privado

FTC's Crackdown on Health Data Sharing

What it means and how to comply

AUTHORS

Debra J Farber CEO, Principled LLC

Vaibhav Antil CEO, Privado.ai

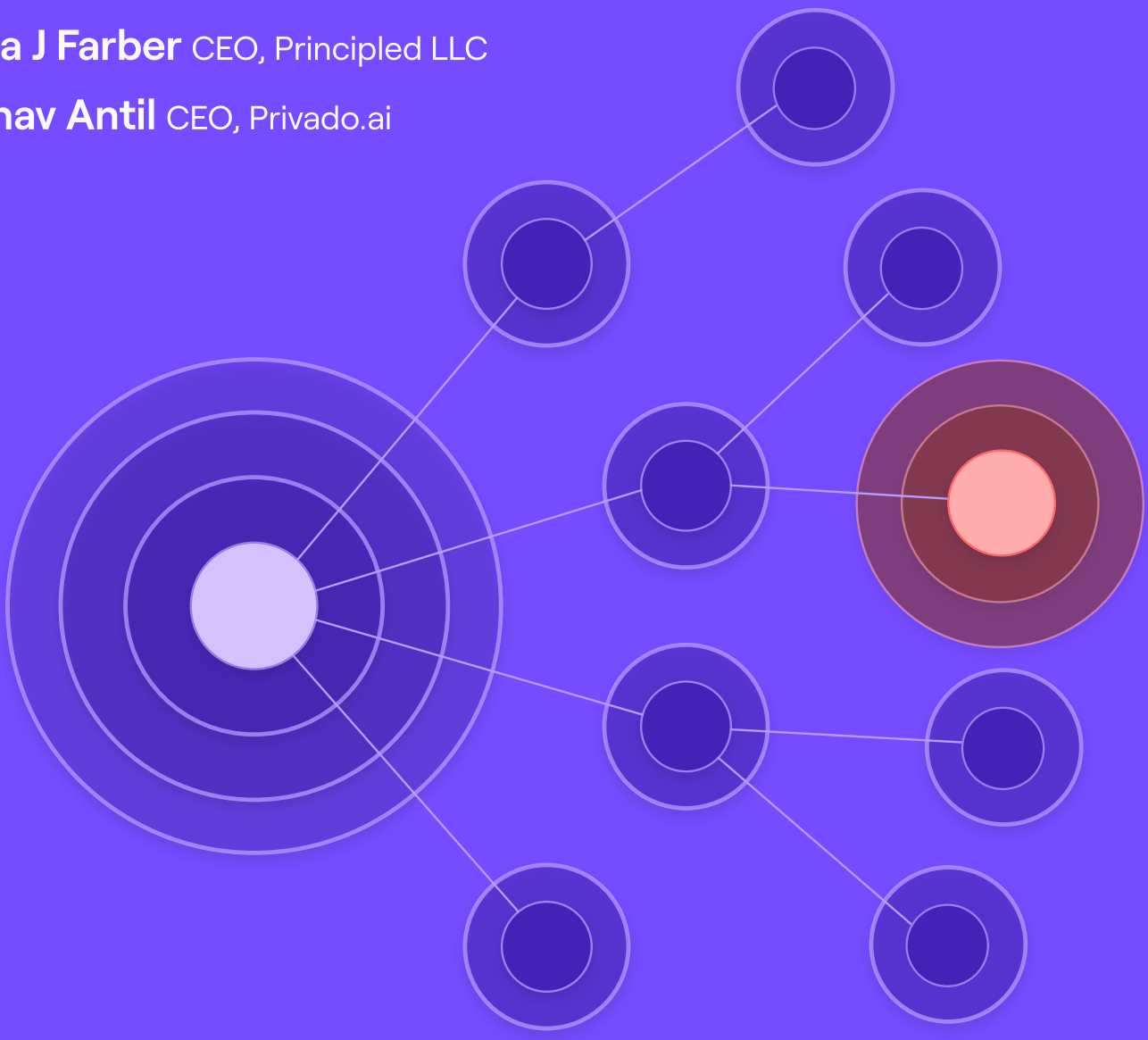


Table of Contents

Overview & Objective

In the aftermath of Roe v. Wade, 410 U.S. 113 (1973), the FTC shared guidance declaring its commitment to crack down on illegal data usage & data sharing by software organizations.

This publication covers the guidance issued by the FTC and U.S. Department of Health & Human Services [HHS] since the Dobbs case overturned Roe v. Wade and its implications. The guide further examines the actions taken by the United States federal government, outlines how organizations can avoid illegal data usage & sharing, and explains how to protect location and health data collected and used by consumer health apps.

