Catholic University Journal of Law and Technology

Volume 30
Issue 1 *Fall 2021*

Article 7

2021

"Times They Are A Changin'" - Can the Ad Tech Industry Survive in a Privacy Conscious World?

Meaghan Donahue
Catholic University of America (Student)

"*TIMES THEY ARE A CHANGIN*" – CAN THE AD TECH INDUSTRY SURVIVE IN A PRIVACY CONSCIOUS WORLD?

Meaghan Donahue[*]

Just like death and taxes, advertising seems to be one of the only things we can be certain about as consumers in twenty-first century America. This is evidenced by the fact that every day, whether you are aware of it or not, you are exposed to anywhere between six and ten thousand promotional messages on a variety of platforms.[1] On your phone, your television, or the newspaper you pick up on the way to work, the advertisements you interact with are not random. Rather, they are strategically placed in front of you in hopes that you relate to the content and feel compelled to buy the product. This is the central goal of all advertising campaigns – connecting products with people who want or need to buy them. In any lucrative advertising campaign, it is necessary to understand who exactly your audience is and how to reach them.[2] No matter how innovative the content of an advertisement may be, making sure it is seen by the right

[*] *Juris Doctor* Candidate, Columbus School of Law, 2022; *The Catholic University Journal of Law and Technology*, Managing Note and Comment Editor, 2021-2022; Bachelor of Arts, American University, 2019. Many thanks to Charlotte Kress for her assistance and advice in drafting this article, and to my fellow JLT Vol. 30 Executive Board members for their editorial advice. Thank you to my parents, family, friends, and fiancé, who have offered their consistent support through the entirety of my academic career. This article is dedicated to my grandfather, my best friend, and biggest source of inspiration, Edward J. McCormick Sr., J.D. (1941-2021). Without him none of this would be possible.

1 Sam Carr, *How Many Ads Do We See A Day In 2021?*, PPC PROTECT (Feb. 15, 2021), https://ppcprotect.com/how-many-ads-do-we-see-a-day/.

2 *Steps to Finding Your Target Audience*, MKTG. EVOLUTION, https://www.marketingevolution.com/marketing-essentials/target-audience (last visited Nov. 8, 2021) ("Your target audience refers to the specific group of consumers most likely to want your product or service, and therefore, the group of people who should see your ad campaigns. Target audience may be dictated by age, gender, income, location, interests or a myriad of other factors.").

audience is paramount to its success. Understanding who to serve an advertisement to relies on audience segmentation, driven by market data and consumer information.[3] The amount of consumer information available, and the efficient means of access to it, has skyrocketed since the early days of advertising, changing the landscape in ways unimaginable only decades ago.[4]

Targeted advertising has been common practice since the 1930s and the dawn of the radio soap opera.[5] These daytime dramas earned their titles thanks to companies like Procter & Gamble, who capitalized on the profitability of serving advertisements for soap and laundry detergent to the shows' housewife-dominated viewership.[6] Beginning in the 1970s, advertisers started using psychographics to segment audiences by lifestyle, rather than gender alone.[7] Marketers looked to factors such as "attitudes, beliefs, opinions and personality traits" to find the perfect audience for their content – increasing their return on investment by only paying to serve ads to the consumers most likely to buy their product.[8] In decades past, where mediums such as print and television reigned supreme, the task of content placement was fairly uncomplicated.[9] However, all of this changed with the advent of the internet.

The internet changed marketing in many positive ways. Today, online advertising is cheaper than traditional print or television advertisements, has the potential to reach a seemingly limitless number of customers, provides increased speed, and allows companies to monitor the efficiency of their efforts in real-time.[10] However, the biggest impact the internet has had on the advertising industry is increased access to the consumer data used to segment markets and serve targeted content.[11] Now, "[p]eople and machines . . . [use] tracking tools

---

3 *Id.*

4 Roy de Souza, *A Short History of Targeted Advertising*, ZEDO (May 27, 2015), https://www.zedo.com/short-history-targeted-advertising/.

5 Daniel Ganninger, *Why Are Daytime Dramas Called Soap Operas?*, KNOWLEDGE STEW (Sept. 5, 2017), https://knowledgestew.com/2017/09/why-daytime-dramas-called-soap-operas.html.

6 *Id.*

7 de Souza, *supra* note 4.

8 *Id.*

9 JOHN DEIGHTON & LEORA KORNFELD, THE SOCIOECONOMIC IMPACT OF INTERNET TRACKING 8 (Interactive Advert. Bureau Feb. 2020), https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf ("For most of the centuries-long history of advertising, advertisers bought media. They relied on publishers, including broadcasters, to assemble audiences of readers and viewers, and chose the most relevant of these audiences for their particular purposes. The *Wall Street Journal* assembled one kind of audience, while *Look* magazine assembled a different kind.").

10 George Abraham, *10 Major Advantages of Online Advertising/Digital Marketing*, ONLINE MKTG. BLOG (May 13, 2010), https://www.georgescifo.com/2010/05/10-advantages-of-online-advertising/.

11 DEIGHTON, *supra* note 9, at 8.

such as cookies to identify browsers and to track consumer activities on the internet, often without giving consumers a choice . . . ."[12] Advertisers increase returns by only paying for ads being shown to their niche consumer base, and publishers can sell their highly precise ad placements for a premium.[13] While this has inherently benefitted the efforts of advertisers and publishers, it has left many consumers and lawmakers concerned about potential implications and looking for regulatory answers to what many consider an invasion of privacy.[14] As the conversation around state and federal privacy legislation intensifies, and large corporations work to change internal practices to emphasize consumer privacy, the fate of the digital targeted advertising industry, particularly smaller startups, hangs in the balance.[15] However, by shifting away from current industry standards and utilizing new technologies and modeling practices, the ad tech industry will be able to retain its lucrative ability to target consumers, while promoting and respecting user privacy.[16]

This article will introduce the ad tech ecosystem and the ways legislation and private sector policy reform threaten the current nature of digital targeted advertising. First, it will explain the complex and multifaceted nature of advertising technology and the personal information collected by companies in order to fuel it. Next, it will discuss the California Consumer Privacy Act, the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act and other proposed state and federal privacy legislation and the potential impact on the way the ad tech industry conducts business. Finally, it will analyze the current industry response, and hypothesize what the future of targeted advertising will look like in a world with broadly enacted comprehensive privacy legislation, coupled with corporate policies that reject the use of intrusive technological practices such as third-party tracking cookies and browser fingerprinting.

---

12 *Id* at 3.

13 Ibrahim Pataudi, *HackFwd Project: Ad-Tech for Dummies with a Mind Towards Mobile*, MEDIUM (Feb. 17, 2017), https://medium.com/@ibrahimpataudi/hackfwd-project-ad-tech-for-dummies-with-a-mind-towards-mobile-ec797bd47f9c.

14 *See generally* Andrew Blustein, *Why Lawmakers Are Keeping Ad Tech Under Such Close Scrutiny*, ADWEEK (Aug. 26, 2020), https://www.adweek.com/programmatic/why-lawmakers-are-keeping-ad-tech-under-such-close-scrutiny/ ("Ten . . . members of Congress signed a July 31 letter to the Federal Trade Commission asking the regulatory agency to investigate 'widespread privacy violations by companies in the advertising technology industry that are selling private data about millions of Americans, collected without their knowledge or consent.'").

15 *Id.*

16 Elizabeth Anne Watkins, *Guide to Advertising Technology*, COLUM. JOURNALISM REV. (Dec. 4, 2018), https://www.cjr.org/tow_center_reports/the-guide-to-advertising-technology.php.

I. BACKGROUND

A. The Issue: Weighing the Benefits of Targeted Advertising against Privacy Concerns

We've all been there—while scrolling through our Instagram feed, online shopping, or watching a YouTube video, our browser serves up an advertisement for something we were just talking about. We ask, "is my computer listening to me?" If only it was that simple. By collecting and analyzing the data provided by what we search, the locations we frequent, and the accounts we interact with, the internet is helping advertisers understand our wants, needs, desires, and beliefs and, in essence, read our minds.[17]

Advertising technology, sometimes referred to as "programmatic advertising," or "ad tech," is an umbrella term used to describe "the system of software programs, data servers, marketing agencies, and data markets which facilitate the sale of user data and the display of advertising messages to users of the internet, including search engines and social-media sites and apps."[18] Using this data, advertisers serve targeted content based on the habits, beliefs, and sometimes, prejudices and biases of consumers.[19] Advertising technology has completely changed the way brands engage with consumers. Now, "[a]dvertisers can buy access to the people they want to reach because they have the data to find them and are able to do so without having to pay for access to unwanted people who often make up a large part of a publication's audience."[20] As this article will detail in Section II, b., advertisers buy this access by engaging with other players in the ad tech ecosystem, exchanging monetary value for access to consumer information.[21]

The intricate system of technology that makes up the ad tech ecosystem is responsible for the internet we know today.[22] For example, "[c]onsumers benefit from getting more relevant ads, which advertisers will pay more to place, which

---

17 *Id.*

18 *Id.*

19 DEIGHTON, *supra* note 9, at 6; *See also* Dipayan Ghosh & Ben Scott, *Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You*, TIME (Mar. 19, 2018), https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/ (discussing the way Cambridge Analytica used "highly sensitive personal data taken from Facebook users without their knowledge to manipulate them into supporting Donald Trump . . ." in the lead up to the 2016 election).

20 DEIGHTON, *supra* note 9, at 8.

21 *See infra* Section II.b.

