Hashed & Salted | A Privacy and Data Security Update
March 2024

Sensitive Data Takes Center Stage—and Other Trends We're Watching in 2024

Recent actions by states, as well as by the Federal Trade Commission (FTC), suggest that 2024 will be a pivotal year for the implementation and enforcement of new data protection laws, particularly those focused on health-related and other sensitive data.

New state laws are imposing additional responsibilities on handlers of sensitive consumer health data. Federal enforcement actions are calling out businesses that misuse emerging technology such as artificial intelligence (AI), and new privacy-enhancing technologies (PETs) have arrived on the scene. We can also expect heightened enforcement efforts, as well as follow-on class action lawsuits, that will pose significant challenges for businesses that collect and use this health data for targeted marketing or analytics.

New State Laws

The state of Washington enacted the My Health My Data Act (MHMDA), the nation's first privacy-focused law that protects personal health data not covered by the Health Insurance Portability and Accountability Act (HIPAA). The MHMDA applies to legal entities that conduct business in Washington or provide products and services targeted to consumers in the state and determines when and how to collect, process, share or sell consumer health data. The MHMDA covers consumer health data that identifies a consumer's past, present or future physical or mental health status including, but not limited to:

- Individual health conditions, treatments, diseases or diagnoses
- Social, psychological, behavioral and medical interventions
- Health-related surgeries or procedures

- Use or purchase of prescribed medication
- Bodily functions, vital signs or symptoms
- Diagnoses or diagnostic testing, treatment or medication
- Gender-affirming care information
- Reproductive or sexual health information
- Biometric data
- Genetic data
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
- Data that identifies a consumer seeking health care services
- Any information that a regulated entity or a small business, or their respective processors, uses to associate or identify a consumer with the data above that is derived or extrapolated from non-health-related information, such as proxy, derivative, inferred or emergent data used by any means, including algorithms or machine learning

Attorney Advertising

The MHMDA goes into effect on March 31, except for small businesses, which have until June 30 to comply with the new law. For more details about the MHMDA, see Loeb & Loeb's February client alert.

Nevada enacted similar legislation in June 2023. Senate Bill 370, modeled after Washington's MHMDA, aims to protect consumers' sensitive data, including health information. One key difference between the two laws: The Washington law provides consumers with a private right of action, while the Nevada law does not. The Nevada law also takes effect on March 31.

While Washington and Nevada have enacted health data–specific privacy laws, other states have also proactively addressed health-related data, in other ways. Just as its comprehensive privacy law, the Connecticut Data Privacy Act (CTDPA), was set to go into effect in July 2023, Connecticut passed amendments to the law expanding the law's definition of sensitive data to include consumer health data and adding new provisions imposing requirements specific to that data, including provisions prohibiting entities from processing or selling consumer health data without first obtaining consent. In addition to Connecticut's recent amendments, more than a dozen states have passed comprehensive privacy laws that treat health data as part of the category of sensitive data that requires enhanced opt-in or opt-out processes.

Entities covered by these new laws' stringent regulation of the collection and use of sensitive data, including health information, should expect heightened enforcement efforts. This includes the potential for class action suits, which pose significant challenges for businesses that gather sensitive data for targeted marketing or analytics.

FTC Continues Focus on Sensitive Consumer Data

The commission started off the year with enforcement actions against X-Mode Social Inc. and InMarket Media for allegedly collecting and selling identifiable sensitive location data without consumer knowledge, in violation of the FTC Act.

The FTC filed a complaint against data broker X-Mode for failing to implement policies to remove sensitive locations from the raw location data it sold and to ensure that users of its apps, as well as third-party apps that used X-Mode's software development kit, were fully informed about how their location data would be used. For more details about the X-Mode action, see Loeb & Loeb's January Quick Take.

Separately, the agency accused data aggregator InMarket Media of not fully informing consumers and obtaining their consent before collecting and using their location data for advertising and marketing.

The FTC's actions against X-Mode and InMarket Media prohibit the companies from:

- Conducting certain data-related activities
- Using automated technologies
- Adhering to unreasonably long data-retention periods

Additionally, the FTC orders require the companies to:

- Delete and direct third-party deletion of data collected (including deletion of algorithms trained on that data)
- Honor consumer complaints
- Implement reasonable retention policies
- Take steps to verify the source of the data obtained proper consent
- Provide adequate notices to consumers
- Regularly conduct vendor assessments
- Annually certify compliance with the above requirements to the FTC for a certain number of years

The FTC relied on its regulatory authority over both unfair and deceptive practices to bring its claims against X-Mode and InMarket Media.

