Sourcepoint

GUIDE

NAVIGATING THE MAZE: U.S. PRIVACY LAWS AND SENSITIVE DATA

This guide aims to bring some clarity to U.S. privacy laws – especially those regarding sensitive data — and provide practical insights for Data Protection Officers, Chief Privacy Officers, digital marketers, and others tasked with developing data protection initiatives.

sourcepoint.com

EXECUTIVE SUMMARY

As data becomes increasingly central to our lives and businesses, understanding the legal frameworks that govern sensitive data is more critical than ever. Yet, with an evolving landscape of federal and state laws in the U.S., along with a patchwork of industry standards, navigating these laws can be tricky.

This guide aims to bring some clarity to U.S. privacy regulations — especially those regarding sensitive data — and provide practical insights for Data Protection Officers, Chief Privacy Officers, and others tasked with developing data protection initiatives. By implementing focused and thoughtful strategies, organizations can safeguard data effectively and comply with the ever-changing regulatory standards.

The objective of this guide is to:

- Explain how different laws in the U.S. define sensitive data
- Introduce the entities enforcing sensitive data privacy, and how
- Share what companies can do to safeguard sensitive information and protect themselves
- Deliver a step-by-step framework for evaluating your sensitive data practices

84 %

of U.S. state comprehensive privacy laws require opt-in consent to process sensitive data

Maryland

is the first state to **prohibit** processing sensitive data unless strictly necessary to provide products or services.

Washington

is the first state to provide for a private **right of action** if sensitive data under the “My Health, My Data” law is improperly processed.

INTRODUCTION

In the U.S., there is no comprehensive privacy law at the federal level, similar to GDPR in Europe, that governs data privacy for all U.S. states. Rather, privacy is regulated through a patchwork of state, sectoral and federal laws.

As of July 2024, nineteen U.S. states have enacted comprehensive consumer data privacy laws, each including provisions specifically addressing certain types of personal data that are arguably higher risk or more sensitive than other types of personal data (e.g., sexual orientation or racial or ethnic origin). At the federal level, the FTC has the authority under Section 5 of the FTC Act to address matters that constitute unfair or deceptive acts or practices (UDAP) against entities in its jurisdiction. Most U.S. states also have UDAP laws.

These new state privacy laws and recent FTC enforcement have sought to **expand definitions of the personal and sensitive data that is subject to protection**, introducing another layer of complexity for data and privacy professionals.

In this guide, we explore these broadening definitions and what this means for your data and privacy programs.

CONTENTS

PART ONE: DEFINING SENSITIVE DATA

What constitutes sensitive data? The nuances of that question, especially in the U.S., could fill dozens of pages; remember that the absence of a federal framework governing the definition of "sensitive" has left individual states to step in and define this for themselves, leading to variance from state to state.

For example, many states emphasize the protection of religious beliefs as sensitive data, however California includes the protection of philosophical beliefs. There are also small, seemingly semantic (yet potentially impactful), differences regarding the protection of sexual orientation as opposed to sex life or sexuality. Though Washington state's "My Health, My Data" law only applies to "consumer health data", the definition and application of the term is quite broad, including health-related inferences derived or extrapolated from non-health data.

Let's start a bit more simply. Most state and federal laws addressing sensitive data fall into one or more of these categories:

- Health data
- Racial or ethnic origin
- Citizenship or immigration status
- Religious beliefs
- Sexual orientation
- Precise geolocation
- Genetic or biometric data
- Financial data
- Children's data

Sensitive data inferences

But the sensitive data categories listed above are just one piece of the puzzle. Sensitive data *inferences* are becoming a focal point in privacy legislation, particularly with the advent of laws such as Washington's "My Health, My Data" Act.

A distinguishing feature of the Washington Act is its broad definition of consumer health data. The law extends protection not just to explicit health information but also to health-related inferences derived or extrapolated from non-health data. This includes data that identifies or infers a person's past, present, or future physical or mental health status, social and behavioral interventions, and even the use or purchase of prescribed medications. Additionally, it includes data about bodily functions and vital signs, and precise location information that could indicate attempts to receive health services or supplies.

For example, if a consumer's purchase history includes prenatal vitamins and maternity clothing, an inference might be made about the consumer's pregnancy status. Per the Washington Attorney General's published FAQs, such an inference would require the same level of consent as explicit health information. In their view, consent is crucial in preventing unauthorized use of inferred health data, which can be just as sensitive as direct health information.

Washington is not alone in this stringent approach. Nevada and Colorado have also implemented consent requirements for sensitive data inferences. In Washington and Nevada, consent is necessary for processing consumer health data that is not needed to provide a requested product or service, including health-related inferences derived from non-health data. A pertinent example is the Washington AG's discussion of assignment of a "pregnancy prediction score" to shoppers based on their purchase of specific products. This type of profiling, without consent, would be prohibited under these laws.

