The Future of Online Privacy and Advertising Targeting Methods

Evelyn Mukherjee

INFO601-03

Professor Bowler

14 December 2022

The current landscape of digital advertising is about to change upon Google's announcement to remove cookies from their popular browser, Google Chrome. As leaders in the advertising industry, Google's third-party cookie removal has put many advertisers and companies into a frenzy of finding new cookieless advertising methods. This choice was inspired, or rather pushed, by a majority of consumers' increased frustration, mistrust, and confusion with data collection and usage on the company's end. Consumers interact with cookies on an almost daily basis, but are not aware of what comes with clicking the "Accept Cookies" button. Companies are collecting and selling user data, many times unbeknownst to the user, and give little to no information to consumers on what they are doing with the collected data. While third-party cookies are integral to many advertising companies in order to provide insight into their consumer's online behavior and provide tailored advertisements to users that could lead to increased conversion rates for the company, it comes at the cost of leaving consumers in the dark with where their data is going and how it is being used. Concerns from consumers are starting to rise, and trust in large companies is decreasing. It is crucial that Google uses its influence as a large company to empower the consumer and their privacy in their pursuit for creating new advertising methods, as it is owed to the consumer to be more aware of their online presence and how third-party cookies are affecting them. The practice of data collection is a highly debated topic surrounding user privacy and data protection, and it's important to first look into the large ambiguity that comes with privacy policies and data collection transparency on the user's end.

The first step to data collection is through the user's browser with the help of cookies. Data is typically collected online using small text files called "cookies". Cookies can collect information and activity on pages you have visited, save your usernames and passwords, save items in your cart, deliver targeted ads, and customize your overall web experience by saving preferences on websites even when you close out of them (Pantelic et al. 2-3). There are three main categories of cookies many users interact with on a regular basis: persistent cookies, session cookies, and third-party cookies (ftc.gov). Persistent cookies can save data for extended periods of time, such as login information and passwords for specific websites. Your browser will typically ask you to store this information, rather than do it automatically. Session cookies are immediate cookies that only work for the amount of time you are on a web browser. These cookies are normally used for saving shopping cart items. Third party cookies are cookies that collect your user data to be sent to different websites to help enhance and personalize the online advertisements that you see. The data they collect can range from how long you're on the web page to the different sites you visit in that browsing period. Third party cookies are the most controversial, as they collect your data and send it to various different locations, many times unbeknownst to the user. Despite being the most controversial, advertising companies rely heavily on the user data provided by third-party cookies in order to target advertisements properly.

Ironically, the purpose of cookies created in 1991 by Lou Montulli was to protect the user's privacy while saving their progress on different websites. Cookies were designed to create a personalized web experience between the user and their server, with no intention of the stored data being shared (Johnson, S.). It wasn't until advertisers realized they could look at the back end of websites and their HTML to view cookies and the data stored in them. One of the first companies that realized they could see data stored in a cookie was an advertising company called Double Click, which was later bought by Google in 2008 (Mills). Advertisers originally only tracked cookies to make sure they weren't double-counting a single user, but the use of cookies slowly evolved into gathering data on users to optimize ad targeting and placement. Despite the function of cookies changing from their initial creation, internet users have always had concerns about their privacy due to cookies. In a podcast episode of Hidden Heroes by Steven Johnson, Montulli stated, "Cookies by themselves are not a bad actor—but cookies plus images served from third parties all work together to allow ad trackers." (Johnson, S.) A singular cookie does not have the ability to expose anyone's identity or personal information. Our worries should be over those in control of our data, rather than the thing collecting it. As cookies and advertising have evolved, we have reached a period of intense concern and confusion over what really happens with the data collected on the many websites we visit on a regular basis.