At the end of February, the FTC continued this line of enforcement with an action against Avast Limited. The FTC accused Avast of unfairly collecting consumer browsing information through its browser extensions and antivirus software, storing it in granular form indefinitely, and selling that data without the appropriate notice and consent. The FTC also asserted that this behavior was an unfair act or practice. Notably, Avast used an algorithm to deidentify the data before sharing it with clients. But the FTC found that step insufficient as Avast attached a unique ID to each browser, which was attached to every website that browser visited and included time stamps, device types and general location information. Additionally, Avast failed to prohibit its buyers from reidentifying data. The settlement order:

- Prohibits Avast from selling browsing data
- Requires affirmative express consent for selling or leasing browsing data from non-Avast products to third parties for advertising purposes

- Requires data and model deletion
- Requires Avast to implement a comprehensive privacy program

Following the decision, the FTC published a blog post in which it claimed that browsing data was sensitive data "full stop." While the Avast decision speaks to certain specific instances of sensitive browsing behavior, the blog post goes beyond that to classify all browsing data as sensitive. This position goes beyond previous statements and is not aligned with current industry practices. It is unclear whether the FTC could impose this position on a different set of facts, but it does signal the agency's desire to do so.

At the end of last year, Rite Aid was in the FTC's hot seat for deploying AI-based facial recognition technology for security purposes without taking reasonable measures to prevent harm to consumers. Between 2012 and 2020, Rite Aid allegedly used AI-based facial recognition technology to identify customers who may have shoplifted or engaged in other problematic behavior. In the process, some customers were wrongly accused by employees because the store's facial recognition technology falsely identified customers as matching someone who had previously been flagged as a shoplifter or other type of problem customer, according to the FTC.

The FTC barred Rite Aid from using facial recognition technology for security purposes for five years. Rite Aid will be required to discontinue using the AI technology if it cannot control potential risks to consumers.

Other Trends We're Watching

Privacy-Enhancing Technologies (PETs). In response to escalating data restrictions, PETs are expected to gain more traction in the coming year. Companies are increasingly exploring PETs to facilitate targeted advertising while safeguarding user privacy. That means regulators will follow suit by turning more attention to these technologies, which will necessitate robust evaluation processes to ensure compliance with stringent privacy standards.

The FTC defines PETs, such as end-to-end encryption, as "a broad set of tools and methods aimed at providing ways to build products and functionality while protecting the privacy of users' data." PETs allow a company to offer products and services without having any access (or only limited access) to a user's data. While the concept of PETs is promising, the FTC has already warned that companies making representations to consumers about their use of PETs must follow the law and that they must ensure that any privacy claims or representations are accurate.

PETs can't replace a robust privacy program, and users should keep in mind that new technology always runs the risk of implementation issues.

Consent-Based Data Usage. Opt-in consent mechanisms may be getting more attention this year. Despite existing regulations, widespread adoption of opt-in consent mechanisms for sensitive data usage remains elusive. However, mounting regulatory pressures may prompt companies to revisit their strategies, potentially offering incentives to secure consumer consent. This shift would mirror the trend occurring in the European Union and underscores the imperative for businesses to adapt their data privacy models to align with evolving regulatory landscapes.

Auditing and Accountability. State privacy laws mandate comprehensive auditing, internal assessments and accountability measures that require companies to demonstrate their adherence to contractual obligations and regulatory standards. Expect to see heightened scrutiny from state regulators, including the California Privacy Protection Agency (CPPA), with potential implications emerging for cybersecurity assessments and risk evaluations.

Continued State-Centric Regulation. Speaking of state regulation, with no federal privacy legislation in sight, the regulatory landscape continues to be dominated by a patchwork of state laws. Businesses will have to navigate increasingly complex compliance requirements tailored to individual state mandates, stressing the continuing importance of proactive regulatory monitoring and strategic adaptation in 2024.

Proactive measures to enhance data-governance frameworks, cultivate transparency and prioritize compliance efforts remain essential to mitigate regulatory risks and safeguard consumer trust.

Related Professional

Jessica B. Lee . . . . jblee@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.