Digital Advertising Privacy Law

Travianna Tighe

Department of Communication, University of Nebraska Kearney

JMC-414: Communication Law

Dr. Ralph Hanson

May 9, 2025

When a user clicks “accept terms and conditions” on the newest social media platform or “accept cookies” to continue scrolling on a website they want to view, they are potentially exposing sensitive personal information to be auctioned off to third-party advertisers, and this often without their complete understanding. The current digital advertising landscape was not always the threat it is to digital users today. With the advancement of digital media being integrated into our daily lives and the high return investment companies see on targeted advertisements, it has quickly become a normalized invasion of privacy that has recently concerned American people and policymakers alike. This has led to the first state laws to protect citizens’ private information, which have been used as a means of defense seen in cases such as *Sweeney v. Life on Air, Michie v. The Trade Desk and Penning v. Microsoft Corp.* The legal landscape surrounding digital advertising privacy is rapidly evolving. Landmark legislation and major lawsuits are beginning to challenge how tech companies collect and use consumer data. As this public concern grows, federal regulation and stricter enforcement will reshape advertising practices and start an era of continued legal transformation around the topic.

Digital Advertising didn’t always look like it does today. In the article “Data Privacy in Digital Advertising Towards a Post-Third-Party Cookie Era,” authors Çınar and Ateş explain how it did not start as the effective industry we see today. They state, “online advertising practices have evolved from the rudimentary and ineffective pop-up and banner ads, to involuntary and invasive adware installations to more recent data-driven techniques such as collaborative filtering, contextual and personalized advertising, and behavioral targeting” (Çınar & Ateş, 2022).

What started as simple banner ads in the 1990s quickly became more targeted and specific with the introduction of cookies. Çınar and Ateş elaborate that cookies were created in

1994 to make web browsing more convenient. The idea was to help users stay logged into their banking website or saving preferences (Çınar, N., & Ateş, S., 2022). The intent behind this online tool was to help internet users, but as their popularity grew, the purpose of the creation changed. According to author of the article, "Times They are Changin" Can the Ad Tech Industry Survive in Privacy Conscious World?" author Meghan Donahue describes how companies quickly realized they could use cookies to track users across multiple websites, which transformed them into powerful tools for targeted advertising and a significant source of privacy concerns (Donahue, 2021).

Worries began to be raised early on, especially regarding minors' information being collected on websites that were marketed to them, and parents grew concerned about their children's internet use. In response, Congress passed the Children's Online Privacy Protection Act (COPPA) in 1998 to regulate data collection from kids under 13. (Children's Online Privacy Protection Rule, 1998). The Federal Trade Commission enforces this act, and it was one of the first pieces of legislation to protect people's data from being collected and sold to advertisers online. Since then, a few federal privacy laws have been passed that regulate data collection and use to protect citizens further, but do not specifically address digital advertising practices like ad targeting and cookie tracking. As a result, a few state legislators are beginning to step up to safeguard their citizens and ensure their data cannot be unlawfully shared by these methods. One of the most impactful state acts that has been used to bring about many cases since its passing in 2020 is the California Consumer Privacy Act. The authors of the article, "Data Protection and Privacy Law in the Context of Digital Advertising and Tracking," Clara Hoffmann and Tobias Meier, present the CCPA as a state law that gave California citizens control over their data by allowing them to know what data they are collected about them, requiring the option to opt out of

sharing their information and to delete all of the information that has been collected about them (Hoffmann & Meier, 2024). More states, such as Virginia and Colorado, have followed in California's legislative footsteps, creating their own acts to protect their citizens' privacy rights against these big platforms. There has been a push for a federal law similar to the CCPA to allow protections for all states, In 2022, the American Data Privacy and Protection Act (ADPPA) made it furthest than any previous federal privacy bill, however it was unable to reach a full vote in the House of Representatives due to concerns from California lawmakers about it overriding sections of the CCPA (Bailey, 2024). Since the ADPPA failed, the new American Privacy Rights Act (APRA) aims to create a national privacy standard and address issues like AI and youth protections. As concerns grow, the future of digital advertising will keep being debated, especially with different state laws creating confusion.

