PROGRAM MATERIALS
Program #3620
January 30, 2026

Data Tracking Cases and Legislative Trends

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Data Tracking Cases and Legislative Trends.

Overview & Agenda

- Tracking and using consumer's data without consent is a high stakes game. From class actions to federal and state government enforcement actions, the settlements are significant and show no signs of slowing down. The purpose of this webinar is to look at the Federal Trade Commission's focus, as well as state governments laws and regulations. Compliance suggestions will also be addressed.
- Agenda
  - What is data tracking and consumer privacy?
  - Current enforcement actions & class action settlements.
  - Legislative initiatives
  - Risk mitigation.
  - Conclusion

Threshold Questions & Answer

- Have you ever wondered why some online ads you see are targeted to your tastes and interests?
- Or how websites or apps remember your preferences from visit to visit?

The answer is online tracking.

Data Tracking & Consumer Privacy

How and Why Websites and Apps Track You Online According to the Federal Trade Commission.

- Websites may track your online activity by using a cookie or pixel to identify you even after you leave the site.
  - Computer cookies are files that allow websites and web servers to remember your device and browsing activity.
  - Pixels are "**the smallest unit of an image on a television or computer screen**, used to measure or describe how clear an image is."
- Or they may use device fingerprinting — a technique that uses your browser's unique configurations and settings to track your activity.
- When you use an app on your smartphone, advertisers may use a unique advertising identifier to track you.
- Companies also may track your activity on different internet-connected devices, like your laptop and your smartphone.

So why do companies want to track your online activity?

•save your preferences and information, like your username or things you left in your shopping cart
•show you personalized content like local weather and stories about topics you're interested in
•gather analytics about your visit to a website, like the pages you visited,
how much time you spent on the site, and the type of device and browser you used
•remember the things you searched for online
•show you personalized ads based on your browsing history or your location

First-Party Versus Third-Party Tracking

- When a website you visit tracks you, that's **first-party tracking**.
- When a website you visit lets another company track you, that's **third-party tracking**.

The caveat with third-party tracking? Notice to consumers is required, the ability to opt-out needs to be provided and depending on the data type (e.g., individually identifiable health information (IIHI) or sensitive personally identifiable information (PII)).

Third-Party Tracking

- Third-party tracking companies can track you across most websites you visit.
- Third-party tracking lets advertisers show you targeted ads based on your interests and online activity. For example, if you visit a website about running and fitness, you might see ads for running shoes when you visit other websites.

What To Do About Online Tracking and Personalized Ads

- **Delete History** - If you don't want to see ads based on your previous online activity, delete cookies and clear your browsing and search history. On your phone, delete or reset identifiers used to track you.
- Adjust Privacy Settings - The privacy settings in your browser give you some control over the information websites collect about you.
  - For example, you can choose to block websites from seeing your browsing history. Or choose not to share your location with them.
  - The protections vary by browser. Some have a private browsing mode that deletes your browsing history after you end your session, but it doesn't block websites from seeing your online activity.
  - There also are browser extensions, or plug-ins, that give you some privacy controls. If you're considering one, read reviews from reputable sources to learn what options they offer.

Privacy Settings on SmartPhones

- Your browser's privacy settings also let you choose whether to allow or block personalized ads based on your browsing history. And your phone also has a setting that lets you opt out of personalized ads from the company that makes the operating system (for example, Apple or Google).
- You'll find this setting in the "advertising" section of your phone's privacy settings. In all these cases, you'll still see ads, but they won't be personalized based on your browsing history.

