal regulators, specifically the Federal Trade Commission (FTC), have responded to evolving privacy and cybersecurity concerns. As such, the below includes a section on the FTC's role in enforcing privacy and cybersecurity violations through its authority to bring actions for unfair or deceptive acts or practices under Section 5 of the FTC Act.[2]

Health Insurance Portability and Accountability Act

The HIPAA statute itself says little about privacy and security directly but instead creates privacy standards for "covered entities" through the rules developed by the Department of Health and Human Services (HHS). HIPAA establishes a framework of rules governing how specific "covered entities" secure, transmit, and protect "individually identifiable health information." HIPAA requires that covered entities, originally healthcare providers, health insurance plans, and healthcare clearinghouses, comply with a series of rules and standards.

As a result of the HIPAA statute, there are three rules promulgated under HIPAA that practitioners should consider when advising on health information practices:

- The Privacy Rule[3]
- The Security Rule[4]

authorized by the individual. Entities must respect patients' right to access, amend, and restrict their data, and develop specific procedures to support compliance. There are also specific rules related to the sale of PHI or the use of PHI for marketing. The Privacy Rule is the most expansive in coverage, containing a mini-security rule, requiring contracts with business associates which govern their use of PHI, and setting out principles for de-identification of PHI.

The Security Rule builds upon the mini-security provisions in the Privacy Rule and sets forth detailed requirements for the protection of electronic PHI. Covered entities must implement reasonable administrative, physical, and technical safeguards to protect the PHI they process.

Lastly, under the Breach Notification Rule, covered entities must disclose data breaches to both HHS and individuals whose PHI has been compromised. The rule creates the opportunity for affected entities to conduct a risk assessment to determine whether there is a low probability of compromise of the impacted information to avoid these notification obligations.

Notably, the 2009 HITECH Act[6] extended certain elements of the HIPAA rules to reach covered entities' service providers and contractors (called business associates under the HIPAA rules). Under the HITECH Act, business associates can be directly liable under HIPAA for certain violations, including failing to comply with the Security Rule and failing to provide breach notification to a covered entity or another business associate.

HIPAA serves as a baseline for health information compliance, and explicitly does not preempt more protective state laws. Importantly, HIPAA does not cover many entities and types of data involved in the healthcare system, including health apps, fitness trackers, university student health clinics, or most pharmaceutical companies. States have increasingly looked to fill this gap in coverage under HIPAA by passing

Family Educational Rights and Privacy Act

FERPA protects the privacy of education records at all schools that receive applicable federal education funds. FERPA gives privacy rights related to education records to the parents of minors and then transfers these rights to the students once they turn 18. Schools must guarantee parents or students access to and the ability to correct errors within the student's educational record and must obtain their consent to release information from that record, although directory information such as names or addresses may be disclosed without consent after notifying the student or parent. As under HIPAA, schools are required to include certain limiting contractual provisions in agreements with their service providers. That said, many non-school entities, such as emerging education technologies (EdTech), receive school data under the school official exception, which allows a platform to receive personally identifiable information from education records without parental consent if certain criteria are met.

FERPA similarly serves as a baseline, preempting state laws which would allow for disclosure of records not otherwise permissible under FERPA, such as state freedom of information laws. Further, states have passed a wide range of student privacy laws, most of which prescribe all or some of the following four requirements: notice and consent, use or collection limitation (particularly in the context of third-party applications or targeted advertising), data breach notification, and deletion. Many states also require that schools extend their privacy obligations via contract to third parties that process or handle student data on behalf of covered entities.

Gramm-Leach-Bliley Act

The GLBA[7] governs financial institutions and other organizations that offer financial services and products such as financial advising, insurance, or investment. The relevant provisions concerning personal data are generally split into the GLBA Privacy Rule and the GLBA Safeguards Rule. The Privacy Rule requires regulated organizations to

financial products or services.

The Privacy Rule requires that financial institutions provide a written privacy notice at the start of their relationship with a customer and annually thereafter. These privacy notices must include, among other requirements:

- An explanation of what information is collected
- Where and with whom the information is shared
- How such information is used
- How the information is protected
- Whether the organization is sharing information with third parties
- Notice of the customer's right to opt out of such sharing with nonaffiliated third parties, subject to certain exceptions

The Safeguards Rule, on the other hand, requires companies to develop, maintain, and implement a comprehensive information security program to keep personal information secure. These provisions require that the written information security program contain administrative, technical, and physical safeguards to protect customer information. For example, under the FTC's Safeguards Rule, an entity must undertake comprehensive risk assessments, appoint a qualified individual to be responsible for the institution's information security program, conduct annual penetration testing of information systems, protect consumer information through encryption, multifactor authentication, and proper storage, and much more.