Colorado's legislation is slightly broader, encompassing all sensitive data, including sensitive data inferences that, alone or in combination with other data, can reveal sensitive information. An example described in the law is the inference of an individual's sexual orientation from their web browsing history, especially when combined with other personal data. This comprehensive protection highlights the state's commitment to safeguarding personal information against unauthorized inferences that could lead to discrimination or other harms.

The rationale behind these laws may reflect a growing perception that inferences made from seemingly innocuous data can reveal highly sensitive information about individuals.

An FTC director described the potential harms of such inferences thusly: "Standing alone, these data points may pose an incalculable risk to personal privacy. Now consider the unprecedented intrusion when these connected devices and technology companies collect that data, combine it, and sell or monetize it. This isn't the stuff of dystopian fiction. It's a question consumers are asking right now."

With the advent of big data analytics, it has become increasingly easy for organizations to draw detailed inferences about a person's health, behavior, and personal life from data that was not originally collected for those purposes. Regulators argue that inferences can then be used in ways that are not always transparent to the consumer, such as targeted advertising, eligibility determinations, or even employment decisions.

SENSITIVE DATA DEFINITIONS

Download our state- by-state sensitive data definition chart.

PART TWO: ENFORCEMENT & AGENCIES

Enforcement is an important component of any regulatory system. It's important to understand the entities involved in both holding organizations accountable for privacy law requirements and facilitating consumer complaints.

State attorneys general enforcement

Many of the state attorneys general have been enforcing the sensitive data requirements of state privacy laws; it just isn't always made public.

A six-month report published by the Connecticut Office of the Attorney General reveals that early enforcement activity under the Connecticut Data Protection Act (CTDPA) focused on sensitive and teens' data in particular.

Per the report, notices of violation were issued to various entities, including a grocery store using biometric software without proper consent, a major web service provider deploying palm recognition services, and a car brand with connected vehicle data concerns. Additionally, a genetic testing company faced scrutiny after a data breach exposed sensitive records. For teens' data, a peer messaging app was targeted for its data practices.

These enforcement efforts highlight the importance of obtaining consent for collecting and using sensitive data, ensuring data security measures, and providing heightened protections for minors in Connecticut, and other relevant jurisdictions.

Federal enforcement of health data privacy

The FTC has been active in enforcing health data privacy through two avenues: (1) Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices and (2) the Health Breach Notification Rule (HBNR), a rule issued pursuant to the FTC Act that applies to certain entities not covered by HIPAA and requires notification to consumers and the FTC of any breach of unsecured identifiable health information.

Over the last few years, the FTC has broadened the definition of "breach" under the HBNR to include any sharing of health information without consent from the user. They have reinforced HBNR against health apps such as GoodRx and Premom that weren't getting consent for the sharing of health data with third parties.

WHAT IS SECTION 5 OF THE FTC ACT?

The FTC Act provides the Federal Trade Commission with investigative and enforcement authority as it relates to the prevention of unfair and deceptive business practices.

Per Section 5, practices are deceptive if they mislead consumers and unfair if they cause substantial, unavoidable harm without countervailing benefits.

Under this interpretation of the HBNR, Premom was subject to a multistate settlement with the FTC for allegedly disclosing sensitive health data, such as facts about a user's sexual and reproductive health, to third-party tracking SDKs.

GoodRx was also sanctioned for allegedly failing to notify consumers, the FTC, and the media about the company's unauthorized disclosure of health data to its advertising partners, as is required by the HBNR. Additionally, GoodRx was found to have violated the FTC Act by sharing sensitive personal health information for years with advertising companies and platforms — contrary to its claims — thus misleading consumers about the extent of their data privacy.

Meanwhile, an FTC complaint against another health app, BetterHelp, Inc., focuses on violations of the FTC Act, specifically for unfair and deceptive practices. These include collecting, using, and disclosing consumers' health information without affirmative express consent, and misrepresenting the privacy and security of that information. Additionally, BetterHelp allegedly falsely implied compliance with HIPAA by displaying seals suggesting third-party verification of their practices, which was not the case. Per the FTC, these actions led to substantial consumer harm, including potential stigma, embarrassment, and financial injury due to inflated service prices based on deceptive privacy assurances.

The consequences for these companies were significant. In the case of GoodRx and BetterHelp, the companies were required to pay civil penalties of $1.5 and $7.8 million, respectively, in addition to taking corrective action to prevent future unauthorized disclosure of users' sensitive data.

HEATH DATA ENFORCEMENT

Learn more about health data enforcement, including 13 takeaways from recent FTC actions, here.