Privacy Settings on Apps and Social Media

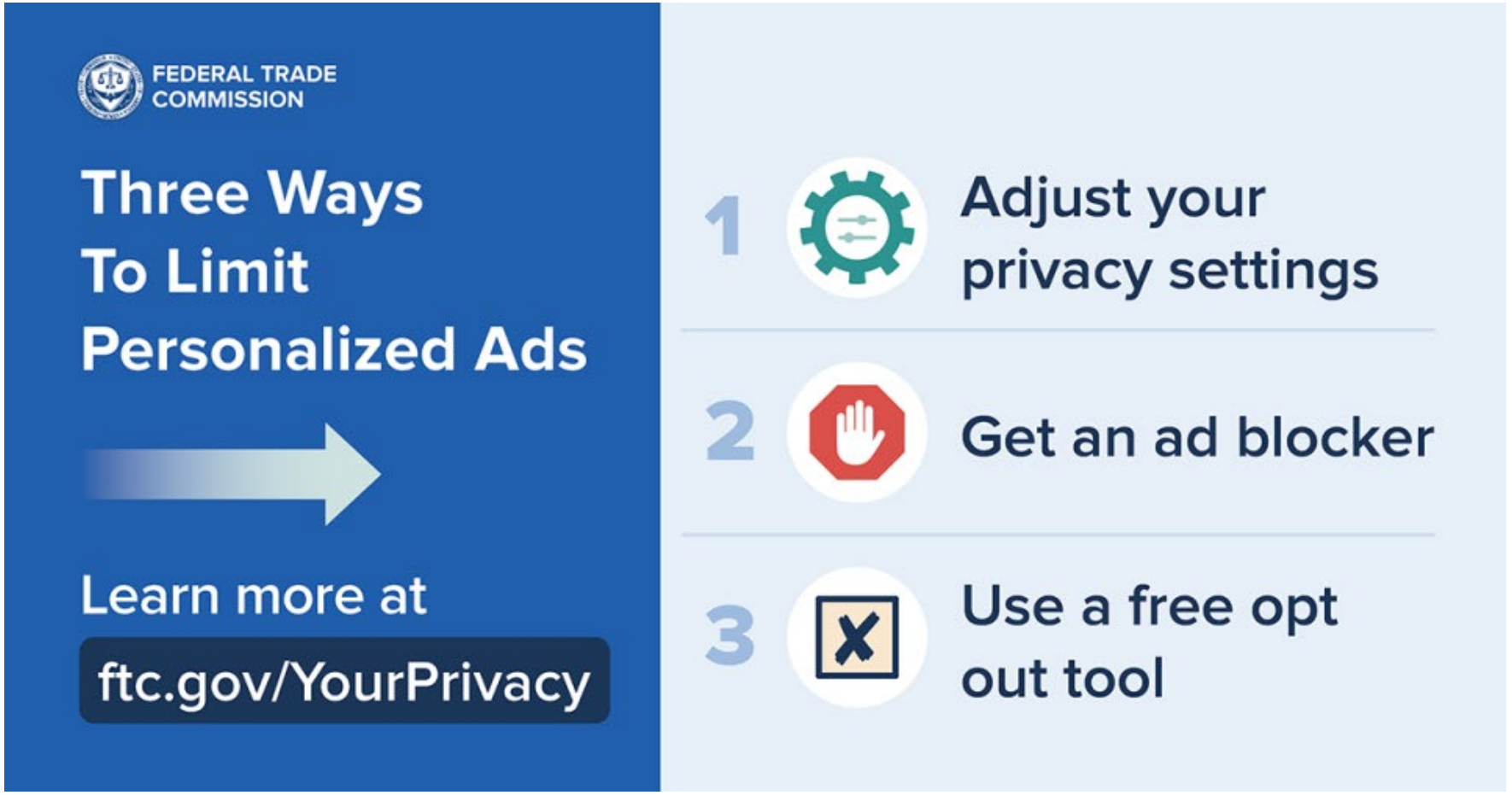
Social media, and other apps, may also track your online activity. Go to your account settings to see how they use your information and adjust your settings to match your preferences.

Some apps may ask for access to information from your device, like your location, your contacts, or your photos.

Go to the privacy settings on your smartphone to see what information they can access from your device.

Consider turning off unnecessary permissions or deleting apps that request a lot of permissions they don’t need to function.

Other Options



Enforcement Actions & Class Action Cases

Federal Trade Commission Privacy & Security Enforcement Actions

- The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce.

Recent FTC Cases

- General Motors LLC., et al., In the Matter of (January 14, 2026)
- NGL (January 6, 2026)
- Disney (December 31, 2025)
- Illusory Systems/Nomad (December 16, 2025)
- Support King, LLC (SpyFone.com), In the Matter of (December 8, 2025)
- Illuminate Education, Inc., In the Matter of (December 1, 2025)
- Apitor (October 1, 2025)
- Iconic Hearts Holdings, Inc., U.S. v. (September 29, 2025)
- Pornhub/Mindgeek/Aylo (September 3, 2025)
- Roca Labs, Inc. (July 9, 2025)
- GoDaddy Inc., et al., In the Matter of (May 21, 2025)

Attorney General Ken Paxton Finalizes Historic Settlement with Google

Attorney General Ken Paxton announced that Google has signed the historic $1.375 billion

settlement agreement with the State of Texas, marking the conclusion of two of the largest

data privacy enforcement actions ever brought by a single state against the tech giant.

Don’t Mess with Texas!

