

# Unfair and Deceptive Cookie Banners: The Next Wave of Privacy Litigation?

Article By:

Erin Jane Illman

---

Today, encountering a cookie banner is a common experience for most individuals who peruse the internet. These banners inform website users of the presence of cookies or other tracking technologies through language such as, “This website uses cookies. By clicking ‘accept,’ you consent to the use of all cookies.” Many states require companies to provide consumers with certain disclosures regarding tracking technologies, and some require that users are provided an opportunity to opt-out of tracking. However, even in states without specific disclosure or opt-out requirements, businesses may still be at risk. In July 2024, the Office of the New York State Attorney General (OAG) published guidance that provides some clear examples of what is acceptable and what is considered misleading in the flow, language, and design of cookie banners.

## New York’s OAG Investigation

New York does not yet have a comprehensive set of privacy regulations, so there is no requirement that websites give users the opportunity to opt-out of tracking. However, the NY OAG guidance states that if a business makes inaccurate or misleading representations about tracking on their website, they are at risk of violating New York’s consumer protection laws. Thus, if a website displays a cookie banner that is faulty, that business can be prosecuted under New York law despite the lack of a specific privacy regulation. Even more concerning is that New York’s Unfair, Deceptive, or Abusive Acts or Practices (UDAP) provides for a private right of action with an attorney’s fees provision, increasing the likelihood and incentive for future litigation (N.Y. Gen. Bus. Law § 349(h)).

The New York OAG analyzed several popular websites and found that many continued to track users after they had opted out of tracking. The investigation identified several causes of this defect. For example, many websites separate tags or cookies based on categories (such as marketing or fraud detection). Websites often give users the option to disable tracking for certain categories. However, if tags are miscategorized or uncategorized, tracking can remain active after a user attempted to disable a specific category.

Additionally, the investigation found that some websites may be mistakenly relying on “limited data use” features offered by third-party cookie providers. While certain companies provide businesses with the option to have more control over data use, many such features are only available in states with comprehensive privacy laws. In states without such regulations, providers may continue to

collect and use consumer data.

Further examples of potential pitfalls identified by the OAG investigation include misconfigured cookie consent tools that fail to adhere to consumers' chosen privacy settings; tags and cookies that are not configured to a website's specific privacy controls; and websites only applying privacy choices to third-party cookies while continuing to use other tracking technologies.

The New York OAG guidance provides very clear examples of what is not allowed in cookie banners, such as hidden "save" features, accept only options, or confusing accept buttons. The guidance also provides some recommendations for businesses to prevent potential legal violations. These recommended processes include designating a specific individual to manage tracking technology, investigating new technology before it is used, and conducting appropriate testing and review of tracking tools.

## Key Takeaway

Companies should regularly audit and assess their use of tracking technologies and the disclosure and opt-out functionality in their cookie banners, and they should refer to the "dos and don'ts" published by the New York OAG, in conjunction with the regulatory, legislative, and litigation developments in this area.

*\*Tamara Boles is a co-author of this post and a J.D. graduate from the University of Alabama School of Law. She is not yet licensed to practice law.*

© 2025 Bradley Arant Boult Cummings LLP

---

National Law Review, Volume XIV, Number 267

Source URL: <https://natlawreview.com/article/unfair-and-deceptive-cookie-banners-next-wave-privacy-litigation>