The FTC recently approved significant modifications to its version of the Safeguards Rule. Among other changes, the new rule will require nonbanking financial institutions regulated by the FTC, including financial technology companies, mortgage brokers, credit counselors, financial planners, and tax preparers, and others, to report certain data

The GLBA is enforced by various financial regulators that have jurisdiction as the primary regulator over the types of financial institutions they regulate. This can range from the Consumer Financial Protection Bureau (CFPB) to the Securities and Exchange Commission (SEC) to state insurance commissioners. These various regulators have released guidance and enforce sector-specific GLBA regulations for the industries they oversee. All other entities that otherwise meet the definition of a "financial institution" as defined under the GLBA but do not fall under the purview of a primary financial regulator fall under the regulatory umbrella of the FTC for GLBA purposes.

Federal Trade Commission and General Section 5 Authority

The FTC has jurisdiction over most for-profit organizations and individuals doing business in the United States, other than those in the telecommunications, financial, and transportation industries, which are primarily regulated by other federal agencies. (Note that nonprofits are generally excluded from the FTC's jurisdiction.)[8] The FTC Act was established to regulate questionable business practices and protect consumers. Specifically, Section 5 of the FTC Act prohibits unfair or deceptive acts and practices in commerce, which can include consumer privacy violations and engaging in improper data collection, use, and disclosure practices.[9] Section 5 is also routinely applied to penalize organizations that do not have reasonable data security practices. As such, the FTC can bring enforcement actions for Section 5 violations. Notably, practices inconsistent with FTC guidance have the potential to result in corrective action by the Commission under Section 5 if the Commission finds those practices to be unfair or deceptive after an investigation.

Individuals or companies responsible for the collection, storage, use, disclosure, or other processing of personal information should ensure that those activities do not violate Section 5's prohibition on unfair or deceptive acts or practices.

- The representation, omission, or practice must mislead or be likely to mislead the consumer.
- The consumer's interpretation of the representation, omission, or practice must be reasonable under the circumstances.
- The misleading representation, omission, or practice must be material.[10]

To avoid liability under a deception theory, companies should ensure that statements, including those regarding their practices, do not mislead a consumer in any material way. Further, companies should remain consistent with the promises made to consumers about the collection, use, storage, or dissemination of personal information. The FTC has consistently enforced the "deceptive" prong of Section 5 for privacy violations, including in 2023 with enforcement actions against companies such as GoodRx, BetterHelp, and Vitagene. All of these enforcement actions alleged that these companies failed to uphold the promises they made to consumers regarding how their data was being used or disclosed (in addition to other violations).

In determining whether an act or practice is unfair, the FTC requires that the act or practice "cause{} or {be} likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[11] In determining whether an act or practice is unfair, the FTC "may consider established public policies," but "[s]uch public policy considerations may not serve as a primary basis for [a determination of unfairness]."[12] The FTC has historically relied on the unfairness test in the context of enforcement actions involving companies' misuse of consumer data and, in recent years, has adopted an increasingly broad view of what constitutes unfairness in this sphere, sweeping in such practices as inadequate cybersecurity controls and unnecessary retention of customer data, among others.

The FTC was particularly active in 2023 in using the "unfairness" prong of Section 5 to bring enforcement actions against companies for alleged privacy violations. For example, in the GoodRx and BetterHelp

not obtain consumers' affirmative consent prior to disclosing their health information for this purpose. The implication of the FTC using the "unfairness" prong instead of the "deceptive" prong of Section 5 for privacy enforcement actions is that the FTC is essentially creating new substantive privacy compliance requirements for all companies, regardless of the disclosures they make in their privacy policies or other publicly available documents. The FTC has historically taken this approach with its data security enforcement cases (and continues to do so) but has now expanded this framework to its privacy cases.

The FTC also regularly issues guidance that can provide practitioners insight on how the FTC views certain issues. For example, in 2023, the FTC issued guidance[13] on how companies can better protect health information, as well as how companies can avoid misusing biometric data.[14] These guidance documents, inspired by recent FTC enforcement actions, indicate where the agency is likely to focus its attention in the future.

For practical guidance on use case-specific privacy laws, data specific privacy laws, and comprehensive state privacy laws, follow this link to read the complete article.

Not yet a Practical Guidance subscriber? Follow this link to sign up for a free trial to read the complete article.