Attorney General Paxton previously sued Google for unlawfully tracking and collecting users’ private data regarding geolocation, incognito browsing activity, and biometric identifiers. The settlement obtained by Attorney General Paxton for these combined abuses far eclipses that of any other one state’s settlement against Google for similar claims, with the largest single-state settlement to date outside of Texas being $93 million. Additionally, a forty-state coalition secured $391 million in its privacy case against Google, which is almost one billion dollars less than what Attorney General Paxton secured for Texas alone. Attorney General Paxton thanks Norton Rose Fulbright, who served as outside counsel to the Office of Attorney General.

This settlement follows Attorney General Paxton’s $1.4 billion settlement with Meta (formerly Facebook) for illegal biometric data collection and his $700 million and $8 million settlements with Google for anticompetitive and deceptive trade practices.

Class Action Settlements

Google Incognito Mode: Google agreed to a $68 million settlement to delete billions of data records collected from users in Incognito mode, acknowledging the feature did not prevent data collection as implied.

Google Children's Privacy: A $8.25 million settlement was reached over allegations of collecting data from children via the Play Store.

Facebook User Privacy: Users in the U.S. active between May 2007 and December 2022 may be eligible for payments in a, now, $725 million settlement.

Inova Health Data Breach: A $3.1 million settlement exists for those whose data was shared with third parties via tracking pixels on their website.

Legislative Initiatives.

Data Protection Laws in United States

- See Appendix A.

Risk Mitigation

Ways to Mitigate Risk and Increase Compliance

- Update Policies and Procedures
- Update Public Facing Privacy Policies to meet various state and international standards
- Train workforce members
- Provide adequate disclosures to consumers and provide an option to opt out. Think cookies!
- Appreciate state, federal and international laws and penalties.

Conclusion

Parting Thoughts

Thank You and Questions

Rachel V. Rose – Attorney at Law, PLLC

Houston, Texas

(713) 907-7442 * www.rvrose.com

LAST MODIFIED 6 FEBRUARY 2025

Data protection laws in the United States

United States privacy law is a complex patchwork of national,

state and local privacy laws and regulations. There is no comprehensive national privacy law in the United States. However, the US does have a number of largely sector-specific privacy and data security laws at the federal level, as well as many more at the state (and local) level. In recent years, beginning with California in 2018, states have begun to introduce and enact their own comprehensive privacy laws. Although bipartisan draft bills (e.g., the American Privacy Rights Act of 2024) have been introduced since then , changes in the political climate, industry influence, and the increasing complexity of privacy concerns have stifled efforts of passing an omnibus law. Thus, a comprehensive privacy law on the federal level is not expected to pass any time soon.

Federal and State Privacy Laws and Regulations

Federal laws and regulations

include those that apply to financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, children's online privacy, telemarketing, email marketing, biometrics, and communications privacy laws.

There are also a number of state privacy and data security laws that can overlap with federal law(s)—some of these state privacy laws are preempted in part by federal laws, while others are not. Some US states have also privacy and data security laws and regulations

beyond requirements imposed by federal laws—such as data security laws, secure destruction, Social Security number privacy, online privacy, biometric information privacy, and data breach notification laws. Generally, these state laws apply to personal information about residents of or activities that occur within each of these states, respectively. Thus, many

businesses operating in the United States must comply not only with applicable federal law, but also with numerous state privacy and security laws and regulations.

For example, California alone has more than 25 state privacy and data security laws, including the comprehensive CCPA, which provides definitions and broad individual rights and imposes requirements and restrictions on the collection, use, disclosure, and processing of personal information of CA residents. The CCPA is unique among the existing state comprehensive privacy laws in that, it applies not only to personal information related to consumers but also in the HR and B2B context. Enforcement of the updated CCPA regulations, which were finalized March 29, 2023, commenced on March 29, 2024, by the newly established California Privacy Protection Agency, referred to as the 'CPPA' or 'Agency.' On November 8, 2024, the Agency

Board voted to commence supplementary CCPA rulemaking on certain additional regulatory subjects: CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies. Specifically, the proposed regulations seek to (1) update existing CCPA regulations; (2) implement requirements for certain businesses to conduct privacy risk assessments and complete annual cybersecurity audits; (3) implement the right to access and opt-out of being subject to ADMT; and (4) clarify when insurance companies must comply with the CCPA. The public comment period for these proposed regulations closes on February 19, 2025.

The CPPA also enforces the "Delete Act," effective January 1, 2024, which imposes deletion obligations on data brokers, thereby allowing consumers to more easily delete their personal information held by data

brokers in California. Under the Delete Act, the CPPA must establish an accessible deletion mechanism by January 1, 2026. This mechanism is intended to allow consumers to make a single verifiable deletion request to have their data deleted by data brokers and their associated service providers or contractors.