22 *See generally* David Benady, *Can Advertising Support a Free Internet?*, THE GUARDIAN (Nov. 7, 2016), https://www.theguardian.com/media-network/2016/nov/07/can-advertising-support-free-internet.

in turn generates more revenue for publishers, thereby fostering free, ad-supported content that also benefits consumers."[23] However, "free" is a loaded term–we all know too well "there's no such thing as free lunch."[24] So how do the richest companies on the web continue to rake in money and users? Instead of charging consumers for services (i.e., Gmail, Facebook, Google Search, etc.), advertisers pay a premium for access user data, which platforms in turn use to serve consumers the most relevant advertisements possible.[25] User data, in many ways, has become the product and advertising has become the service.[26] This has proven to be an extremely lucrative model for web services companies and social media platforms.[27] In 2017, nearly all of Google and Facebook's profit came from digital advertising services,[28] and in 2018, the market for digital advertising topped $100 billion in the United States.[29]

B. The Ad Tech Ecosystem Explained

The ad tech ecosystem is a web of complicated, interconnected entities that, at its core, is designed to connect buyers and sellers within the digital advertising space by the most efficient and lucrative means available.[30] Ad tech exists in two forms – "[1] an open web ecosystem or [2] a walled garden."[31] An open-web ecosystem relies on industry collaboration and the broad-scale exchange of user data, whereas walled gardens consist of only one, usually large entity, and rely on its own first-party data.[32] Understanding who the major market players are and how the technology functions is essential to comprehending the potential privacy implications and the impact of legislative efforts on ad tech practices.[33]

When you think of traditional advertising, you likely envision a fairly simple

---

23 Alan L. Friel, *Ad and Publishing Industries Confront CCPA Challenges while Congress Considers Privacy*, 37 No. 03 WESTLAW J. COMP. & INTERNET 02 (2019).

24 *See generally* Fred Shapiro, *You Can Quote Them*, YALE ALUMNI MAG. (Mar. 2009), https://yalealumnimagazine.com/articles/2399-you-can-quote-them.

25 Benady, *supra* note 22.

26 Vincent Tabora, *In Big Data, the Consumer Is the Product*, MEDIUM (Nov. 1, 2019), https://medium.com/swlh/in-big-data-the-consumer-is-the-product-ad9bf0423d9a.

27 *Id.*

28 Daniel Kessler, *This is Your Digital Fingerprint*, MOZILLA (July 26, 2018), https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint/.

29 Megan Graham, *Digital Ad Revenue in the US Surpassed $100 Billion for the First Time in 2018*, CNBC (May 7, 2019), https://www.cnbc.com/2019/05/07/digital-ad-revenue-in-the-us-topped-100-billion-for-the-first-time.html.

30 *With CCPA Enforcement, Programmatic Can Prove Its Worth*, MEDIAMATH (Sept. 14, 2020), https://www.mediamath.com/news/with-ccpa-enforcement-programmatic-can-prove-its-worth/.

31 DEIGHTON, *supra* note 9, at 15.

32 *Id.*

33 Ian Simpson, *What Exactly Is AdTech?*, CLEARCODE, https://clearcode.cc/blog/what-is-adtech/#adtech-&-the-advertiser-publisher-relationship (last updated Nov. 27, 2020).

two-step process that involves a brand buying space to place content on a platform or in a publication. This largely describes contextual advertising in an age before advertising technology.[34] To reach desired target markets, advertisers would directly buy space on websites or in publications that their target audience was likely to visit.[35] From there, one advertisement would be served to every visitor of the site or reader of the publication, no matter if this person fell within their target audience or not.[36] While workable, this practice was financially inefficient, as advertisers were paying to serve content to their target audience, as well as to consumers who would likely never buy their product.[37] This changed drastically with the introduction of advertising technology and behavioral advertising.[38] Now, the process is highly complex, involves multiple intermediaries, and is largely facilitated by software and algorithms in real-time.[39]

The open web ad tech cycle begins the same way as traditional contextual advertising, with a buyer, or the advertiser, and a seller, or the publisher.[40] These entities exist on opposite ends of the ad tech equation. Publishers are the websites, blogs, or social media platforms that sell the opportunity to display ads on their pages to advertisers.[41] They rely on supply-side platforms (SSPs) to manage display space inventory in real-time.[42] Advertisers, on the other hand, are the companies trying to buy digital advertising space.[43] They rely on demand-side platforms (DSPs) "to buy impressions across a range of publisher sites, [] targeted to specific users based on information such as their location and

---

34 James Chen, *Contextual Advertising*, INVESTOPEDIA, https://www.investopedia.com/terms/c/contextual-advertising.asp (describing contextual advertising as "an automated process where a promotional message is matched to relevant digital content.") (last updated Apr. 19, 2021),

35 *What is Programmatic Advertising? The Ultimate 2022 Guide: A Brief History of Display Advertising and The Rise of Programmatic*, MATCH2ONE, https://www.match2one.com/blog/what-is-programmatic-advertising/#A_brief_history_of_display_advertising_and_the_rise_of_programmatic (last updated Sept. 22, 2022).

36 *Id.*

37 *Id.*

38 Michael Wlosik, *What Is Behavioral Targeting and How Does It Work?*, CLEARCODE, https://clearcode.cc/blog/behavioral-targeting/ (last updated Nov. 25, 2020) (defining behavioral advertising as "a method that allows advertisers and publishers to display relevant ads and marketing messages to users based on their web-browsing behavior.").

39 *Id.*

40 Simpson, *supra* note 33.

41 Smit Srivastava, *Programmatic Advertising: The Complete Life-Cycle for the Beginners*, MEDIUM (Dec. 30, 2019), https://medium.com/@smit.srivastava/programmatic-advertising-the-complete-life-cycle-for-the-beginners-c1b0291d01fd.

42 *What is Programmatic Advertising? The Ultimate 2022 Guide: A Brief History of Display Advertising and The Rise of Programmatic*, *supra* note 35.

43 Srivastava, *supra* note 41.

their previous browsing behavior."[44] DSPs sometimes analyze user information from their own databases, but often work with a Data Management Platform (DMPs)[45] – software designed to manage user data like cookies and mobile identifiers from across the web.[46] DMPs aggregate the millions of data points they collect and create profiles of customers and users which then are used to find the perfect spot for an ad creative depending on the inventory made available by the publishers and their DSPs.[47]

Advertisers and publishers rely on DSPs and SSPs largely because of the speed with which the buying and selling occurs and the large quantity of content and user data involved.[48] The vast majority of ad tech is facilitated through real-time bidding,[49] which "refers to the buying and selling of online ad impressions through real-time auctions that occur in the time it takes a webpage to load."[50] Real-time bidding increases the speed and accuracy with which ads are served, and occurs on a "per-case basis," meaning that content of the advertisement is tailored to the individual user.[51] To facilitate real-time bidding, DSPs and SSPs run requests through Ad-Networks and Ad-Exchanges, which operate as marketplaces for the buying and selling of digital advertisements and serve as the connection between the supply and demand sides of the equation.[52] When a user launches a publisher's web page, the SSP communicates to the Ad Exchange exactly what type of display space is available.[53] When the Ad Exchange indicates the availability of inventory, the "DSP analyses the value of

---

44 Jack Marshall, *WTF Is a Demand-Side Platform*, DIGIDAY (Jan. 8, 2014), https://digiday.com/media/wtf-demand-side-platform/; Will Kenton, *Impression*, INVESTOPEDIA (Aug. 10, 2020), https://www.investopedia.com/terms/i/impression.asp ("An impression is a metric used to quantify the number of digital views or engagements of a piece of content, usually an advertisement, digital post, or a web page. Impressions are also referred to as an 'ad view.'").

45 Srivastava, *supra* note 41.

46 Ginny Marvin, *MarTech Landscape: What Is a Data Management Platform (DMP)?*, MARTECH (Apr. 22, 2016), https://martechtoday.com/what-is-dmp-martech-landscape-174298 (explaining cookies and mobile identifies "creates targeting segment for their digital advertising campaigns.").

47 Laura Starita, *How Does a Data Management Platform Work?*, GARTNER (Nov. 20, 2019), https://www.gartner.com/en/marketing/insights/articles/how-does-a-data-management-platform-work.

48 Srivastava, *supra* note 41.

49 *See generally What is Programmatic Advertising? The Ultimate 2022 Guide: A Brief History of Display Advertising and The Rise of Programmatic*, *supra* note 35 (noting that over 80% of digital marketing in the United States is done through programmatic advertising).

50 Marshall, *supra* note 44.

51 *What is Programmatic Advertising? The Ultimate 2022 Guide: A Brief History of Display Advertising and The Rise of Programmatic*, *supra* note 35.

52 Srivastava, *supra* note 41.

53 *What is Programmatic Advertising? The Ultimate 2022 Guide: A Brief History of Display Advertising and The Rise of Programmatic*, *supra* note 35.

the impression for the advertisers based on the information it has regarding the impression either directly from its user profile database or from third-party [DMPs]."[54] The result is a highly relevant advertisement placed on a user's screen nearly instantaneously.[55]

The biggest players in the ad tech space are, unsurprisingly, Facebook and Google.[56] Referred to as the "duopoly," these tech-giants control an estimated 60% of the global digital advertising market.[57] Google in particular controls a huge portion of the ad tech market, worth an estimated $40.05 billion in 2019.[58] Google and Facebook's strength comes largely from their seemingly limitless pool of user data; the pair has almost 4 billion combined monthly users.[59] From these users, they collect scores of personal information like name, email, and phone number, in addition to location data, search history, purchase history, views, comments, and more.[60] This pool of data allows the duopoly to facilitate the buying and selling of premium ad space at a higher price, which advertisers willingly pay to ensure their content is seen by only the most relevant audiences.[61]

The largest platforms on the web have access to such a populous base of users that they do not need to rely on obtaining information from traditional data brokers to target consumers.[62] Facebook and Google, in addition to Apple, Amazon (collectively referred to as "GAFA") and others, function as "walled gardens," which are "closed ecosystem[s], operated by people within the ecosystem, without the involvement of an outside organization."[63] These companies keep their "technology, information, and user data to [themselves], with no intention of sharing…" and run their own miniature version of the ad

---

54 Srivastava, *supra* note 41.

55 *What is Programmatic Advertising? The Ultimate 2022 Guide: A Brief History of Display Advertising and The Rise of Programmatic*, *supra* note 35.