Executive Summary

- With Roe v. Wade, 410 U.S. 113 (1973) overturned by the Supreme Court of the United States, individuals seeking abortion in certain states face a renewed fear of criminal prosecution if their data is shared or leaked. To remedy this, the Federal Government of the United States came out with a directive to the FTC to protect users' health & location data, along with a couple of proposed bills from other senators.

- The US Department of Health & Human Services issued guidance explaining how the federal law protects private medical information & clarifies that health care providers who are bound by HIPAA's Privacy and Security Rules are not required to disclose information to third parties. The guidance further explains what data types it considers sensitive; the illegal data flows developers should be on the lookout for; and warns companies about deceptive statements around anonymization.

- To comply with the FTC's guidance, organizations must:

  - Discover the data types collected and shared by your organization's products.

  - Audit the data flowing from your product to third parties, and check what it retains.

  - Check the claims you're making in your privacy notices against your product's code to ensure it's consistent.

Section: 1

Roe vs Wade judgment: Privacy implications & real-life risks

Roe vs Wade judgment: Privacy implications & real-life risks

With Roe v. Wade, 410 U.S. 113 (1973) overturned, there's a renewed fear of criminal prosecution among individuals seeking an abortion in certain states. Because any data about them could now, if it's shared, can lead to them getting prosecuted for murder or assisted murder.

To provide relief to individuals, United States President, Joe Biden, issued an Executive Order directing he FTC to protect users' health & location data, and Senator Elizabeth Warren announced a bill, called the Health and Location Protection Act, to shore up this risk to individuals and prevent privacy harm.

Aftermath of Roe v. Wade, 410 U.S. 113 (1973) judgment

1. Sharing health data (e.g., pregnancy and abortions) may expose individuals to criminal prosecution (e.g., murder) & civil lawsuits in some states.
2. The Federal Government's directive for FTC to protect the health & location data of users
3. Sen. Elizabeth Warren (D-MA)'s proposed bill — the Health and Location Protection Act

Real-life risk: Sharing health data by organizations

The current practice of collecting and retaining extensive digital information by organizations on individuals can be used as a tool to crack down on people seeking reproductive care in certain states to criminal prosecution and civil lawsuits.

This practice is entirely legal under the current laws. As a result, there's a state versus federal government stand-off within the United States, with each stakeholder holding a varying degree of desire to legislate or protect what they believe is worth protecting.

> *We've already seen, but we anticipate that tech companies will be issued subpoenas for people's search histories and search information.*

Dana Sussman
Deputy executive director,
National Advocates for Pregnant Women

Implication: Biden's Executive Order to the FTC

The federal government's Executive Branch moved quickly to support individuals' right to reproductive privacy. So, President Biden issued a directive to the FTC to protect users' health and location data in relation to reproductive healthcare services. Gist of the President's executive order:

*"To address the potential threat to patient privacy caused by the transfer and sale of sensitive health-related data and by **digital surveillance related to reproductive healthcare services,** and to protect people seeking reproductive health services from fraudulent schemes or deceptive practices."*

"The Chair of the Federal Trade Commission (FTC) is encouraged to consider actions ... to protect consumers' privacy when seeking information about and provision of reproductive healthcare services."

The Health and Location Protection Act

Furthermore, Senator Warren has proposed a bill: The Health and Location Protection Act, which prohibits the sale or transfer of information about location and health data that is not covered by HIPAA. If passed, it explicitly tasks the FTC with developing rules to implement the ban.

The bill introduces levers that the FTC and State Attorneys General can use to enforce compliance if they find companies violating the law. So, for instance, they could force an organization that is collecting reproductive health data fraudulently or deceptively to delete it on command.

If an organization is found in violation, the government agencies could obtain a permanent temporary or preliminary injunction and civil penalties.

The bill introduces an innovative tool: disgorgement of unjust enrichment.

It would penalize organizations that falsely claim their ability to anonymize data before selling or using it for analysis. With disgorgement, the agencies can not only make companies delete any data but also force a company to throw away any AI models they might have trained with this data.

Section: 2

FTC & HHS guidance to organizations

FTC and HHS's guidance

Consumer health apps that collect and share health information ("Vendors of Personal Health Records") are not covered by HIPAA, yet must comply with the Federal Trade Commission (FTC) Act, which means that they must ensure that their disclosure statements (e.g. privacy policies, consent disclosures, etc.) are not deceptive; Such apps must be transparent about their practices and may not lie to users about personal data collection and usage. Furthermore, such health apps must adhere to the FTC's Health Breach Notification Rule if there's a compromise of unsecured individually identifiable health information.