Big tech companies know digital advertising privacy laws and attempt to align their policies to ensure trust and clear communication with users. For example, in Google's "Advertising Policies Help" section, they state that advertisers must follow all laws regarding digital advertising on their platforms, including "may not run personalized ads, make use of any third party trackers, or otherwise attempt to collect personal information from minors or on content set as made for kids" (Ads & Made for Kids Content, n.d.). However, this is not constantly monitored well or correctly applied. New York Post business reporter Thomas Barrabi gives a specific example from this past year in his article titled, "Google, Meta Hatched Secret Deal to Target Teens on YouTube with Instagram Ads: Report." He explains how Instagram ran a YouTube advertisement targeting children and underage users to download their app by placing it in a category that targeted "unknown users," fully aware that most of this section includes children (Barrabi, 2024). Not only does this violate Google's policy, but it is also a direct attempt

to advertise to minors and violates COPPA. Barrabi further acknowledges that both Google and Instagram employees knew that the campaign was breaking the law and unethical, but continued to run it and keep it under wraps until some internal leaks were made by employees who exposed both companies for their harmful intentions (Barrabi, 2024). This led to outrage online, and many advocates for children's privacy online are asking for legislation to secure further protection for underage individuals online, with the Kids Online Safety Act. Also referred to as the "COPPA 2.0," this Act would require opt-in consent for collecting data from teens aged 13 to 16 and further ban targeted ads (Bonner, 2024). So, while legal restrictions are supposed to protect children from digital advertising targeting and tracking, this example explains how there can be a gap between company policies and actual enforcement. This is why many support stronger legislation like COPPA 2.0 and believe it is needed to hold companies accountable and protect minors' online information better.

Privacy in digital advertising is an essential topic to be addressed in a legal context in the current digital landscape because it dramatically affects every internet user and has the power to harm public trust in technology. As stated earlier, when accepting cookies or agreeing to the terms and conditions, people do not understand the detailed information they give away about themselves. Çınar and Ateş further elaborate, sharing that the AdTech industry is collecting and storing data that is not just basic information, but also health records, location history, search history and even predictions about users' future actions (Çınar & Ateş, 2022). While this may be stated somewhere in some terms and conditions that a user agreed to, most of the population does not realize the extent to which detailed information about them is being used to feed them products and take advantage of their privacy. Although most Americans are unaware of what is being collected about them, most are still worried about what is happening to their information.

According to the Pew Research Center's article titled "How Americans View Data Privacy," states that 81% of Americans are concerned about what companies are doing with their data and 73% believe that they have no control about what happens with the information they are collecting (McClain, Faverio, Anderson, & Park, 2023). As more lawsuits and news articles describe the unethical and legal concerns regarding people's data being sold online to make them more likely to buy a specific product, the way people use platforms and technology is expected to change. In the article titled "Digital Advertising: Present and Future Prospects," the authors argue that trust within these companies will change, and all of the valuable aspects that exist on the internet and social media like communication with those from around the world, entertainment, learning opportunities, will be lost for users who are concerned about their information being sold and misused (Lee & Cho, 2020). While this is a legal issue for U.S. citizens, it is also a significant ethical issue concerning the many people it influences, and the industry is rapidly growing in power.