56 Connor Finnegan, *How Facebook and Google Track Your Online Behavior*, MEDIUM (Feb. 13, 2019), https://medium.com/@ConnorFinnegan/how-facebook-and-google-track-your-online-behavior-26f161d370ab.

57 Michal Wlosik & Michael Sweeney, *Walled Gardens v. Independent AdTech: The Fight for Ad Dollars and Survival*, CLEARCODE, https://clearcode.cc/blog/walled-garden-vs-independent-adtech/ (last updated June 18, 2021).

58 Graham, *supra* note 29.

59 Wlosik, *supra* note 57; Graham, *supra* note 29.

60 Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have on You*, SECURITY.ORG, https://www.security.org/resources/data-tech-companies-have/ (last visited Nov. 19, 2021).

61 *How Facebook Makes Money from Personal Data*, PRIV. TRUST, https://www.privacytrust.com/blog/how-facebook-makes-money-from-personal-data.html (last visited Nov. 6, 2021).

62 Rashmita Behera, *What Does 'Walled Garden' Mean in Ad Tech*?, ADPUSHUP (June 18, 2019), https://www.adpushup.com/blog/walled-garden-in-adtech/.

63 *Id.*

tech ecosystem within their walls.[64] This is directly juxtaposed to the nature of ad tech on the open web, which requires that entities from the supply and demand side swap user data to enhance tracking abilities.[65] The current state of the ad tech ecosystem is fueled by the sharing of this information.[66] Consequently, the monopolistic practices of the biggest collectors of user data have the potential to make market entry difficult for smaller entities.[67]

Publishers and advertisers alike are drawn to walled gardens, as they provide a "one stop shop" that can easily facilitate cross-device tracking of billions of consumers, provide a more secure means of data processing, and produce highly accurate consumer profiles that result in more efficient ad placement without the use of traditional tracking mechanisms.[68] However, putting so much power in the hands of the few may prove to be dangerous without proper industry standards or transparency regulations in place.[69] With the amount of reliable user data being collected and associated with personally identifiable information, eerily accurate profiles of users that go beyond the needs of targeting are being created that, in the case of a companywide cyber-breach, could put users at heightened risk.[70] In the past two years, Google and Facebook have come under fire for their practices – for example, Unilever, a leading global advertiser, threatened to pull all advertising from the sites, comparing the duopoly's transparency regarding data collection and use to that of a "swamp."[71]

C. How Data Fuels Ad Tech

With a high-level understanding of the technology that fuels the ad tech industry and the major players who control it, it is next necessary to understand

---

64 *Id.*

65 DEIGHTON, *supra* note 9, at 13.

66 Behera, *supra* note 62.

67 *Id.*

68 Callan Smith, *Walled Gardens in Digital Advertising – Explained*, PUBGALAXY (Sept. 28, 2020), https://www.pubgalaxy.com/blog/ad-tech/walled-gardens-in-digital-advertising-explained/; *see also* Rashmita Behera, *Cross-Device Tracking: Why the Industry Needs It | Benefits + Challenges*, ADPUSHUP (Mar. 19, 2019), https://www.adpushup.com /blog/cross-device-tracking/ ("The idea [behind cross-device tracking] is to create a detailed profile of each user by tracking his/her interactions even if they are using multiple [devices and] then storing/using that data whenever required. For instance, in the ad tech industry, such data can be used to run ad campaigns targeted across devices.").

69 *Data Security: 25 Important Facts & Statistics for 2021*, SECURITY.ORG, https://www.security.org/resources/data-security-facts-statistics/ (last updated May 10, 2021); Wlosik, *supra* note 57.

70 *See generally id.* (explaining current data on business' data breaches and cybercrime against consumers).

71 Charles Riley, *Unilever to Facebook and Google: Clean Up 'Swamp' Or We'll Pull Ads*, CNN BUS. (Feb. 12, 2018), https://money.cnn.com/2018/02/12/media/unilever-advertising-facebook-google-swamp/index.html.

what exactly is being collected in order to achieve accurate targeting. Consumers are targeted based on data collected via methods such as cookies, fingerprints, persistent identifiers, and mobile device identifiers.[72] While these practices do not explicitly attach a user's "real" name to their browsing activity, "the data they derive from websites you visit, social platforms you use, searches you perform, and content you consume, can be considered personally identifiable" and allows data management companies to "build a general profile of who you are (age range, location, language, interests, etc.) and sell this insight to advertisers and marketers who use it to relentlessly serve you personalized ads and content recommendations across the web."[73] The highly sensitive nature of the information, coupled with the ease with which ad tech companies can access it further exasperates the need for meaningful safeguards.

1. Cookies

At the core of the ad tech industry's pervasiveness is the cookie. Cookies are "small strings of code and data that websites install onto a user's computing device and subsequently read so that they can recognize the user on a subsequent encounter."[74] In the early days of the internet, the cookie was used to facilitate e-commerce and allow users to customize their online experiences.[75] Today, cookies are the primary way ad tech companies collect information to serve consumers targeted behavioral advertisements.[76]

A large number of cookies we interact with on a daily basis are benign.[77] These are known as first-party cookies, and the data collected is only readable by the website that placed the cookie.[78] A first-party cookie is considered such if it "comes from the domain whose name is the one shown in the visitor's browser's window."[79] While highly informative and accurate, first-party data is difficult to share and requires a website owner to invest in building out robust customer data sets. [80] Third-party cookies, on the other hand (also known as "tracking cookies"),[81] are placed by a website other than the domain a user is

---

72 DEIGHTON, *supra* note 9, at 8, 10.
73 Kessler, *supra* note 28.
74 DEIGHTON, *supra* note 9, at 9.
75 *Id.* at 9.
76 *Id.* at 8.
77 Denis Anon, *How Cookies Track You Around the Web and How to Stop Them*, PRIVACY.NET (Feb. 24, 2018), https://privacy.net/stop-cookies-tracking/.
78 DEIGHTON, *supra* note 9, at 9.
79 *Id.*
80 SHILPA PATEL ET AL., THE DIVIDENDS OF DIGITAL MARKETING: RESPONSIBLE MARKETING WITH FIRST-PARTY DATA 5 (Bos. Consulting Grp., 2020).
81 Michal Wloski & Michael Sweeney, *What's the Difference Between First-Party and*

visiting.[82] Like first-party cookies, these "tracking cookies" can reveal information such as search terms, page views, and location data.[83] Additionally, a common practice for data-collecting entities is to place a cookie with a random identifier on a user's device to anonymously keep track of that user's data and create a more complete consumer profile across the internet over time.[84] However, since cookies can only be read by the domain that placed them, without more, a third-party cookie is not terribly valuable.[85]

To create a more detailed illustration of a user's likes, interests, beliefs, and habits, platforms engage in "cookie synching" by matching unique user identifiers, building profiles, and exchanging the information attached across DSPs, SSPs, DMPs advertisers, and publishers.[86] Additionally, platforms can match their third-party cookies with "email addresses, locations, device IDs, logins, and sometimes physical addresses," making targeting even more accurate.[87] The result is a complete user profile (usually comprised of age range, gender, location, etc.) that can be sold to advertisers and used to inform premium ad placement in real-time.[88]

Despite the ad tech industry's dependence on them, third-party cookies are nearing extinction.[89] Safari, Firefox, and most recently, Google, have all pledged to eliminate the use of third-party cookies over the coming years, leaving many in the industry worrying about the future of targeted advertising.[90] However, the Interactive Advertising Bureau (IAB), an industry group comprised of over 650 of the biggest names in digital media and advertising, predicts that the phasing out of cookies will not necessarily signal the end of targeted advertising on the web.[91] If anything, the decline of third-party tracking cookies will serve to foster innovation across the targeted advertising industry.[92]

Third-Party Cookies?, CLEARCODE, https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/#third-party-cookies (last updated July 23, 2021).

82 *How to Protect Your Privacy Online*, FED. TRADE COMM'N., https://www.consumer.ftc.gov/articles/0042-online-tracking (last updated May 2021).

83 DEIGHTON, *supra* note 9, at 11.

84 Maciej Zawadziński, *What Is Cookie Synching and How Does It Work?*, CLEARCODE, https://clearcode.cc/blog/cookie-syncing/ (last updated Nov. 25, 2020).

85 *Id.*

86 *Id.*

87 DEIGHTON, *supra* note 9, at 11.

88 *The Advantages of a Real-Time Customer Profile*, REDPOINT GLOB. (Nov. 25, 2020), https://www.redpointglobal.com/blog/the-advantages-of-a-real-time-customer-profile/.

89 *What the End of Third-Party Cookies Means for Advertisers*, DELOITTE (Feb. 12, 2020), https://www.deloittedigital.com/us/en/blog-list/2020/what-the-end-of-third-party-cookies-means-for-advertisers.html.

90 *See, e.g.*, Kateryna Sorokina, *How Third-Party Cookies Elimination Will Affect Programmatic Ecosystem*, ADTELLIGENT (Mar. 12, 2020), https://adtelligent.com/how-third-party-cookies-elimination-will-affect-programmatic-ecosystem/.

91 DEIGHTON, *supra* note 9, at 10.

92 Jeremy Hudgens, *The Great Cookie Countdown: What's Next for Advertising Without*

Google asserts that its elimination of third-party cookies will enhance user privacy.[93] However, smaller digital ad platforms are concerned this is a tactic aimed at increasing the tech giant's already firm grip on the industry by forcing smaller players to cooperate within its walled garden.[94] In a world without cookies, the IAB predicts that "ad spending [will] be diverted to a small number of very large digital publishers whose first-party relationships with consumers are so extensive that they can operate without tracking."[95] Additionally, with the majority of consumer data now being locked in the proverbial walls of the biggest players on the internet, the price of targeted advertising spots could potentially skyrocket, posing a huge problem for smaller players and stifling market entry.[96] An illustration of this is Google's "Privacy Sandbox," which among other things, imminently threatens to replace third-party cookies with application program interfaces ("APIs") that advertisers can use for "ad selection and other key features 'without allowing users' activity to be tracked across websites.'"[97] Another facet of the Privacy Sandbox's targeting function is the Federated Learning of Cohorts ("FLoC"), which collects user information directly through their browser and categorizes users into "cohorts."[98] Based on these categorizations, advertisers have the ability to select their targeted cohort, and serve content based on the group's demographics.[99] While on paper Google's efforts seem like a win for privacy advocates, many remain concerned that the Privacy Sandbox could do more harm than good.[100]

Third-Party Cookies?, FORBES (Mar. 5, 2020), https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/03/05/the-great-cookie-countdown-whats-next-for-advertising-without-third-party-cookies/.