Future of Privacy Law

Privacy professionals should remain aware of new legal developments that might affect their matters. Practitioners need to understand whether and how sector, industry, data-specific, and comprehensive privacy laws apply to a particular matter and how to reconcile different legal requirements. At the state level, privacy professionals should be aware of developments in state data-specific laws, as they represent a novel step in the privacy landscape and bring new compliance requirements. Although the recurring similarities among

Finally, practitioners should pay close attention to enforcement actions brought by the FTC and other regulators involving privacy compliance as those will provide insight into how regulators are approaching novel privacy issues.

Kirk Nahra is a partner at WilmerHale. He has been a leading authority on privacy and cybersecurity matters for more than two decades. He co-chairs the firm's Cybersecurity and Privacy Practice as well as the Artificial Intelligence Practice.

Arianna Evers is special counsel at WilmerHale. She advises clients on their development and use of AI and other emerging technologies.

Ali Jessani, Genesis Ruano, and Samuel Kane are associates at WilmerHale.

To find this article in Practical Guidance, follow this research path:

RESEARCH PATH: Data Security & Privacy > Industry Compliance > Practice Notes

Related Content

> CALIFORNIA CONSUMER PRIVACY RESOURCE KIT (CCPA AND C

For extensive coverage of what a new associate should know about data s privacy-related tasks that the associate will encounter in a law firm enviro

> FIRST-YEAR ASSOCIATE RESOURCE KIT: DATA SECURITY AND PR

For an overview of current practical guidance on generative artificial intelli ChatGPT, and similar tools, see

> GENERATIVE ARTIFICIAL INTELLIGENCE (AI) RESOURCE KIT

For resources to guide counsel on applying rules under the Health Insuranc Portability and Accountability Act of 1996 (HIPAA) that impact employers group health plans they sponsor, see

> HIPAA RESOURCE KIT

For a legislation tracker that highlights key comprehensive privacy legislati introduced and/or actively pending at the state level governing the collecti of consumer personal information by private entities, see

> PRIVACY LEGISLATION TRACKER: STATE COMPREHENSIVE CON PRIVACY BILLS (2024)

For an updated listing of state biometric privacy laws applicable to private that are comparable to the Illinois Biometric Information Privacy Act, see

For a weekly updated regulatory enforcement tracker that highlights the re key recent enforcement actions undertaken by the Federal Trade Commiss regarding the regulation and protection of consumer privacy in the United

> FEDERAL TRADE COMMISSION (FTC) CONSUMER PRIVACY ENFORCEMENT TRACKER

For a review of prominent recent guidance and enforcement actions under the Office of Civil Rights at the U.S. Department of Health and Human Ser regarding compliance with HIPAA, see

> HIPAA REGULATORY ENFORCEMENT TRACKER

To watch a video that highlights the fundamentals of the Family Educatior and Privacy Act, including whom and what it applies to, the key requireme enforcement, see

> FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) VIDE

For an evaluation of the Gramm-Leach-Bliley Act's privacy requirements ar comply with them, see

> GRAMM-LEACH-BLILEY ACT (GLBA) PRIVACY REQUIREMENTS

> TELEMARKETING PRIVACY STATE LAW SURVEY

For a discussion of what persons and entities are subject to the Controlling Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SI see

> CAN-SPAM ACT COMPLIANCE

For step-by-step guidance in employment situations for handling consume and investigative consumer reports under the federal Fair Credit Reporting related state and local laws, see

> FAIR CREDIT REPORTING ACT (FCRA) AND STATE MINI-FCRAS: S STEP GUIDANCE FOR COMPLIANCE

For an analysis of how organizations should plan for and manage a data br including notification requirements, see

> DATA BREACH PLANNING AND MANAGEMENT

For more information on the Children's Online Privacy Protection Act, whic parents and legal guardians in control over the collection, use, and disclosu children's personal information, see

> CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA) COMF

(Feb. 17, 2009). **7.** Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999). **8.** 15 U.S.C.S. § 45(a). **9.** 15 U.S.C.S. § 45. **10.** *See* Federal Trade Commission, Policy Statement on Deception (Oct. 14, 1983). **11.** 15 U.S.C.S. § 45(n). **12.** *Id.* **13.** Elisa Jillson, Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases, Federal Trade Commission (July 25, 2023). **14.** Federal Trade Commission, FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023).

TAGS:

FEATURESPECIAL3 DATA SECURITY & PRIVACY

SPRING EDITION 2024 PRACTICE TRENDS