Federal Trade Commission

The FTC's guidance addresses its authority to regulate when it comes to health information not covered by HIPAA.

- Vendors of personal health records (i.e., consumer health apps) must put safeguards in place to protect individually identifiable health information and ensure they do not use or disclose your health information improperly.
- These vendors must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- They must have procedures in place to limit who can view and access your individually identifiable health information and train employees on how to protect that information.

The FTC's guidance can be put into three buckets:

1. Data Types considered sensitive by the FTC
2. Deceptive data flows and sharing
3. Unclear statements about anonymized data use

Data types

The two data types considered sensitive by the FTC [and mentioned in the Health and Location Protection Act] are: 1) location and 2) health data. By combining both data types, organizations might be able to re-identify individuals tied to their health information. If your org collects location and health data, ensure that you secure these data types, conduct a threat model for ways in which internal employees and third-party partners can abuse this data, and put in place appropriate technical measures that thwart any re-identification efforts.

Data flow

The FTC is wary of sensitive data sharing with third-parties where unaudited data is transmitted from the organization to third-parties - like external SDKs or data brokers - and could be sold to state governments or companies that might use it for targeting or profiling without consent. Organizations should audit their data flows and be transparent about them in their privacy notices.

Anonymization

Organizations have collected excessive personal data on people, so a person could be re-identified even with a little piece of information. Since there is no technical standard for data anonymization, each organization may have its definition. If an organization makes public claims that it anonymizes this data, but the dataset still has data points that can be used to re-identify people or can easily be combined with another dataset to re-identify, then the org may be liable for an deceptive trade practice under The FTC Act and opens itself up to regulatory enforcement, fines, and loss of consumer trust .

Health and Human Services

The Office of Civil Rights, a division within Health and Human Services, which enforces any HIPAA violation by Covered Entities or their Business Associates, issued guidance for individuals about the need to protect the privacy and security of their health information that is not covered under HIPAA when using their cell phones or tablets.

The guidance:

The HIPAA Rules generally do not protect the privacy or security of your health information when it is accessed through or stored on your personal cell phones or tablets. *The HIPAA Rules apply only when PHI is created, received, maintained, or transmitted by covered entities and business associates.*

It is not possible to eliminate your digital footprint entirely. But there are steps you can take to decrease how your cell phone or tablet collects and shares your health and other personal information, such as where you go and what you do, without your knowledge.

Read more

Section: 3

Steps to comply with the guidance

Steps to Comply with the guidance

Here's a step-by-step plan to understand how you can comply with the guidance.

FTC's guidance can be divided into three large buckets:

1. Data types collected and shared
2. Privacy notices
3. Data flow to third-parties via SDKs & APIs

Identifying data types

Most apps collect some information about the user. Apps either use the collected data to provide a service, monetize your data, or to improve the product -- with your consent.

But some data types collected by the apps are deemed sensitive by the FTC.

Health

Your apps can collect health data when users fill out a form about their weight or health condition manually, from smart connected devices, and from phone sensors.

Location

Location can be collected in multiple ways: by permission in a mobile app, GPS, a connected smart device, or IP addresses. If an IP address is flowing to address the case, an organization can figure out the course location of the user from that. Thus, IP address itself is enough to link back to one's location.

Device identifier

Device identifiers include IDFA in Apple devices and unique device IDs for Android and PCs. These IDs can be used to identify a person individually and then target them.

Indirect sensitive data

This data might not fall in the general category when you think of sensitive data, but they could identify a person and reveal a lot of information about them.

- Email addresses
  Example: for users who have a mental health app, and if an email address for the app gets breached, much can be gleaned about that person from just associating their email address with the mental health app.
- Other Apps on phone
  Example: if a user has any other sensitive app on their device, like a period tracker or a diabetes management app, and an unassociated application collects information on the apps installed. That alone is enough to profile them.

Privacy notices

Privacy Notice requirements have matured from needing a simple link at the bottom of a website - where you talk about how your organization handles user data - to "just-in-time" notices deployed across app stores, inside forms, and within other places inside your product. Because your organization makes privacy promises to your users at multiple places, not just in your privacy policy notice – each of which must be monitored and kept updated.