93 David Temkin, *Charting a Course Towards a More Privacy-First Web*, GOOGLE (Mar. 03, 2021), https://blog.google/products/ads-commerce/a-more-privacy-first-web/.

94 Pamela Bump, *The Death of the Third-Party Cookie: What Marketers Need to Know About Google's Looming Privacy Pivots*, HUBSPOT, https://blog.hubspot.com/marketing/third-party-cookie-phase-out (last updated Mar. 2021).

95 DEIGHTON, *supra* note 9, at 4.

96 Seb Joseph, *In the Absence of Third-party Cookies, Publishers Are Building Walled Gardens of Their Own*, DIGIDAY (Feb. 7, 2020), https://digiday.com/marketing/absence-third-party-cookies-publishers-building-walled-gardens/.

97 Abner Li, *Google Provides Privacy Sandbox Update, Plans Chrome Updates to Protect Credentials & Prevent Tracking*, 9TO5GOOGLE (Oct. 6, 2020), https://9to5google.com/2020/10/06/google-privacy-sandbox-update/.

98 Bennet Cyphers, *Google Is Testing Its Controversial New Ad Targeting Tech in Millions of Browsers. Here's What We Know*., ELEC. FRONTIER FOUND. (Mar. 30, 2021) https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres.

99 *Id.*

100 Mark MacCarthy, *Controversy Over Google's Privacy Sandbox Shows Need for an Industry Regulator*, BROOKINGS (June 23, 2021), https://www.brookings.edu/blog/techtank/2021/06/23/controversy-over-googles-privacy-sandbox-shows-need-for-an-industry-regulator; Cyphers, *supra* note 98.

2. Browser Fingerprinting and Mobile Ad IDs

A less-commonly known tool of the ad tech industry is browser fingerprinting—"a tracking technique capable of identifying individual users based on their browser and device settings."[101] Sometimes referred to as probabilistic IDs, this method can also be used on mobile devices.[102] To identify a user's "fingerprint," platforms look to elements such as language preferences, operating system, time zone, screen size, settings and device model.[103] Analyzing this unique combination, platforms can identify and track users across the web with 99% accuracy without the use of a cookie.[104] Browser fingerprinting is unique in that it gives users very little ability to opt-out.[105] Unlike cookies, which can be blocked or limited through browser settings, users cannot eliminate their browser fingerprint without completely overhauling their computer settings on a regular basis.[106] The seemingly sinister nature of the browser fingerprint means that, "even if you were to employ multiple recommended privacy precautions (such as masking your IP address through a VPN and deleting or blocking cookies), trackers can still use your digital fingerprint to re-identify and re-cookie your device when you visit a website."[107] Due to the negative public image associated with fingerprinting practices, many browsers including Google and Firefox employ methods that render this practice incompatible with their services.[108]

On mobile devices, third-party cookies are limited.[109] Instead, platforms largely access and track user data through Mobile Advertising IDs (MAIDs).[110]

---

101 Kessler, *supra* note 28.

102 *Mobile Identity Guide for Marketers*, INTERACTIVE ADVERT. BUREAU 7, https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf (last visited Nov. 8, 2021).

103 Nick Briz & Clayton D'Arnault, *This Is Your Digital Fingerprint*, THE DISCONNECT (2018), https://thedisconnect.co/two/your-digital-fingerprint/.

104 *Id.*

105 Shanthi S, *Digital Marketers Worry About Google's 'Walled Garden' After Third-Party Cookies Ban*, INC42 (Jan. 24, 2020), https://inc42.com/features/digital-marketers-worry-about-googles-walled-garden-after-third-party-cookies-ban/.

106 *Id.*; *see also* Rachel Kraus, *Google's New Cookies Tools Will Protect Privacy – and Ensure Its Dominance*, MASHABLE (May 8, 2019), https://mashable.com/article/google-chrome-cookies-privacy-changes/ ("Chrome is also tackling the rise of fingerprinting, which it describes as 'underground . . . harder-to-detect methods that subvert cookie controls.'").

107 Briz, *supra* note 103.

108 Frederic Lardinois, *Google Proposes New Privacy and Anti-Fingerprinting Controls for the Web*, TECHCRUNCH (Aug. 22, 2019), https://techcrunch.com/2019/08/22/google-proposes-new-privacy-and-anti-fingerprinting-controls-for-the-web/; Kessler, *supra* note 28.

109 *See generally* Shruti Lele, *Cookies in Mobile: Do They Exist?*, SOC. MEDIA TODAY (Dec. 18, 2014), https://www.socialmediatoday.com/content/cookies-mobile-do-they-exist.

110 DEIGHTON, *supra* note 9, at 10.

MAIDs are anonymous, persistent identifiers comprised of unique strings of numbers set by the devices operating system that can be used to track users across multiple applications.[111] MAIDs are especially useful to advertisers targeting users across multiple computers and mobile devices.[112] The biggest players in the operating system market each have their own unique version of MAIDs: Apple's "Identifier for Advertising" (IDAF) and Google's "Android Advertising ID" (AAID) are the most popular.[113] This tracking information is available to all app developers on a case-by-case basis,[114] effectively supplementing for a process such as cookie synching.[115] To track users across multiple devices using MAIDs, third-party data managers look to personally identifiable information associated with the application ("deterministic" approach) or make statistically-backed inferences ("probabilistic" approach) in order to create individual consumer device graphs that are used to target consumers.[116] As compared to cookies, MAIDs are generally considered to be more privacy-friendly, as users can easily edit their location preferences and turn off mobile advertisement tracking in their device settings.[117] To that effect, in January 2021, Apple announced changes to its IDFA included in the iOS 14 software update, requiring every application to acquire user permission before sharing data with third parties.[118] Additionally, the update will provide users with a "privacy nutrition label," listing the apps that request or have access to their data, leaving ad tech companies worried about access to mobile consumer data.[119]

The collection and analysis of user data has fueled the ad tech industry's success of the past decade, allowing publishers and advertisers to reap large

---

111 *Mobile Ad ID (MAID): Advertising User Device Identification for Mobile Campaigns*, ONAUDIENCE, https://www.onaudience.com/resources/mobile-ad-id-user-identification-for-mobile-ad-campaign (last visited Sept. 14, 2021).

112 *Mobile Identity Guide for Marketers*, *supra* note 102, at 2.

113 *Id.* at 4.

114 *Id.* at 6.

115 DEIGHTON, *supra* note 9, at 14.

116 *Mobile Identity Guide for Marketers*, *supra* note 102, at 6–7.

117 Kim Komando, *How to Stop Your Smartphone from Tracking Your Every Move, Sharing Data and Sending Ads*, USA TODAY, https://www.usatoday.com/story/tech/columnist/komando/2019/02/14/your-smartphone-tracking-you-how-stop-sharing-data-ads/2839642002/ (last updated Mar. 7, 2019).

118 Dean Takahashi, *Apple Spells Out How Soon Its IDFA Privacy Changes Will Take Effect*, VENTUREBEAT (Jan. 27, 2021), https://venturebeat.com/2021/01/27/apple-spells-out-how-soon-its-idfa-privacy-changes-will-take-effect/.

119 *Id.*; *But see* Arsen Kourinian, *How Expansion of Privacy Laws, Adtech Standards Limits Third-Party Data Use for Retargeting*, IAPP (Sept. 14, 2021), https://iapp.org/news/a/how-the-expansion-of-data-privacy-laws-and-adtech-standards-limits-companies-ability-to-use-third-party-data-for-retargeting/.

financial gains.[120] However, this has also subjected consumers to violations of their personal information.[121] As consumers become increasingly aware of the potential insecurity of their personal information online, and lawmakers push to introduce comprehensive privacy legislation, the ad tech industry will be forced to reinvent its practices or risk being run out of business.[122]

II. CURRENT LEGISLATION

A. The California Consumer Privacy Act and Its Successors

The call of advocates seeking privacy reform was first answered by the California state legislature.[123] Passed on July 28, 2018, and in full effect as of January 2020, The California Consumer Privacy Act (CCPA) was the first comprehensive privacy law enacted in the United States.[124] Similar to the European Union's General Data Protection Regulation (GDPR), CCPA, "guarantee[s] strong protection for individuals regarding their personal data and appl[ies] to businesses that collect, use, or share consumer data, whether the information was obtained online or offline."[125]

The CCPA is the brainchild of Alastair MacTaggart, a wealthy San Francisco real estate developer who first became concerned about his online-privacy after a chat with a Google engineer over dinner.[126] MacTaggart, through his advocacy group "Californians for Consumer Privacy,"[127] spent over $3 million gathering more than 600,000 signatures to qualify the original version of the initiative for

---

120 Erica Sweeny, *71% of Consumers Worry About Brands' Handling of Personal Data, Study Finds*, MKTG. DIVE (May 14, 2018), https://www.marketingdive.com/news/71-of-consumers-worry-about-brands-handling-of-personal-data-study-finds/523417/.

121 Herman Li & A. Nill, *Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy?*, 43 J. CONSUMER POL'Y. 723, 725 (2020).

122 Jonathan McGruer, *Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance*, 15 WASH. J. L. TECH. & ARTS 120, 138 (2020).

123 *Id.*

124 Hannah Huerta, *California Consumer Privacy Act Overview*, PDC FLOW (Oct. 15, 2019), https://www.pdcflow.com/office-operations/california-consumer-privacy-act-overview/.