In August 2022, the California legislature passed the California Age-Appropriate Design Code (CAADC), which was slated to take effect July 1, 2024, and would apply to companies that meet the definition of "business" under the CCPA and that provide online services that are likely to be accessed by individuals under 18 years of age. However, on September 18, 2023, a California District Court issued an injunction blocking the law from coming into effect on First Amendment grounds. Following an appeal to the Ninth Circuit by the California Attorney General's office, the fate of the law is currently uncertain. More

information on the California Age-Appropriate Design Code is available online.

Similarly, Maryland has enacted the “Kids Code” and Connecticut amended its Consumer Data Protection Act to include similar protections for children’s personal information. Moreover, in January 2025, the Federal Trade Commission (FTC) finalized significant changes to the federal Children’s Online Privacy Protection Act (COPPA). While the FTC periodically reviews the COPPA rule, these rule changes are the first amendment to COPPA since 2013. According to the FTC, the final amended rule reflects technological advancements since COPPA was last amended and is intended to enhance online safety for children. More information on the amended rule is available online. The combined efforts of federal and state regulators are intended to pave the way for a safer digital landscape and ensure that children's privacy is prioritized

in an increasingly connected world.

Beyond California's CCPA, additional comprehensive state privacy laws have also taken effect, including the

- Colorado Privacy Act,
- Connecticut Data Privacy Act (including amendments regulating consumer health data, children's data, and social media platforms),
- Delaware Personal Data Privacy Act,
- Florida Data Privacy and Security Act,
- Iowa Consumer Data Protection Act,
- Montana Consumer Data Privacy Act,
- Nebraska Data Privacy Act,
- New Hampshire Consumer Expectation of Privacy Act,

- New Jersey Personal Data Privacy Act,
- Oregon Consumer Privacy Act,
- Texas Data Privacy and Security Act,
- Utah Consumer Privacy Act, and
- Virginia Consumer Data Protection Act.

While not identical, the these comprehensive state privacy laws are, with the exception of the CCPA, substantially similar to each other in most respects, but may differ in certain regards, for example, scope, privacy notice disclosures, privacy rights, and certain key definitions. These state laws are also generally inapplicable to personal information collected about, and processed in the context of, employee and business relationships. While the CCPA has some practical similarities with these state laws, it adopts

more granular definitions, requirements, and restrictions that vary considerably from these laws, and, notably, also applies to personal information collected from California residents in employment and B2B contexts.

There have also been significant developments in the health data space, beginning in 2023 with Washington passing the landmark My Health My Data Act (MHMD). The law ostensibly applies only to consumer health data, but its exceptionally broad definitions and scope combined with its private right of action may mean its enforcement touches on data many companies may not typically consider “health” data. More information on the MHMD Act is available online. Since MHMD, other states have followed suit—Nevada passed the Nevada Consumer Health Data Privacy Law through senate bill 370, effective March 31, 2024, and Connecticut amended the Consumer Data Privacy Act to

include similar provisions for protecting consumer health data, effective October 1, 2023.

Finally, the pace of state privacy legislation has continued to accelerate overall, with the following states also passing their own comprehensive privacy laws or variations thereof, and even more states introducing similar legislation:

- Tennessee (effective July 1, 2025)
- Minnesota (effective July 21, 2025)
- Maryland (effective November 1, 2025)
- Indiana (effective January 1, 2026)
- Kentucky (effective January 1, 2026)
- Rhode Island (effective January 1, 2026)

Enforcement of

Unfair and Deceptive Trade Practices

In the United States, consumer protection laws, which prohibit unfair and deceptive business practices, provide another avenue for enforcement against businesses for their privacy and security practices.

At the federal level, the US Federal Trade Commission (FTC) uses its authority to protect consumers against unfair or deceptive trade practices, to take enforcement actions against businesses for materially unfair privacy and data security practices. The FTC uses this authority to, among other things, take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate or misleading privacy and security statements, including in privacy policies

- Failing to abide by applicable industry self-regulatory principles

- Transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or M&A transaction, in a manner not expressly disclosed on the applicable consumer privacy policy

- Violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of standards established in their prior enforcement precedents

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. State attorneys general also

sometimes work together on enforcement actions against companies for actions that broadly affect the consumers of multiple states (such as data breaches).