Privacy notices example:

- Apple app store nutrition labels
- Play Store data safety labels
- Notices sprinkled across your app

Example: you might take location permission and then give context as to why your organization is needs to collect location permission, and then consent becomes another thing to monitor.

To avoid privacy harms to users of your app and to comply with regulations, you should audit these notices and your data collection and use practices to ensure that whatever you're promising matches what your app's code is doing.

Data flow to third-parties

Identify the data flow from your app to third parties by auditing your code. Start by auditing the SDKs and APIs connected to your app, which are often used to track app usage, data warehousing, and advertising.

If you see any of them are data brokers, make sure to go back and audit those flows and determine what data is shared with each of them, and that your privacy policy commitments are actually reflected in your code.

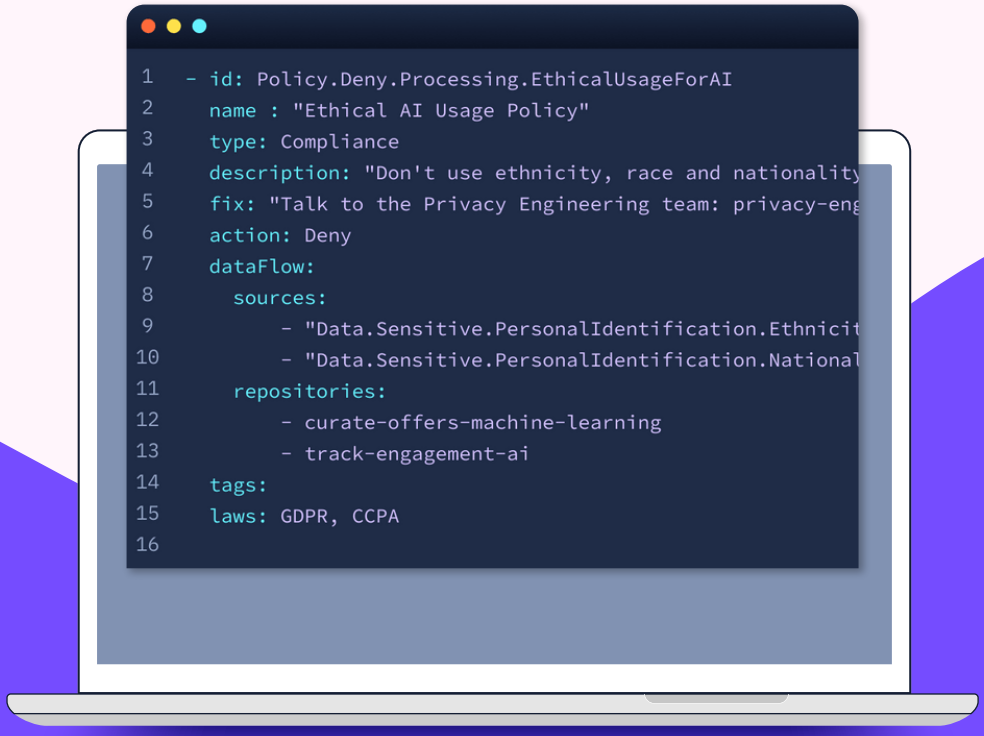
Section: 4

Embed privacy policies as a guardrail in Software Development Life Cycle (SDLC) with Privado

Privado:
The Privacy scanning tool

Privado is a static code scanning solution purpose-built for security & privacy teams. The tool connects with source code management tools, scans the code, and helps you discover the personal data collected by your product, how data is used, the status of your data flows, and where there are leakages to logs. Privado also flags privacy issues in the code for GDPR violations, CCPA and other state law violations, or common weakness enumeration (CWE) vulnerabilities.

Privado enables organizations to enforce the promises it made in user-facing privacy policies during code checks. Suppose a product team proposes a new, out-of-scope feature whose code doesn't comply with the organization's users-facing privacy notices. Privado detects it and creates an alert that stops the feature from going into production and provides just-in-time guidance on preventing the violation within integrated developer tools like GitHub and JIRA.



About Privado Inc

At Privado, we have a core belief that people deeply care about safeguarding their privacy from governments and corporations alike and that trust and privacy are critical for the internet economy to function. Our mission is to empower developers to create privacy-first products that prevent harm to people, comply with global data protection laws, and enable trust from stakeholders.

Our static code analysis platform lets you track whether your developers are sharing personal data across third-party apps and what are those data types. Schedule a demo to learn how we track personal data flows to third-parties.

Great brands trust us:

Contact:

hello@privado.ai

@PrivadoHQ

Privado.ai