125 *Comparing Privacy Laws: GDPR v. CCPA*, ONETRUST DATAGUIDANCE & FUTURE OF PRIVACY FORUM 5 (Dec. 2019), https://fpf.org/wp-content/uploads/2019/12/ComparingPrivacyLaws_GDPR_CCPA.pdf [hereinafter ONETRUST DATAGUIDANCE & FUTURE OF PRIVACY FORUM]

126 Ben Alder, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 28, 2018), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country.

127 *Californians for Consumer Privacy Is Dedicated to Protecting and Expanding Privacy Rights for Consumers***,** CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/about-us/ (last visited Sept. 19, 2021).

the state's November 2018 election.[128] With tech companies in an obvious frenzy, MacTaggart and California lawmakers reached a "take it or leave it" deal, resulting in a "scaled back" version of the proposal that was eventually passed into law.[129] Thus, the first comprehensive privacy bill in United States history was born.[130]

Broadly, the CCPA gives consumers the right to know exactly what kind of data companies are collecting about them, restricts the sale of their personal information, and allows consumers to sue these companies if they fail to adequately protect their data.[131] In addition, it grants the State Attorney General "broad rule-making authority and the power to impose substantial penalties for violations."[132] The CCPA takes the approach that consumers have ownership interest in their personal online privacy, and establishes five general rights of Californians.[133] These rights include:

> (1) The right of Californians to know what personal information is being collected about them[;] (2) The right of Californians to know whether their personal information is sold or disclosed and to whom[;] (3) The right of Californians to say no to the sale of personal information[;] (4) The right of Californians to access their personal information[;] [and] (5) The right of Californians to equal service and price, even if they exercise their privacy rights.[134]

The CCPA applies to entities doing business in California that either have gross revenues greater than $25 million, buy, sell, receive, or share for commercial purposes the personal information of at least 50,000 consumers, households, or devices, and/or make 50% or more of annual revenue from selling user data a year.[135] The CCPA does not explicitly define "doing business in California," but based on the California Franchise Tax Board's definition,[136] it

---

128 Laura Sydell, *Do Not Sell My Personal Information: California Eyes Data Privacy Measure*, NPR (May 28, 2018), https://www.npr.org/sections/alltechconsidered/2018/05/28/614419275/do-not-sell-my-personal-information-california-eyes-data-privacy-measure.

129 Ben Alder, *'Take It or Leave It' Deal Reached in California Legislature to Avoid Fight over Internet Privacy*, CAPRADIO (June 21, 2018), https://www.capradio.org/articles/2018/06/21/take-it-or-leave-it-deal-reached-in-california-legislature-to-avoid-fight-over-internet-privacy-ballot-measure/.

130 *See generally* CAL. CIV. CODE § 1798.100 (2018) (effective until Jan. 1, 2020).

131 Alder, *supra* note 129.

132 JONES DAY, CALIFORNIA CONSUMER PRIVACY ACT GUIDE 3 (2020).

133 Mark Diamond, *Quick Overview: Understanding the California Consumer Privacy Act (CCPA)*, ASS'N OF CORP. COUNS. (July 26, 2019), https://www.acc.com/resource-library/quick-overview-understanding-california-consumer-privacy-act-ccpa.

134 CAL. CIV. CODE § 1798.120 (West 2020).

135 CAL. CIV. CODE § 1798.140(c)(1) (West 2020) (effective until Dec. 31, 2022).

136 ONETRUST DATAGUIDANCE & FUTURE OF PRIVACY FORUM, *supra* note 125, at 9

is reasonable to assume that even out-of-state entities collecting information from California citizens are subject to the CCPA's restrictions.[137] California is the most populous state in the U.S., and 77.8%[138] of its almost 40 million residents[139] regularly use the Internet. Thus, the likelihood of most, if not all, major ad tech players being subject to CCPA's jurisdiction is high.

If a business is subject to the CCPA, they are tasked with an onslaught of responsibilities.[140] Upon request, qualifying entities are required to inform inquiring consumers of any data collected about them over the previous 12 months.[141] These entities are required to provide this information within 45 days by revealing who the entity is sharing data with, and how the data is being used.[142] Additionally, businesses must provide users with the ability to delete the data collected about them, and must provide "a clear and conspicuous link on the business' internet homepage, titled 'Do Not Sell My Personal Information.'"[143] The CCPA imposes a few other key restrictions that have a direct effect on the ad tech ecosystem and the potential to change the way companies collect and monetize information.[144]

One of the most relevant implications of the CCPA is its broad definition of "personal information," which is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[145] This encompasses a broad range of user data, including, "[i]dentifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol [("IP")] address, email address, account name, social security number, driver's license number, passport number . . . ," and biometric information, geolocation data, and deidentified data that can be linked back to respective

("Doing business in California consists of 'actively engaging in any transaction for the purpose of financial or pecuniary gain or profit' and an out-of-state entity can be considered as doing business in California if it meets certain thresholds (see Section 23101 of the Revenue and Taxation Code).").

137 Christy Harris & Charlotte Kress, *Examining Industry Approaches to CCPA "Do Not Sell" Compliance*, FUTURE OF PRIV. F. (Dec. 19, 2019), https://fpf.org/2019/12/19/examining-industry-approaches-to-ccpa-do-not-sell-compliance/.

138 *Internet Access in the United States in 2019, by State*, STATISTA (Jan. 27, 2021), https://www.statista.com/statistics/184691/internet-usage-in-the-us-by-state/.

139 *QuickFacts California*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/CA.

140 Kean Graham, *How CCPA Will Pan Out and Affect the Ad Tech Industry*, MONETIZE MORE (Jan. 8, 2020), https://www.monetizemore.com/blog/ccpa-pan-out-affect-ad-tech-industry/.

141 CAL. CIV. CODE § 1798.130 (West 2020).

142 Graham, *supra* note 140.

143 CAL. CIV. CODE § 1798.135 (West 2020).

144 *See* Graham, *supra* note 140.

145 § 1798.140(o)(1).

users.[146] Personal information also notably includes any inferences from information used "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" under the CCPA.[147] For ad tech companies, this translates to basically all information traditionally used to track and target consumers.

The CCPA also sets forth a relatively broad definition of the "sale" of user data that reaches beyond monetary exchange.[148] Under the CCPA, "sale" includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."[149] While this version of interpretation is less expansive than the one MacTaggart proposed in his original ballot initiative, it still may require ad tech companies to alter, or at least reexamine, their practices.[150]

As previously noted, a large majority of the data ad tech companies use to target consumers fall under the CCPA's definition of protected "personal information."[151] Additionally, under the law, the process of sharing this information among DSPs, SSPs and ad exchangers likely constitutes a sale, even without an explicit monetary exchange.[152] Since the law's language specifies "monetary or *other valuable consideration*,"[153] it is likely the value gained through this information exchange would qualify an entity as a covered business. However, the language is ambiguous – resulting in no real answer absent meaningful litigation or regulatory guidance. Though the state Attorney General has the power to issue explanatory regulations and conduct rulemakings to guide

---

146 § 1798.140(o)(1)(A).
147 § 1798.140(o)(1)(K).
148 § 1798.140(t)(1).
149 *Id.*
150 Letter from Mary Ross & Alastair Mactaggart to the Initiative Coordinator, OFF. OF THE ATTORNEY GEN. (Nov. 17, 2017), https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf ("'Sell,' 'selling,' 'sale,' or 'sold,' means: (A) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for valuable consideration; or (B) sharing orally, in writing, or by electronic or other means, a consumer's personal information with a third party, whether for valuable consideration or for no consideration, for the third party's commercial purposes.").
151 § 1798.140(o)(1).
152 Tim Peterson, *WTF is the CCPA's Definition of Sale*, DIGIDAY (Feb. 7, 2020), https://digiday.com/marketing/wtf-ccpas-definition-sale/.
153 § 1798.140(t)(1).

the law's implementation, the topic of sale has not yet been directly addressed.[154]

Ad tech companies use and exchange data in a variety of ways, elevating the often-frustrating ambiguity of the text of the Act. For example, "[a] publisher passing a device ID to an ad tech firm to fill a programmatic ad impression or an advertiser sharing a list of IP addresses to an agency to plan a targeted ad buy could be considered a sale of data under the law. Or they could not be."[155] As private actions pursuant to the CCPA are brought to court in California and the state Attorney General issues guidance, the ambiguity regarding the definition of "sale" will likely be clarified.[156]

For ad tech companies whose business models rely on the exchange of data, the CCPA's service provider exemption contains a potential loophole.[157] Under the CCPA, a service provider is "a company that processes personal information collected by another company, but only for the purposes specified in a written contract between the companies."[158] In acquiring the title of "service provider," companies may proceed with their data sharing practices without it being considered a sale.[159] However, being a service provider comes with important limitations, namely, a prohibition on "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business."[160] This would, for example, prohibit an ad tech company designated as a service provider from using device IDs "collected by a publisher in order to serve targeted ads on the publisher's site . . . to build a device graph in order to track people across the internet."[161]

Despite its limitations, there is some consensus that the CCPA's service provider exemption seems to present a viable opportunity for companies that would otherwise be covered by the CCPA.[162] For example, in its CCPA compliance framework, the IAB requires participating downstream technology companies to function as service providers[163], creating a "simple and efficient

---

154 CAL. CODE. REGS. tit. 11, § 999.301.

155 Tim Peterson, *'We're Not Going to Play Around': Ad Industry Grapples with California's Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/.

156 Napa Valley Educators' Ass'n. v. Napa Valley Unified Sch. Dist., 329 Cal. Rptr. 395, 399 (Cal. Ct. App. 1987).

157 Tim Peterson, *WTF Is CCPA's Service Provider Designation?,* DIGIDAY (Dec. 4, 2019), https://digiday.com/marketing/wtf-ccpas-service-provider-designation/ [hereinafter *WTF Is CCPA's Service Provider Designation?*]

158 *Id.*; § 1798.140(v).

159 *WTF Is CCPA's Service Provider Designation?*, *supra* note 157.

160 § 1798.140(v).