Legal cases have emerged regarding digital advertising and privacy being shared across platforms using the CCPA as a defense as early as the same year the act began. In April 2020, plaintiff Heather Sweeney sued a popular video chatting app during the COVID-19 pandemic called Houseparty, alleging that it had multiple CCPA violations, starting the case *Sweeney v. Life On Air, et al.* Sweeney claimed that the Houseparty app was sharing personally identifiable information (PII) with Facebook and other third-party apps to be shown targeted advertisements without allowing her to withdraw (Swigart, 2020). While some users may not worry about their information being shared, it is serious, and legal ramifications have been put in place to prohibit this. According to the article, "CCPA Case Tracker," information being shared across platforms included personal identifiers, such as location, device information, time zone, phone carrier and a

unique advertiser identifier (CCPA Case Tracker, n.d.). The unique advertiser identifier is the most concerning among the data shared. A unique advertiser identifier, also known as an IDFA, is a one-of-a-kind code matched to each device, which allows advertisers to track and profile individual users without needing their name, address, or email (Swigart, 2020). This type of information holds a significant monetary value as the more an advertiser knows about a consumer, the more likely they can target their specific needs and interests, which increases the likelihood of buying the product advertised to them. The article CCPA Case Tracker states that Sweeney argued Houseparty was violating four parts of the CCPA, including:

- "Failure to provide adequate notice of collection, use, or sale of PII."
- "Sharing information with a third party without notifying or giving individuals a right to opt out."
- "Failure to provide a clear and conspicuous 'Do Not Sell My Personal Information' link on their webpage."
- "Failure to keep PII private." (CCPA Case Tracker, n.d.).

As a result, Sweeney only asked for the court to stop Houseparty from continuing these practices that invade user privacy without their full knowledge and to award money to the individuals they have caused harm to (CCPA Case Tracker, n.d.). Overall, this was one of the first landmark cases that involved the CCPA and began a discussion about what is being shared with third-party apps and how this information is breaking state laws, and kickstarted other states to begin to create similar laws of their own to protect citizens' advertising profiles being used without legal ramifications.

A more recent case with similar circumstances would be the *Michie v. The Trade Desk.* The AdWeek article by Kendra Barnett titled "Two Lawsuits Allege The Trade Desk Secretly

Violates Consumer Privacy Laws" explains the case filed on March 28, 2025, in the Northern District of California. This lawsuit accused Trade Desk, a $25 billion digital advertising platform that helps brands buy targeted ads across the internet, of breaking laws by monitoring millions of consumers through a program called Adsrvr (Barnett, 2025). Plaintiffs in this case believe that this breaks several aspects of the CCPA, as it profiles and tracks users without their knowledge for consent across devices and various parts of the internet. Trade Desk's use of the Adsrvr program is accused of violating the CCPA, as it involves cross-device tracking, allowing the company to create detailed consumer profiles based on behavior across all sorts of devices. The plaintiffs have raised this significant privacy concern, as consumers are often unaware that they are being monitored in this way. They accused the Trade Desk of collecting personal data, device IDs and even health information, which were sold to third parties during real-time ad bidding (Barnett, 2025). The lawsuit alleges that the detailed profiling of customers caused bid values to be inflated. They see a larger profit on users during auctions that have more personal information tracked about them (Barnett, 2025). This means that The Trade Desk not only helps advertisers place ads, but also controls what the companies learn about a user, which it can use to increase the cost of ad space to target specific individuals with a higher likelihood of buying their product. Barnett elaborates that this lawsuit is not just an aim to settle or win damages by the plaintiff, but is a part of a larger effort to develop stronger privacy laws that will apply across platforms (Barnett, 2025). *Michie v. The Trade Desk* represents not just a legal battle over a specific company's unlawful and unethical practices, but also a shift in how consumers value their data and highlights the growing call for platforms to be transparent about what they are doing with digital advertising privacy.