As consumers are becoming more concerned and confused with where their data is going (Auxier et al.), there have been many federal and state acts that have been created in an attempt to combat this problem. Currently, California is the only state with a privacy protection act that closely resembles the General Data Protection Regulation in the EU. The California Consumer Protection Act gives residents the rights to know what data is being collected, whether it is being sold and if so to whom, access to their personal data, the right to say no to their data being collected, and the right to equal services and prices regardless of whether they exercise their privacy rights or not (Moschovitis, "North American Regulations"). Following suit, Utah, Colorado, Virginia, and Connecticut are currently the only other states with legislature (Desai, iapp.org). On the federal level, the American Data Privacy and Protection Act is the most recent privacy protection act introduced on July 20, 2022 (congress.gov). If signed, this act will give consumers more autonomy over their data, including the rights to view, edit, and opt out of targeted advertising on the websites they visit. Websites will be required to give a notice to consumers about their cookie policies, as well as give them the option to change their cookie settings or opt out of data collection on the website altogether. There are high hopes for this bill, as it could provide guidelines for further regulation and act as a huge incentive for companies to start being more transparent. With little regulation, companies are not required to be transparent, leaving it up to their confusing privacy policies to inform consumers.

Privacy policies and data collection are now a part of our everyday life - whether it's scrolling on a news or social media website, shopping online, or even creating an email account - our data is being collected and shared with the website hosts and others if the company collecting our data sells it to other parties (Pantelic 4). The CCPA has pushed sites to disclose their cookie policies to users, which has incidentally affected the entire U.S. as non-California residents and California residents visit the same sites, but it can become meaningless if users do not know what they are reading or if the privacy policies are not explicit in the ways they are collecting data. While 81% of Americans agree to privacy policies presented to them on a monthly basis, only 22% read a majority of them. 13% of people understand a great deal of what is being said in privacy policies, while 55% only understand some of what is being said (Auxier et al.). In a cookie policy readability study done by Elizabeth Rawlings, the average reading level of adults Americans between the 7th and 8th grade reading level, while the average reading level needed to understand privacy policies is 12th grade level (Rawlings 4). Due to a low level of understanding, there is a higher concern for an individual's privacy protection. Even with new privacy acts being passed to protect consumer rights, only 3% of Americans understand the acts and policies that have been put in place to protect their privacy (Auxier et al.).

There is a large knowledge gap between the information presented by companies and the level of knowledge the user has on privacy and data collection. As written by Estee Beck concerning privacy literacy with middle school students, it is imperative that people are being taught what they need to know to protect themselves online as many internet users are forming their online identities from a young age (Beck 137). While it's not the individual's sole responsibility to become informed on privacy rights and how companies use their information, there needs to be more education and awareness on this topic as we reach an extremely highly technological age. Even as the legislature works to protect our rights as internet users, technology and methods for data collection will only become even more advanced which could possibly further the knowledge gap between companies and consumers. It is crucial for companies to find ways to create a more transparent and understandable method to informing consumers how their data is being collected and where it is going, as it has been shown that privacy policies are not the most effective ways to provide users and consumers with the proper information needed for them to make informed decisions about their personal information. When it comes to online privacy, it seems as though the two main threats are the individual consumer's knowledge and the company's ability to be transparent about the data collection that is present on their platforms.

Behavioral advertising, or third-party advertising, is among the most popular advertising methods but comes at a huge cost to user privacy. Third-party advertising uses the data collected from third-party cookies to precisely tailor and place ads on a user's browser. It's important to note that third-party cookies are far more connected than you think. A single cookie could be placed by a company which is then shared within that company's network, which can range from as little as five to over one hundred other companies. There's a high possibility that when you visit one website, hundreds of other websites that you may not have visited before are gaining that information as well without you knowing (Johnson, G. 2:15). According to a survey taken by 500 senior level marketers, 51% said their company relies heavily on third-party data, and 32% said they used a combination of both first- and third-party data. Only 7% of respondents stated they started using other sources of data following Google’s announcement of phasing out third-party cookies (Innovid). This leaves a large number of retailers and advertisers scrambling to find alternative methods without sacrificing a large amount of their profit typically earned by using Google Ads. It is a difficult task, as online advertising supported by third-party data has played such a big role in how companies get new customers on their websites.