Key Areas of Privacy Class Action

Privacy class actions continue to be a significant risk area in the United States, including in the context of biometric privacy (under the Illinois Biometric Privacy Act), text messaging (under the federal Telephone Consumer Privacy Act) and call recording, wiretapping and related claims under the California Invasion of Privacy Act, the Video Privacy Protection Act (VPPA) and other state laws. Online monitoring and targeting activities—including via cookies, pixels, chat bots, and so-called "session replay" tools—are an area of particular focus in the eyes of both regulators and plaintiff's attorneys. Under the CCPA, data breaches due to inadequate security measures,

allow for a private right of action. The highlight the evolving landscape of privacy litigation, emphasizing the need for businesses to comply with stringent data protection regulations to avoid legal repercussions.

Continue reading

Change

Next topic →

About us
Insights
Careers
Locations
News
Events
Law&
Alumni

office
Subscribe
Contact us

Legal notices
Privacy policy
Cookie policy
Modern slavery

Data Loss Prevention (DLP) , Data Security

Study: Future IT Workers Would Sell Patient Data

Nearly 60% of Tech Students Said They'd Violate HIPAA If the Price Was Right

Marianne Kolbasuk McGee (HealthInfoSec) • January 26, 2026

A University of Buffalo research study found that a concerning percentage of future IT workers would disclose patient records in violation of HIPAA if the price was right. (Image: Getty Images)

Budding IT insiders can be corrupted into giving up protected health information, say university researchers who also found a correlation between an interest in white hat hacking and a propensity for conducting illegal breaches.

See Also: AI Tool Data Exposure Risks Drive Need for Stronger Controls

A survey of 523 information systems management and data analytics students by the State University of New York at Buffalo found that nearly 60% of respondents said they would leak information about a very famous patient in exchange for amounts ranging from less than $10,000 to more than $10 million, depending on the perceived probability of getting caught and the salary level of the employee.

Students were told to imagine themselves having post-college financial difficulty and a friend who works at a media company. Roughly six out of every 10 students said they would give up the data of the famous patient. The amount required varied on the scenario, with students told to imagine a greater salary needing a bigger payoff.

Students with a self-professed interest in white hat hacking had a statistically significant need for less money to cough up the famous patient's data, researchers said.

The research also found correlations between interest in white hat hacking and willingness to engage in black hat or gray hat activities, so long as students received assurances that they wouldn't be caught.

Researchers didn't assess whether students possessed the skills necessary to illegally hack, telling them to assume that they do. They defined a black hat as someone willing to digitally steal money and a gray hat as someone who might hack a company that supports a political candidate the student doesn't like or hacking the social media account of an extremist.

"Insider cybersecurity threats are driven as much by economic and behavioral factors as by technology," said Lawrence Sanders, a professor emeritus at the University of Buffalo's department of management science and systems, and one of the researchers involved in the study.

The research builds upon a 2020 study involving 523 students with an average age of 21 who were about to enter the workforce. That earlier survey found 46% of respondents would accept a certain amount of money in exchange for violating HIPAA, also depending upon the circumstances.

In that study, 79% of respondents said they would hand over a politician’s medical records to a media outlet in exchange for $100,000 in order to pay for an experimental medical treatment for their mother that was not being covered by insurance.

Some experts called the research findings unsettling.

"On a macro level, it shows two disturbing items: a lack of respect for another person's sensitive information; and a moral compass that is off-track," said regulatory attorney Rachel Rose.

"From a bioethics perspective, patient autonomy and the related right to privacy are very valued and a cornerstone of trust in the medical system," she said.

Sanders advised medical practices to conduct background screenings. "Controls and monitoring can also help," he said.

Background checks on prospective workers only go so far, Rose said. Healthcare entities must take measures - including technical, administrative and physical to help prevent the likelihood of these types of insider incidents, Rose said.

Workforce training that illustrates potential consequences of malicious behavior is critical, she said. "Emphasize criminal penalties and provide actual examples as part of training and throughout the year as part of continuing security and privacy awareness," she suggested.

Sanders encouraged employers "to work closely with employees and support them when they have financial difficulties or are under stress for whatever reason," to help mitigate potential insider breaches.

About the Author

Marianne Kolbasuk McGee

Executive Editor, HealthcareInfoSecurity, ISMG

McGee is executive editor of Information Security Media Group's HealthcareInfoSecurity.com media site. She has about 30 years of IT journalism experience, with a focus on healthcare information technology issues for more than 15 years. Before joining ISMG in 2012, she was a reporter at InformationWeek magazine and news site and played a lead role in the launch of InformationWeek's healthcare IT media site.