Another recent filing regarding digital advertising privacy law includes *Penning v. Microsoft Corp.* In the article by Michael Adams titled "Ad Tracking Lawsuits Allege Illegal Surveillance of Internet Users by Microsoft, Others," he writes about how Microsoft uses advertising pixels to break American laws about collecting data. (Adams, 2025). Pixels are pieces of code that track what people do on websites and the data they enter on them, and send it back to companies. Plaintiff Stacy Penning from Washington filed a lawsuit against Microsoft's tracking tool in March 2025, known as Adnxs Pixel, stating that it recorded his information on a Buzzfeed webpage and then proceeded to share it with multiple other websites through Microsoft's advertising platform called Xandr (Adams, 2025). This is being done without the user's consent, with no opt-in option, so they had a legitimate claim to sue, stating that Microsoft was breaking the policies in the CCPA and some other federal laws. While Penning is the plaintiff of this case, there are also five other plaintiffs suing Microsoft claiming like Penning that "a wide range of user data, including demographics, geolocation and sensitive personal details, such as health information, political views and sexual orientation, even if that information was entered on unrelated websites" of being tracked and sold to real-time bidding advertisers through Microsoft's platforms (Adams, 2025). These plaintiffs argue that the data collected and input into a system goes beyond the basic tracking and ask Americans to get the justice they deserve. Many people's privacy is being taken advantage of by these platforms. Penning wrote in his complaint that Microsoft permanently stores personal data and online activity, which is affecting millions of Americans. Microsoft is using it to run its advertising tools, generating billions in revenue through simultaneous ad sales (Adams, 2025). The plaintiffs seek damages and class action certification, including a special California resident subclass to hold Microsoft accountable for unlawful data practices (Adams, 2025). They believe this will be

the first step to keep these major web corporations for the privacy rights they have taken away from millions of Americans and to start a larger conversation that needs to be addressed in the advertising world.

With many lawsuits beginning to arise regarding American citizens' private information being sold to digital advertisers, it will begin to start an uproar of public opinion, and clear laws will need to be set to treat every case and reward those who have been taken advantage of fairly. To do this, there will need to be a single significant federal law applying to all states that clearly outlines the practices companies are and are not allowed to partake in when it comes to selling the users' data on their platforms to advertisers. All platforms should require opt-in for information to be collected, as active consent should occur before tracking starts. With this, big tech companies must be upfront and specific about what data they are asking to collect from users, and the same goes for who they plan to share information with. Additionally, it should allow users to remove their consent at any time, guaranteeing that it will be deleted and no longer used to tailor ads for them. This will be needed to allow all the states to have the same standards regarding digital advertising privacy laws, and platforms can't use the excuse of trying to comply with a multitude of state laws, as more and more states begin to create their own laws in California's footsteps. The proposed American Privacy Rights Act (APRA) will come up for a vote again, and its rulings will likely follow the European Union's General Data Protection Regulation. Also known as the GDPR, the EU enacted this in 2018 to set strict rules for collecting and processing personal data, requiring clear consent, transparency and user rights like access, correction and deletion all backed by heavy fines for if companies do not follow the law (Hoffmann & Meier, 2024). The United States is now seven years behind Europe on this issue, and it must be addressed at the federal level to ensure protections for all citizens.

With these proposed changes that need to be implemented, there are many future predictions and challenges regarding the topic. Companies are beginning to reform their policies to stay on top of new legislation being passed in states. Boerman and Smit further detail how Apple has recently changed its policy to require user consent before it tracks any information. Google is working toward banning third-party cookies and cross-site tracking altogether. (Boerman & Smit, 2023). Changes like these are necessary for brands to show their users that they are taking steps to prioritize privacy on their platforms. Digital advertisers will begin to run into issues because although it causes distrust for users to know their information is being sold to give them more personalized advertisements, they still value customized promotions (Gold & Fischer, 2021). Tensions will grow between those valuing personalization and privacy, and it will be integral that advertisers find a way to balance this line to keep their industry in business.

Digital advertising practices using cookies and data trackers began with the right intentions, but quickly evolved into an intrusive landscape. As a response, many federal acts, such as the COPPA and CPPA, aim to protect citizens' information from being unlawfully used, and public awareness of the issue has increased. With many major lawsuits emerging using these acts as a means of defence, their outcome will not only allow justice to be served, but will also have the power to influence the future of digital media. The results of these cases will have future implications for tech platforms and citizens alike. With this increased knowledge of the practices occurring, the United States government has a duty to protect citizens' privacy, and digital advertisers will have to find a way to change their practices to satisfy not only the needs of their consumers but also their wants and expectations.