There are two main forms of advertising that are largely used amongst companies to precisely target their audience. There is third-party advertising, or behavioral advertising, which is the advertising method surrounded by high concerns of lack of privacy, and there is contextual advertising (Bleier 2). Third-party advertising relies heavily on data collected from third-party cookies, while contextual advertising relies on the user’s browsing history and first-party cookies. Both methods have proven to be successful, but both still require a certain amount of data from the user’s end. A benefit of contextual advertising is its use of machine learning and AI, which helps to predict which advertisements the user would want to see based on their past browsing history. While contextual advertising is praised for taking less data from the user, there are still many concerns surrounding contextual advertising, as it does also take into account the user’s location and IP address, which threatens the safety of the user’s personal information. Additionally, contextual advertising is heavily reliant on the progress of machine learning, making it a risky alternative as it develops further (Bleier 8-9). While Google specifically has relied on third-party cookies to help companies target their advertisements, they have started to use contextual advertising as inspiration for replacing their current third-party data collection method. Despite contextual advertising being a main method in advertising, it is interesting to see Google’s struggle with developing a cookieless method which could be due to the scale of their Google AdSense and Analytics business.

With increased frustration and confusion on the consumer's side, large companies have started to strategize ways to combat the feeling of helplessness and lack of control users have. In 2019, Google announced that they would begin to phase out the use of third-party cookies by default for all users starting in 2022, which has since been pushed to the beginning of 2024 (Google, Inc. "How we're protecting your privacy online"). While they are late to the game considering both Firefox and Safari did this by 2020 (Wood), Google has many more variables that can change the future landscape of online advertising. According to their 2020 annual report, Google reported about 183 billion dollars in revenue, with 147 billion coming from their advertising platform, Google Ads (Security and Exchange Commission 33). Google is known for their advertising, whether through paid search, sponsored videos on YouTube, and selling ad space on various websites. With Google looking to phase out third-party cookies on their browser, many advertisers and data brokers are worried about the future of advertising and how the new landscape of advertising will look.

Google has been at the forefront of developing new methods for cookieless advertising. Shortly after their announcement of the removal of third-party cookies, Google created a collective privacy effort called The Privacy Sandbox (Google, Inc. "Protecting your Privacy Online") which has partners in the advertising industry that are all working together to create solutions that preserve user privacy while still placing personalized advertisements across the web. Through the Privacy Sandbox, Google has been testing different methods that could replace third-party advertising, including their initial test model called "FLoC". FLoC, which is short for Federated Learning of Cohorts, aimed to group users by their interests based on the websites they visited without grabbing any personally identifiable information. The main idea surrounding FLoC was to develop user cohorts based on similar interests, so users would be tracked as a group rather than as individuals. Users would be grouped into cohorts based on their browser history, which would then be observed by both advertisers and websites with ad space (Dutton). Advertisers would then decide which websites would work best for ad placement depending on where the cohorts frequented most. Google was hoping to incorporate federated learning, a decentralized method of data collection in which a machine learning model is downloaded to the user's device, trained, and sent back without sharing the user data into this new method. The FLoC method received a lot of backlash, including debates over whether or not it followed the guidelines set out by the GDPR, and whether this method was actually able to protect user privacy. Having users in cohorts, if anything, meant greater chances of personally identifying someone from a smaller pool. Additionally, there was no federated learning present in Google's user testing, despite their testing goal being to determine the effectiveness of the new method of data collection (Eliot, David, et al. 262-266). Shortly after receiving backlash, Google abandoned this idea and started a new project called Topics.