Federal enforcement of financial data privacy

Five tax prep companies – H&R Block, Intuit, TaxAct, Tax Slayer, and Ramsey Solutions – were warned by the FTC that they may face civil penalties for sharing personal data from taxpayers through tracking pixels. In some cases, these tracking pixels could pick up sensitive information and share it with third parties, without the express consent of the user.

Children's privacy

Aside from health and financial data, the information of children, specifically those under 13, has been a recent minefield of enforcement. The Children's Online Privacy Protection Act – better known as COPPA – imposes requirements on websites or online services directed to children under 13 years of age that are collecting personal information about them, even without having actual knowledge of their age.

Epic Games, the maker of video game Fortnite, agreed to pay a $275 million penalty for violating COPPA and was forced to adopt new privacy default settings for its users. The game's default[3] settings allegedly enabled live text and voice communications between young gamers and strangers.

Amazon's Alexa voice assistant was also caught in the COPPA crosshairs after it was alleged that the service retained voice and geolocation information associated with young users indefinitely by default and failed to honor requests to delete voice and geolocation information. The company settled for $25 million.

Enforcement of children's privacy is happening on the state level as well. For example, in 2024, the California Attorney General and LA City Attorney settled with gaming publisher Tilting Point Media for $500,000 over allegations that the company collected and shared children's data without parental consent for children under 13 and user consent for children 13-15, violating the CCPA and COPPA. Tilting Point must now obtain the proper consent, use a compliant age screen, and review SDKs within its apps. The investigation found the age screen in SpongeBob: Krusty Cook-Off did not encourage accurate age entry and that SDKs were misconfigured, leading to unauthorized data collection.

We can also expect to see enforcement of children's privacy on the east coast soon. Effective in June 2025, the New York Child Data Protection Act requires digital services directed to minors under 18, or those knowing they have such users, to get "informed consent" for non-essential data processing.

Geolocation data and browsing data

Somewhat more controversially for the marketing industry has been the FTC's new emphasis on the sensitivity of geolocation and browsing data data due to its potential to reveal personal details. The FTC's enforcement actions against Avast, an antivirus software company; data broker X-Mode; and marketing firm InMarket underscore the agency's position on geolocation and browsing data data as sensitive.

The FTC highlighted, "Browsing and location data paint an intimate picture of a person's life, including their religious affiliations, health and medical conditions, financial status, and sexual orientation." These companies must now implement stricter privacy measures and obtain user consent.

Additionally, in 2022 FTC sued Kochava, a data analytics company, for selling location data tracking visits to sensitive places like reproductive health clinics and places of worship, reinforcing the need for stringent data privacy protections. Though as of this writing in 2024, Kochava's motion to dismiss was grated with leave to amend, and the FTC has filed an amended complaint.

*

These are just a few examples of the real consequences that companies have faced for failing to respect the requirements around collection, processing, and protection of sensitive information. And while it can be difficult to stay abreast of the changing requirements and technologies, it is a provider's responsibility to be aware of the most recent regulation and take the necessary steps to comply.

But you don't have to do this alone. In the next section, we'll tackle how you can build a focused and effective strategy to identify, evaluate, and protect any data you (or third parties) collect.

PART THREE: PROCESSING SENSITIVE DATA

Now that we have a broad understanding of what constitutes sensitive data, it's important to understand what is required if you are processing or sharing sensitive data. And perhaps unsurprisingly, the requirements also vary from state to state and law to law, though there is significant overlap.

Here are some potential requirements you may have to comply with in order to process sensitive data:

- Data Protection Impact Assessments (DPIAs)
- Enhanced safeguards
- Enhanced disclosures
- Breach notification
- Outright restrictions / bans
- Consent / opt-out rights
- Additional contractual requirements

Collecting consent

Most state comprehensive privacy laws require affirmative consent to process sensitive data. This often means that organizations must obtain explicit permission before collecting or using this data, thereby respecting individual privacy preferences.

Using a Consent Management Platform (CMP) to collect consent for data processing is an effective way to enable compliance with U.S. privacy laws like Virginia's Consumer Data Protection Act (CDPA), Oregon's Oregon Consumer Privacy Act (OCPA), the Texas Data Privacy and Security Act (TDPSA) and others.

A CMP can enable you and your team to configure the appropriate user experience for collecting consent, including language in the notice, placement of the notice on your digital property, as well as the specific categories of data you are collecting and for what purpose. Many CMPs also leverage industry frameworks, which allow a standard mechanism to communicate both consent choices related to sensitive data and opt out choices for personal information. Depending on the framework, these signals can be communicated across multiple properties or throughout a digital ecosystem.

PART FOUR: NAVIGATING SENSITIVE DATA

As we can see, the repercussions of violating privacy laws are costly. Let's explore a 3-pronged approach that you can use to reduce your risk and avoid becoming the next GoodRx or Avast.