References

Adams, M. (2025). Ad Tracking Lawsuits Allege Illegal Surveillance of Internet Users by Microsoft, Others. *AboutLawsuits.* https://www.aboutlawsuits.com/ad-tracking-lawsuits-illegal-surveillance-internet-users-microsoft- others/

Ads & Made for Kids Content. (n.d.) *Google.* https://support.google.com/adspolicy/answer/9683742?hl=en

Bailey, J. (2024). American Privacy Rights Act of 2024: A Renewed Push for a Comprehensive National Privacy Framework. *The American Enterprise Institute.* https://www.aei.org/technology-and-innovation/american-privacy-rights-act-of-2024-a-renewed-push-for-a-comprehensive-national-privacy-framework/

Barnett, K. (2025). Two Lawsuits Allege The Trade Desk Secretly Violates Consumer Privacy Laws. *Adweek.* https://www.adweek.com/programmatic/lawsuits-trade-desk-consumer-privacy-laws/

Barrabi, T. (2024). Google, Meta hatched secret deal to target teens on YouTube with Instagram Ads: Report. *New York Post.* https://nypost.com/2024/08/08/business/google-meta-reportedly-hatched-secret-deal-to-target-teens-on-youtube-with-instagram-ads/

Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: An overview of Past Research and a Research Agenda. *International Journal of Advertising*, *42*(1), 60-68. https://www.tandfonline.com/doi/pdf/10.1080/02650487.2022.2122251

Bonner, R. (2025) COPPA 2.0 Reintroduced – What You Need to Know. *BBB National Programs.* https://bbbprograms.org/media/insights/blog/coppa-2-0

CCPA Case Tracker. (n.d.). *O'Melveny & Myers LLP.* https://www.omm.com/insights/alerts-publications/ccpa-case-tracker/

Children's Online Privacy Protection Rule (COPPA). (1998). *Federal Trade Commission.* https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Çınar, N., & Ateş, S. (2022). Data privacy in digital advertising: Towards a Post-Third-Party Cookie Era. In Privacy (pp. 55-77). *Routledge.* https://www.researchgate.net/profile/NaimCinar/publication/358943407_Data_Privacy_in_Digital_Advertising_Towards_a_Post_Third-Party_Cookie_Era/links/642eac5f20f25554da137def/Data-Privacy-in-Digital-Advertising-Towards-a-Post-Third-Party-Cookie-Era.pdf

Donahue, M. (2021). "Times They are Changin" Can the ad tech industry survive in Privacy Conscious world?" *Catholic University Journal of Law and Technology, 30(1),* 193-[iii]. https://scholarship.law.edu/cgi/viewcontent.cgi?article=1116&context=jlt

Gold, A., & Fischer, S. (2021). Privacy Laws push online ads beyond tracking. *Axios* https://www.axios.com/2021/03/03/privacy-laws-push-online-ads-beyond-tracking?utm_source=.com

Hoffmann, C., & Meier, T. (2024). Data Protection and Privacy Law in the Context of Digital Advertising and Tracking. *Legal Studies in Digital Age*, *3*(3), 15-22. https://www.jlsda.com/index.php/lsda/article/view/34 (link no longer active)

Lee, H., & Cho, C. H. (2020). Digital Advertising: Present and Future Prospects. *International Journal of Advertising*, *39*(3), https://www.tandfonline.com/doi/pdf/10.1080/02650487.2019.1642015

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023). How Americans View Data Privacy. *Pew Research Center*. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Swigart, J. (2020) Sweeney v. Life on Air Inc et al. *Class Action*. https://www.classaction.org/media/sweeney-v-life-on-air-inc-et-al.pdf