Topics is Google's most recent proposed alternative to advertising without cookies. The Topics API works within a user's server to determine a list of "topics" that align with the user's browsing history (Goel). Based on these topics, relevant advertisements will be placed for the user to see. Developers at Google preemptively created a list of 350 topics that each site can be categorized under, which is expected to grow as Topics develops further. There seem to be a few notable improvements with this method in comparison to its predecessor, FLoC. First, your browsing history and most relevant topics will only be shared with the websites you have visited that week, which is a big difference from third-party cookies, as they would share your data with a network of different websites that you may have never visited before . The data collected will remain solely on your server, rather than being sent to others. The information inferred from your browsing history will be available to you in your profile and you will be able to edit the categories given, or completely opt out from using Topics (Israel and Trotz). At first glance, this proposed method seems to be more ethical and more compliant with the GDPR, and Google has also been open about the user testing for Topics, which is an improvement from their lack of transparency with their FLoC testing. If the testing proves the method to be successful enough to replace third-party data tracking and advertising, many companies will follow suit due to Google Chrome making up 65.84% of the global market share, and 50.62% of the United States market share (Statcounter Global Stats). While Topics API seems to address many issues consumers have had with their privacy, there are still some worries with this proposed advertising method and its introduction to the advertising industry.

There are many windows of opportunity for Google as they navigate the new landscape of a soon to be cookieless web. They have the opportunity to gain the trust of consumers by creating a method that really takes into account their concerns for privacy and ambiguity in privacy policies, but it could come at the cost of some of their revenue made by their advertising business. Google, as a leader in digital advertising, needs to make sure their values align with those of the consumer if they wish to be trusted in the future. Consumers have reached a point where they hold no trust in where their data is going and who is handling it, with 81% of Americans stating they have very little to no control over their data that is collected by companies and 72% of Americans expressing they feel that all or most of their online usage is being tracked by companies (Auxier et al.). From both of Google's missions to remove third-party cookies, it seems as though they are more worried about the revenue they would lose from ad placement than the actual concerns of privacy their users have. While Firefox and Safari have already removed third-party cookies, it seems the one aspect holding Google back from making the switch as well is whether or not they will be able to monetize their new advertising product and space for advertisements to the same level they have been achieving over the years. It’s important for Google and the companies they have partnered with to create the Privacy Sandbox to remain open and transparent about the projects they are working on, as they are creating a new foundation for advertising, consumer trust, and consumer privacy.

Concerns demonstrated by many online consumers include the general ambiguity surrounding data collection, a lack of control over where their data goes and who it is shared with, as well as the limited transparency from companies that have the ability to collect their data. If Google wishes to create a new method of targeted advertising, it is extremely important they take into account the concerns and frustrations expressed by consumers, as they are the industry leaders in advertising with many advertising companies and businesses relying on their Google Ads products. Consumers in general have demonstrated a low level of understanding when it comes to their online privacy, leading to higher concern levels and increased frustration. As important as it is for Google to increase transparency and trust in the data collection process, it is just as important that consumers find tools necessary to educate themselves on their rights as consumers, data privacy, and how they can protect themselves in this age of surveillance capitalism. With both working hand in hand, we could create a new age of digital advertising that is trustworthy, transparent, and less ambiguous to the average consumer.

Works Cited

Auxier, Brooke, et al. "4. Americans' attitudes and experiences with privacy policies and laws." *Pew Research Center*, 15 November 2019, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/. Accessed 14 December 2022.

Beck, Estee N. "The Invisible Digital Identity: Assemblages in Digital Networks." *Computers and Composition*, vol. 35, Mar. 2015, pp. 125–40. *EBSCOhost*, https://doi.org/10.1016/j.compcom.2015.01.005.

Bleier, Alexander, On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web (December 7, 2021). Available at SSRN: https://ssrn.com/abstract=3980001 or http://dx.doi.org/10.2139/ssrn.3980001

Congressional Research Service. "H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act." *Congress.gov*, 21 June 2022, https://www.congress.gov/bill/117th-congress/house-bill/8152. Accessed 14 December 2022.

Desai, Anokhy. "US State Privacy Legislation Tracker." *International Association of Privacy Professionals*, 7 October 2022, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. Accessed 14 December 2022.