- **Step 1: Identify** - Understand what data you and your partners are collecting, from what sources, and for what purposes
- **Step 2: Assess** - Evaluate whether the data you collect is sensitive or could trigger sensitive data laws, and what kind of risk you face
- **Step 3: Take Action** - Implement strategies to reduce risk based on your assessment

1. Identify

The identification stage is about gathering a comprehensive understanding about what data you and your third party partners are collecting. It's equally important to know not only what you are collecting, but *how* you are collecting this information, for what purpose, and how long you will retain it. Again, it's important to conduct this exercise for yourself *and* your partners.

Once you have this information documented, you can move on to the second stage.

2. Assess

After you have identified all the data you or your vendors collect, you can now assess how that data could put you at risk for triggering certain laws and regulations.

You will want to understand which laws and regulations apply to your business and consumers. You'll also want to consider whether any of the data you or your partners collect could be considered sensitive, or when combined with other data, if that data could reveal sensitive information or inferences. For example, collecting consumer's precise geolocation data showing that they visited a church, mosque, or synagogue to infer their religious beliefs could constitute a sensitive data inference.

Lastly, you'll want to know if collecting this data is necessary. A regulatory nightmare could be avoided if you determine there are reasonable alternatives to collecting the information you seek. These assessments will be subjective and will largely depend on your company's tolerance for risk. But conversations (and documentation!) in this stage are a crucial part of building your strategy.

3. Take action

The last step in this process is to determine what gaps or risks may exist and how you want to address them. You may find that none of this applies and that you and your partners aren't collecting data that could be considered sensitive. However, based on what we've covered in this e-book so far, chances are that you have at least some level of risk based on how broadly sensitive data is defined across these state laws.

Taking action can take different forms. Some of these include requirements we discussed in Part Three, such as enhanced disclosures to consumers about what is being collected, or different mechanisms for collecting and storing sensitive data. It could also include asking for consent or allowing opt-out rights for users.

Additionally, leveraging Privacy-Enhancing Technologies (PETs) can significantly mitigate regulatory risks associated with processing sensitive data. PETs, such as data anonymization, encryption, and differential privacy, may be appropriate in certain circumstances to ensure that sensitive information remains protected throughout its lifecycle. These technologies may help organizations to enhance data security, comply with stringent regulations, and build consumer trust, all while minimizing the potential for data breaches and unauthorized access. It is important to fully understand a particular PET before implementing it though. Although PETs can be useful tools to reduce risk in certain circumstances, implementing them does not necessary mean you can throw all other privacy obligations out the window.

Even if not required by law, it's a good idea to go through a sensitive data audit exercise anyway — even if just for internal purposes — to help you think through the risks and benefits of sensitive data and any measures you can take to mitigate that risk.

SENSITIVE DATA FRAMEWORK

Whatever path you take, it's important to create an audit trail of your analysis and decision-making.

Download our worksheet to help guide you through this process and assist with documentation.

NOTE: This worksheet is not intended to take the place of any legally required assessment measures. Please consult with your legal counsel for legal requirements applicable to your company.

CONCLUSION

The expansion of what constitutes sensitive data – as well as state-specific privacy regulation – shows no signs of slowing down. Data privacy professionals and their teams must thoroughly understand and take action to keep their organizations compliant.

Key Takeaways

- Definitions of sensitive data are **broadening** and continue to vary by state
- Enforcement agencies like the FTC are taking a closer look at the companies responsible for special categories of sensitive data – such as finance, health, and children's data – **and the technologies they use**
- A documented and focused approach to identify data types you collect, **assess the potential risks**, and take action to ensure compliance is the best strategy for success
- **Knowledge is power!** Seek out resources, partners, and technologies that allow you to make informed decisions

As U.S. privacy law continues to evolve, the importance of staying informed and prepared cannot be overstated. We hope this ebook has clarified the complex definitions surrounding sensitive data, regulatory bodies affecting change, and actionable strategies to use against the evolving privacy landscape. By adhering to these principles, you and your teams can make more educated decisions about your data privacy and protection strategies.

About Sourcepoint

Sourcepoint is the practical data privacy software company trusted by the world's most influential brands. Supporting over 30 billion consumer touchpoints per month, Sourcepoint offers enterprise-grade privacy automation for complex, dynamic compliance challenges. Sourcepoint has offices in New York, Berlin, and London.

To stay informed on the latest developments in data privacy, subscribe to Sourcepoint's **weekly recap of privacy news** or register for one of our upcoming **webinars**.

DISCLAIMER: This guide is meant for informational purposes only and does not constitute legal advice. Please consult with your legal counsel regarding your own strategy or mechanisms for implementation.