161 *WTF Is CCPA's Service Provider Designation?*, *supra* note 157.

162 ONETRUST DATAGUIDANCE & FUTURE OF PRIVACY FORUM, *supra* note 125, at 10.

163 *WTF Is CCPA's Service Provider Designation?*, *supra* note 157.

vehicle from which to create service provider relationships in the data supply chain without the need of having to enter into hundreds of separate contracts," which in turn allows the ad tech cycle to flow without running afoul of the CCPA.[164] While the limitations associated with the label of service provider certainly hinder a company's maximum potential for profitability, for many, it is a welcome alternative to completely shutting down targeted behavioral advertising practices.[165]

Unlike the GDPR, the CCPA does not proscribe that companies obtain user consent[166] ("opt-in") before engaging in a sale of personal information to third-parties.[167] Instead, the law provides that businesses give users the option to prohibit a sale through "[t]he development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information."[168] This is facilitated through the clear and conspicuous addition of a "Do Not Sell My Personal Information" button to a company's web page.[169] In addition, businesses are prohibited from requesting the user's consent again for 12 months.[170] Advocates argue that opt-out regimes, such as this, shift too much responsibility to users, and create only the illusion of consumer privacy and choice.[171]

Even in instances where consumers exercise their rights to opt-out, there are certain ways for companies to continue using consumer data while remaining compliant with the law. Covered businesses are still free to use personal information for "business purposes"[172] within the company, in addition to third

---

164 *IAB CCPA Compliance Framework for Publishers & Technology Companies*, INTERACTIVE ADVERT. BUREAU 5 (Dec. 4, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf.

165 Peterson, *supra* note 155.

166 § 1798.120(c) ("A business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information.").

167 ONETRUST DATAGUIDANCE & FUTURE OF PRIVACY FORUM, *supra* note 125, at 23.

168 CAL. CIV. CODE § 1798.185(a)(4)(C) (West 2020).

169 § 1798.135(a)(1).

170 § 1798.135(a)(5).

171 Meaghan Donahue, *What Do State Privacy Laws Mean For The Ad Tech Industry?*, NEW AM. (Aug. 17, 2021), https://www.newamerica.org/oti/briefs/what-do-state-privacy-laws-mean-for-the-ad-tech-industry/.

172 § 1798.140(d) ("'Business purpose' means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or

party service providers.[173] This is why the service provider exemption detailed above becomes so important—operating as a service provider allows ad tech companies to "process the data collected by another company, even if a person has requested their data not be sold, so long as the service provider only uses the data for the purposes specified in a written contract with the company that collected and shared the data."[174]

At the heart of the CCPA is MacTaggart's desire to protect the interests of Californian consumers and their personal information.[175] The law recognizes that as technological capabilities have continued to advance, "there is an increase in the amount of personal information shared by consumers with businesses…" and "California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information."[176] Particularly, in the realm of digital targeted advertising, the CCPA was the first step in holding ad tech companies accountable for the actions they take with regard to user data.[177]

1. Consumer Privacy Rights Act – CCPA 2.0?

MacTaggart and Californians for Consumer Privacy were back at it again in 2020, only months after CCPA officially went into effect.[178] Their new ballot initiative – the Consumer Privacy Rights Act (CPRA) – was voted into law on November 3, 2020 and expands upon CCPA's basic premise.[179] MacTaggart emphasized the need to amend the CCPA, asserting

> [w]e've laid a historic foundation for consumer rights in California with the passage of the California Consumer Privacy Act, and now it's time to seize that momentum and take the next step in enforcing and expanding the law to keep pace with an industry that is changing at a break-neck pace.[180]

---

processed or for another operational purpose that is compatible with the context in which the personal information was collected.").

173 § 1798.140(2)(a).

174 Peterson, *supra* note 155.

175 Diamond, *supra* note 133.

176 California Consumer Privacy Act of 2018, Assemb. B. 375 (Cal. 2018) (codified § 1798.100).

177 Fredrick Lee, *CCPA Won't be Enough to Fix Tech's Data Entitlement Problem*, TECH CRUNCH (Feb. 7, 2020), https://techcrunch.com/2020/02/07/ccpa-wont-be-enough-to-fix-techs-data-entitlement-problem/.

178 Brandon P. Reilly & Scott T. Lashway, *The California Privacy Rights Act Has Passed: What's in It?*, MANATT (Nov. 11, 2020), https://www.manatt.com/insights/newsletters/client-alert/the-california-privacy-rights-act-has-passed.

179 *Id.*

180 Brian H. Lam, *The Next Act for the Architect of the California Consumer Privacy Act: The California Privacy Rights Act*, NAT'L L. REV. (Jan. 30, 2020),

The CPRA echoes this sentiment – "Rather than diluting privacy rights, California should strengthen them over time."[181]

The changes brought about by CPRA will have tangible implications on the ad tech ecosystem when it goes into effect in January of 2023.[182] Most notably, the CPRA will require new criteria for the regulation of businesses, expanding the threshold consumer requirement from 50,000 to 100,000 and including a broader definition of "sale" that includes the sharing of personal information.[183] It will also include an additional category subject to heightened limitations and requirements for sensitive personal information,[184] new consumer rights such as the right to opt-out of allowing personal information to be used for "automated decision making" such as "profiling," [185] and create the California Privacy Protection Agency.[186]

2. Following California's Lead – Virginia, Colorado, and Other Privacy Law Hopefuls

The CCPA represents the first, and most expansive comprehensive privacy law in American governmental history.[187] However, it will certainly not be the last. Other states such as New York, Washington, and others have used the CCPA as a blueprint to guide the development of their own state-level privacy laws.[188] In October of 2020, the New York State Legislature introduced the "It's Your Data Act" ("IYDA"), which, among other things, aims to expand the State

---

https://www.natlawreview.com/article/next-act-architect-california-consumer-privacy-act-california-privacy-rights-act.

181 *How Prop 24 Embraces and Extends the California Consumer Privacy Act*, CAL. FOR CONSUMER PRIV. (Aug. 23, 2020), https://www.caprivacy.org/how-prop-24-embraces-and-extends-the-california-consumer-privacy-act/.

182 Reilly, *supra* note 178.

183 *Id*.

184 § 1798.140.

185 Alysa Zeltzer Hutnik & Aaron Burnstein, *It's Here: California Voters Approve the CPRA*, AD L. ACCESS (Nov. 4, 2020), https://www.adlawaccess.com/2020/11/articles/its-here-california-voters-approve-the-cpra/ ("Consumers also have a right to opt out of the use of their personal information for automated decision making, which includes 'profiling' in connection with evaluations or decisions about to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. The consumer also has a right to access 'meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.'").

186 CAL. CIV. CODE § 1798.199.40 (West 2020).

187 PRACTICAL LAW DATA PRIVACY ADVISOR, UNDERSTANDING THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA), Note w-017-4166 (West 2021).

188 Jedidiah Bracy, *With the CCPA Now in Effect, Will Other States Follow?*, IAPP (Jan. 2, 2020), https://iapp.org/news/a/with-the-ccpa-now-in-effect-will-other-states-follow/.

constitution's current "right to privacy" and establish consumer rights and business requirements similar to those mandated by the CCPA.[189] Similarly, Washington State tried, and failed, to pass the 2021 Washington Privacy Act ("WaPA"), the state's third attempt at a comprehensive privacy law.[190] WaPA mirrored key components of the CCPA, but added unique provisions devoted to data privacy in public health emergencies – a direct response to the COVID-19 pandemic and the rise of automatic contact tracing technologies.[191] If eventually passed, the WaPA promises to provide Washingtonians with the privacy protection that so many residents have come to expect in their online dealings.[192]

On March 2, 2021, Virginia successfully passed a comprehensive privacy legislation when Governor Ralph Northam signed the VCDPA into law.[193] Echoing key provisions of the CCPA and CPRA, the VCDPA goes a step further with regards to the rights of consumers, providing that controllers must acquire opt-in user consent before processing "sensitive data."[194] However, unlike its fellow state comprehensive privacy laws, the VCDPA does not provide for a private right of action.[195] Most recently, in July, 2021, Colorado became the third state to pass a privacy law of its own – the Colorado Privacy Act ("CPA").[196] Similar to the VCDPA, CPA has no private right of action and also requires covered entities to submit data protection assessments detailing the way sensitive consumer information is handled.[197]

Federal legislators have even gotten in on the action. In July 2021, a cohort

---

189 Heather McArn ET AL., *Is New York's New Consumer Privacy Bill a Bridge Too Far?*, JDSUPRA (Nov. 3, 2020), https://www.jdsupra.com/legalnews/is-new-york-s-new-consumer-privacy-bill-31380/.

190 Cathy Cosgrove, *The Washington Privacy Act Is Back*, IAPP (Sept. 23, 2020), https://iapp.org/news/a/the-washington-privacy-act-is-back/; Khari Johnson, *Washington Privacy Act Fails Again, But State Legislature Passes Facial Recognition Regulation*, VENTURE BEAT (Mar. 12, 2020), https://venturebeat.com/2020/03/12/washington-privacy-act-fails-in-state-legislature-again/.

191 Cosgrove, *supra* note 190.

192 Mitchell Noordyke, *Comparing the New Washington Privacy Act to the CCPA*, IAPP (Jan. 21, 2020), https://iapp.org/news/a/comparing-the-new-washington-privacy-act-to-the-ccpa/.

193 *Virginia Passes Comprehensive Privacy Law*, GIBSON DUNN (Mar. 8, 2021), https://www.gibsondunn.com/virginia-passes-comprehensive-privacy-law/.

194 Virginia Consumer Data Protection Act, S. 1392, spec. sess. (Va. 2021) (enacted) ("'Sensitive data' means a category of personal data that includes: 1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; 3. The personal data collected from a known child; or 4. Precise geolocation data.").

195 *Id.*

196 Christopher T. Patrick, *Colorado Becomes Third State to Enact a Comprehensive Privacy Law*, NAT'L L. REV. (July 9, 2021), https://www.natlawreview.com/article/colorado-becomes-third-state-to-enact-comprehensive-privacy-law.