Dutton, Sam. "FLoC." *Chrome Developers*, 18 May 2021, https://developer.chrome.com/docs/privacy-sandbox/floc/. Accessed 14 December 2022.

Eliot, David, et al. "Culling the FLoC: Market Forces, Regulatory Regimes and Google's

(Mis)Steps on the Path Away from Targeted Advertising." *Information Polity: The International Journal of Government & Democracy in the Information Age*, vol. 27, no. 2, Apr. 2022, pp. 259–74. *EBSCOhost*, https://doi.org/10.3233/IP-211535.

Fazlioglu, Müge. "US Federal Privacy Legislation Tracker." *International Association of Privacy Professionals*, December 2022, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/. Accessed 14 December 2022.

FTC. "Internet Cookies." *Federal Trade Commission*, May 2021, https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies. Accessed 14 December 2022.

Goel, Vinay. "Get to know the new Topics API for Privacy Sandbox." *The Keyword*, 25 January 2022, https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/. Accessed 14 December 2022.

Google, Inc. "How We're Protecting Your Online Privacy." *The Privacy Sandbox*, 2022, https://www.privacysandbox.com/open-web/#the-privacy-sandbox-timeline. Accessed 14 December 2022.

Google, Inc. "Protecting your Privacy Online." *The Privacy Sandbox: Technology for a More Private Web.*, https://www.privacysandbox.com/#privacy-sandbox-news. Accessed 14 December 2022.

Innovid. "Marketers Are Still Reliant on 3rd-Party Cookies." *Marketing Charts*, 13 October 2021, https://www.marketingcharts.com/customer-centric/datadriven-118489. Accessed 14 December 2022.

Israel, Leeron, and Joey Trotz. “Topics API: latest updates.” *Chrome Developers*, 4 November 2022, https://developer.chrome.com/docs/privacy-sandbox/topics/latest/. Accessed 14 December 2022.

Johnson, Garrett. *The Cookies are Crumbling: What’s Next for Digital Advertising?* 3 February 2022. *YouTube*, Questrom School of Business, https://www.youtube.com/watch?v=6y-nIrq4CO0. Accessed 12 December 2022.

Johnson, Steven. “Lou Montulli and the invention of cookie | Hidden Heroes.” *Hidden Heroes*, 21 October 2022, https://hiddenheroes.netguru.com/lou-montulli. Accessed 14 December 2022.

Mills, Elinor. “Google buys ad firm DoubleClick for $3.1 billion.” *CNET*, 13 April 2007, https://www.cnet.com/tech/tech-industry/google-buys-ad-firm-doubleclick-for-3-1-billion/. Accessed 14 December 2022.

Moschovitis, Chris. “North American Regulations.” In *Privacy, Regulations, and Cybersecurity: The Essential Business Guide,* edited by Hilary Poole, Ch. 5. Hoboken: John Wiley & Sons, Inc., 2021

Pantelic, Ognjen, et al. “Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations.” *Sustainability (2071-1050)*, vol. 14, no. 9, May 2022, p. 5015. *EBSCOhost*, https://doi.org/10.3390/su14095015.

Rawlings, E. D. “Do You Know What’s in Those Cookies? An Analysis of the Readability of Social Media Cookie Policies.” *Proceedings of the Association for Information Science and Technology*, vol. 57, no. 1, Oct. 2020. *EBSCOhost*, https://doi.org/10.1002/pra2.300.

Security and Exchange Commission. “Alphabet Inc. Form 10-K.” *Alphabet*, 2 February 2021, https://abc.xyz/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d. Accessed 14 December 2022.

Statcounter Global Stats. “Browser Market Share United States Of America.” *Statcounter Global Stats*, 2022, https://gs.statcounter.com/browser-market-share/all/united-states-of-america#yearly-2009-2021. Accessed 14 December 2022.

Wood, Marissa. “Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default.” *The Mozilla Blog*, 3 September 2019, https://blog.mozilla.org/en/products/firefox/firefox-news/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/. Accessed 14 December 2022.