197 COLO. REV. STAT. §§ 6-1-1309—6-1-1310 (2021) (effective Jan. 1, 2023).

of Republican Senators reintroduced the "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act'', more simply known as the SAFE DATA Act.[198] The SAFE DATA Act would establish consumer "data rights," which requires businesses to provide users the ability to access and edit their data, prohibits the transfer of consumer data without consent, and implements data privacy and data security officer positions.[199] Additionally, the Act promises to establish a victim relief fund through the Treasury Department in order to provide injured consumers with compensation.[200] The Act would preempt current state laws and does provide a private right of action.[201] The notion of federal preemption is controversial in its own right and while not particularly impactful on the practices of ad tech companies, could change the ways consumers redress their injuries when companies violate their privacy rights.

In addition to the SAFE DATA Act, Democrats have introduced bills of their own – including the Consumer Online Privacy Act of 2019 (Cantwell, D-WA),[202] the Online Privacy Act of 2019 (Eshoo, D-CA),[203] the Data Accountability and Transparency Act of 2020 (Brown, D-OH),[204] and the Privacy Bill of Rights Act (Markey, D-MA).[205] As opposed to the Republican backed bill, these proposals provide citizens a private right of action, similar to the one provided in CCPA.[206] While passing federal comprehensive privacy legislation is a top priority of law makers on both sides of the aisle, it seems unlikely there will be consensus any time soon. Until then, consumers must rely on their individual states to pass regulations.[207]

B. CCPA Litigation

CCPA is barely a year old, but there have already been multiple actions brought, many alleging the data collection practices companies use to target

---

198 SAFE DATA Act, S. 4626, 116th Cong. (2020).

199 Rebecca Kern, *Key Republicans Release Privacy Bill Focused on Transparency*, BLOOMBERG GOV'T (Sept. 17, 2020), https://about.bgov.com/news/key-republicans-release-privacy-bill-focused-on-transparency/; S. 4626.

200 S. 4626.

201 Kern, *supra* note 199.

202 Consumer Online Privacy Act of 2019, S. 2968, 116th Cong. (2019).

203 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019).

204 Data Accountability and Transparency Act of 2020, H.R. 6675, 116th Cong. (2020).

205 Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

206 *See* S. 4626.

207 Graham Dean & Ronald Raether, *U.S. Senators Reintroduce Privacy Legislation*, JDSUPRA (Aug. 31, 2021), https://www.jdsupra.com/legalnews/u-s-senators-reintroduce-privacy-4527842/.

consumers with ad content is in violation of the law.[208] Section 1798.150(a)(1) provides a private right of action for

> Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information . . . .[209]

Under this provision of the CCPA, consumers can recover up to $750 per incident, be granted injunctive declaratory relief, or recover based on other forms of relief at the discretion of the trial court.[210] According to a summary of enforcement actions published by the Attorney General's office, the most common violations have to do with non-compliant privacy policies, inadequate opt-out procedures, and lack of CCPA request methods.[211]

In *Sweeney v. Life on Air, Inc*., the plaintiff alleged the social networking application Houseparty failed to inform consumers that the app was sharing the personally identifiable information of users with third parties, including Facebook, without authorization. [212] In her complaint, the plaintiff asserts that "upon downloading and opening the app, Defendant's would send customer information and analytics to Facebook's software development kits ("SDK") . . . ," even though the Defendant explicitly promised the opposite.[213] The complaint alleges Houseparty violated the CCPA by failing to notify the Plaintiff about the sale of her data, failing to provide her with the ability to opt-out of the sale, failing to provide a clear and conspicuous "Do Not Sell My Information" link, and failing to use the personal information collected to keep her personal information private.[214] The case was sent to arbitration in August 2020.[215]

In *Henry v. Zoom*, the plaintiff's complaint alleges Zoom shares data such as device model, location, phone carrier and advertising ID with Facebook without

---

208 *See generally* Complaint at 7, Sweeney v. Life on Air, Inc., No. 3:20-cv-00742 (S.D. Cal. 2020) [hereinafter *Sweeney* Complaint]; Complaint at 3, Henry v. Zoom, No. 5:20-cv-02691-SVK (N.D. Cal. May 4, 2020) [hereinafter *Henry* Complaint]; Complaint at 10, G.R. v. TikTok, Inc., No. 2:20-cv-04537 (S.D. Cal. 2020) [hereinafter *G.R.* Complaint].

209 CAL. CIV. CODE § 1798.150(a)(1) (West 2020) (effective Jan. 1, 2023).

210 *Id.*

211 *California Attorney General Issues Summary of CCPA Enforcement Actions and Launches Consumer Privacy Interactive Tool*, HUNTON ANDREWS KURTH (July 23, 2021), https://www.huntonprivacyblog.com/2021/07/23/california-attorney-general-issues-summary-of-ccpa-enforcement-actions-and-launches-consumer-privacy-interactive-tool/.

212 *Sweeney* Complaint, *supra* note 210, at 7.

213 *Id.*

214 *Id.* at 21–22.

215 Docket, *Sweeney*, No. 3:20-CV-00742.

consumer consent.[216] This unauthorized data sharing is not noted in Zoom's privacy policy.[217] The complaint asserts that Zoom violated the CCPA by using customer information without providing notice, failing to provide customers with the ability to opt-out of the disclosure of their data, and failing to protect user information from a potential data breach.[218]

In *G.R. v. TikTok,* the plaintiff, a minor, alleges TikTok collected and stored biometric identifiers using the applications "proprietary facial recognition technology" which analyzes data such as facial contours and creating templates from this information without informing consumers.[219] The complaint asserts TikTok violated the CCPA by collecting and storing biometric information without notice, failing to inform consumers their biometric information was being shared with unauthorized third-parties (i.e. Facebook), and failing to provide users the ability to opt-out.[220]

As illustrated by the examples of current litigation, proper notice and ability to opt-out are common issues companies have encountered in the early days of CCPA enforcement, suggesting an area to focus improvement.[221] However, there remains much uncertainty surrounding how exactly the ad tech industry will be changed by CCPA enforcement. As Californians continue to invoke the rights concerning their personal data granted to them by CCPA, the limits of the law will become clearer. In turn, the ad tech industry should look to the outcome of litigation and the interpretation of the courts to influence their policies.

III. LOOKING AHEAD – THE FATE OF TARGETED ADVERTISING CONSIDERING COMPREHENSIVE PRIVACY LEGISLATION AND THE DEATH OF THIRD-PARTY COOKIES

Modern consumers have come to expect privacy in their online dealings. A 2018 study found that 91% of respondents believed they had lost control of their personal information on the internet, another 80% were concerned with the way their online information is used by advertisers, and 64% were in favor of more government regulation.[222] As the United States becomes a more digitally literate

---

216 *Henry* Complaint, *supra* note 210, at 3.
217 *Id.*
218 *Id.* at 17.
219 *G.R.* Complaint, *supra* note 210, at 4.
220 *Id.* at 10.
221 *See Sweeney* Complaint, *supra* note 210, at 21; *Henry* Complaint, *supra* note 210, at 17; *G.R.* Complaint, *supra* note 210, at 4.
222 Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, FACT TANK (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/.

society, comprehensive privacy reform becomes more widely adopted, and the largest search engines phase out third-party cookies, ad tech companies will need to adjust their data collection practices and business strategies in order to retain consumer trust and remain complaint with the law.[223]

A. Walled Gardens Are Getting Bigger and More Powerful

Despite the broad distrust of Big Tech and challenges from regulatory agencies, Google, Facebook, and Amazon's walled gardens constitute almost 70% of digital advertising spending in the United States.[224] The firm grip on the digital advertising market enjoyed by the biggest names in technology is strengthening every year.[225] This is demonstrated by the fact that the "non-walled garden" share of the ad tech industry has declined by $1 billion every year since 2016 and is only expected to continue shrinking in the years ahead.[226]

Unsurprisingly, the walled gardens themselves paint a narrative that casts their practices as consumer friendly and privacy law compliant.[227] In promoting its Privacy Sandbox, Google emphasizes its "privacy-first" alternatives to third-party cookies, and the potential benefits this affords consumers and advertisers alike.[228] Essential to the Privacy Sandbox, as previously noted, is the FLoC, which facilitates digital advertising based on interests of "cohorts" and is reportedly equally as effective as traditional third-party cookies.[229] To provide advertisers with the ability to create and target their own audiences, Privacy Sandbox's "First Locally-Executed Decision over Groups Experiment" ("FLEDGE") program makes auction decisions without the use of an ad server, allowing marketers the ability to measure efforts and retarget users in a

---

223 Shanthi, *supra* note 105; *see also* Kraus, *supra* note 106 ("Chrome is also tackling the rise of fingerprinting, which it describes as 'underground . . . harder-to-detect methods that subvert cookie controls.'").

224 Greg Sterling, *Almost 70% of Digital Ad Spending Going to Google, Facebook, Amazon, Says Analyst Firm*, MARTECH (June 17, 2019), https://martech.org/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm/.

225 Allison Schiff, *The Walled Gardens Are Eating Open Programmatic – Here's How They're Doing It*, AD EXCHANGER (May 17, 2019), https://www.adexchanger.com /platforms/the-walled-gardens-are-eating-open-programmatic-heres-how-they-do-it/.

226 *Id.*

227 Chetna Bindra, *Building a Privacy-First Future for Web Advertising*, GOOGLE (Jan. 25, 2021), https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/; Smith, *supra* note 68.

228 Bindra, *supra* note 227.

229 Grace Dillon, *Google Looks to FLoC for Post-Cookie Targeting; IPA Bellwether Forecasts Eventual Recovery*, EXCH.WIRE (Jan. 26, 2021), https://www.exchangewire.com /blog/2021/01/26/google-looks-to-floc-for-post-cookie-targeting-ipa-bellwether-forecasts-eventual-recovery/. *See supra* note 100 and accompanying text.

seemingly privacy conscious manner.[230]

Privacy and consumer rights advocates have remained critical of the Privacy Sandbox, arguing that the elimination of the third-party cookie is more about Google's profit margins than about consumer privacy.[231] This is evidenced by the multiple anti-trust suits brought against Google, including one alleging the elimination of third-party cookies amounts to exclusionary action.[232] Additionally, while facially compliant with privacy laws, experts suggest that Google's FLoC system actually puts user information at risk by essentially developing a "behavioral credit score" that assigns users to multiple cohorts based on a range attitudes, tendencies, and beliefs.[233] The Electronic Frontier Foundation argues this is dangerous, and may allow "[d]iscriminatory advertisers … to identify and filter out [cohorts] which represent vulnerable populations."[234] Considering the sensitive nature of the information used by Google to assign users to cohorts, there is no real guarantee that this information is secure, or what kind of data your cohort assignment reveals about you.[235] In short, walled gardens like the Sandbox are not all that they seem and may pose serious threats to innovation and meaningful consumer choice.[236] Privacy advocates warn, "[t]oday, trackers follow you around the web, skulking in the digital shadows in order to guess at what kind of person you might be. In Google's future, they will sit back, relax, and let your browser do the work for them."[237]

---

230 Dillon, *supra* note 229; Kate Kaye, *WTF Is FLEDGE*, DIGIDAY (Jan. 27, 2021), https://digiday.com/media/wtf-is-fledge/.

231 Bennet Cyphers, *Don't Play in Google's Privacy Sandbox*, ELEC. FRONTIER FOUND. (Aug. 30, 2019), https://www.eff.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1 [hereinafter *Don't Play in Google's Privacy Sandbox*].

232 Kate Kaye, *Why Google's Approach to Replacing the Cookie Is Drawing Antitrust Scrutiny*, DIGIDAY (Feb. 2, 2021) [hereinafter *Why Google's Approach to Replacing the Cookie Is Drawing Antitrust Scrutiny*], https://digiday.com/media/why-googles-approach-to-replacing-the-cookie-is-drawing-antitrust-scrutiny/ ("Under pressure from governments and consumers over data privacy infringement concerns, Google a year ago said it will disable third-party cookies by 2022 in its Chrome browser, which is used by more than 60% of the world's web users."); *Don't Play in Google's Privacy Sandbox*, *supra* note 231; Complaint at 5, Sterling Int'l Consulting Grp. v. Google, LLC, No. 20-CV-9321 (N.D. CA 2020).

233 *Don't Play in Google's Privacy Sandbox*, *supra* note 231; *Why Google's Approach to Replacing the Cookie Is Drawing Antitrust Scrutiny*, *supra* note 232.

234 *Don't Play in Google's Privacy Sandbox*, *supra* note 231.

235 *Id.*; *Why Google's Approach to Replacing the Cookie Is Drawing Antitrust Scrutiny*, *supra* note 232.

236 Meg Grasmick, *Do Walled Gardens Serve Us?*, MEDIUM (Mar. 29, 2020), https://medium.com/trapica/do-walled-gardens-serve-us-5d55ecec30e2.

237 *Don't Play in Google's Privacy Sandbox*, *supra* note 231.

B. What Options Does This Leave for Digital Advertisers Moving Forward? – Renewed Interest in Contextual Advertising and First-Party Data

While more and more of the ad tech market power moves to the hands of the few, and the implementation of comprehensive privacy legislation threatens the current methods of targeted digital advertising, there are still some options that may allow smaller players to survive independent of tracking or third-party data.[238]

One potential solution involves combining good old fashioned contextual advertising with the power of machine learning.[239] Pre-internet contextual advertising traditionally involved placing ads based on webpage content as described earlier in this article.[240] Thanks to the highly evolved artificial intelligence and machine learning technologies, publishers now have the ability to "discern web page sentiment, understand the nuance of language, ascertain the content and tone of images and video, [and] automatically configure ad creative to complement context," allowing them to place contextually targeted advertisements in a quick, efficient, and privacy conscious manner.[241] Targeted contextual digital advertising completely relies on the content of the webpage, while the identity and tendencies of the user remains anonymous, making this a great privacy-preserving option that is favored by industry and consumers.[242] For example, AT&T-owned Xandr utilizes artificial intelligence to analyze "signals from a brand's audience to find patterns in page contexts that are driving high-quality engagement," and then applies "these patterns in real-time to find new audiences who are likely to be similarly receptive to a brand message."[243] Xandr refers to this practice as a "bottom-of-the-funnel-up approach" to pairing users and content and asserts it has allowed the company to successfully broaden the reach of advertising content without compromising user privacy. [244]As a result of the efforts of Xandr and others, the global digital contextual advertising market is expected to grow to $279.2 billion by 2025.[245]

---

238 *Why AI Means the Return of Contextual Targeting*, WARC (Feb. 18, 2020), https://www.warc.com/newsandopinion/news/why-ai-means-the-return-of-contextual-targeting/43241.

239 *Id.*

240 *See infra* Section II.b.

241 *Why AI Means the Return of Contextual Targeting*, *supra* note 238.

242 *Why Contextual Targeting in Advertising Is the Next Big Thing – Again*, BANNERFLOW, https://www.bannerflow.com/blog/contextual-targeting/ (last visited Nov. 19, 2021).

243 Lindsay Rowntree, *3 Ways Collaborating Will Shape the Future of Advertising*, EXCH. WIRE (Dec. 20, 2019), https://www.exchangewire.com/blog/2019/12/20/3-ways-collaboration-shape-future-advertising/.

244 *Id.*

245 Len Ostroff, *Privacy Changes Are Ushering in a New Era of Adtech Collaboration*, DIGIDAY, https://digiday.com/sponsored/privacy-changes-are-ushering-in-a-new-era-of-

Another viable route for digital advertisers involves utilizing their first-party data – the "holy grail" of the internet's cookie-less future.[246] The looming importance of first-party data is evidenced in a report published by World Federation of Advertisers (WFA), asserting that 80% of its members consider it to be "critical" for their future targeting practices.[247] First-party cookies, as explained in Section II-c., collect data such as basic demographics, languages, computer settings, number of clicks and broad geographic location.[248] Publishers can use this information to create data sets that foster meaningful ad placement without the use of the intrusive and dwindling third-party cookies.[249] In fact, publishers report that advertisers regularly inquire about the use of first-party data, and suggest these agreements are often more lucrative and lead to higher-paying advertising agreements.[250] As a result, companies like Vox Media, SHE Media, and other major players in the digital advertising space have invested in ramping up their first-party data sets by utilizing polls, surveys, and other forms of audience research, in addition to analyzing more contextual data such as "what's on the page, where did the user come from, what is the ad creative, what time of day it is, [and] where are they based . . . ."[251]

IV. RECOMMENDATIONS

In the next decade, the ad tech industry will transform into an entity unrecognizable from its current state. From the death of the third-party cookie to the rise of walled gardens and the trend toward adopting comprehensive privacy legislation, publishers and advertisers will need to change their practices

---

adtech-collaboration/ (last visited Nov. 19, 2021).

246 Karuna Sharma, *How Will Google's New Privacy Policy Impact Digital Advertising*, BUSINESS INSIDER (Mar. 5, 2021), https://www.businessinsider.in/advertising/ad-tech/article/how-will-googles-new-privacy-policy-impact-digital-advertising/articleshow/81332416.cms.

247 Georgia Brammer, *Collaboration Is Key to Moving Beyond the Cookie in 2021*, MKTG. (Dec.14, 2020), https://www.marketingmag.com.au/hubs-c/collaboration-is-key-to-moving-beyond-the-cookie-in-2021/; *First-Party Data a Key Concern for Brands, WFA Programmatic Survey Finds*, WARC (August. 20, 2020), https://www.warc.com/newsandopinion/news/first-party-data-a-key-concern-for-brands-wfa-programmatic-survey-finds/43995.

248 *See supra* Section II.c.ii.

249 Tim Peterson*, 'Table Stakes': Why publishers' First-party Data Has Become Prerequisite to Programmatic Ad Sales*, DIGIDAY (Dec. 7, 2020), https://digiday.com/media/publishers-first-party-data-has-become-prerequisite-to-programmatic-ad-sales/.

250 *Id.* ("Not only are advertisers more frequently asking about deal options involving publishers' first-party data, but publishers are finding the deals employing those options are likely to be more lucrative.").

251 *Id.*

and adopt new ways of thinking about digital advertising. The ad tech ecosystem of the future will be one in which publishers and advertisers operating independently of walled gardens will need to work together, prioritize transparency, and place consumer privacy at the center of their business models.

A. Collaboration

Particularly for companies that aim to make use of their first-party data, collaboration will be the key to success. By working together with other members of the ad tech ecosystem, publishers will be able to refine their first-party data sets, and deliver high-quality advertising space that is relevant to consumers and respectful of privacy.[252] Many companies have already begun successfully combining resources in this manner, including Nine and Adobe's "Audience Match" collaboration.[253] By combining Nine's customer data with Adobe's data management platform, Adobe Audience Manager, Audience Match provides Australian digital marketers with the capability to leverage Nine's first-party data in buying digital advertising space.[254] The program works by "matich[ing] hashed email addresses from an advertiser's data with Nine's audience data, creating a fully-addressable audience that's not dependent on cookies with every ad impression linked back to an actual person."[255] By employing a method such as this, ad tech companies can retain the ability to provide relevant ad placements, while prospering in a strictly regulated ecosystem without third-party cookies.

B. Transparency

Ad tech companies will also need to prioritize transparency in their business dealings within the ecosystem in order to retain consumer and client trust. By prioritizing "total visibility" in the buying, selling, and placement process, "buyers can make informed purchase decisions, and advertisers can optimize their spending and ad delivery."[256] In 2018, the IAB Technology Laboratory (the "IAB") released its "Data Transparency Label" to further promote openness in

---

252 Brammer, *supra* note 247.

253 *Id.*

254 *Nine Upfront 2021: Nine Partners with Adobe to Offer People-Based Marketing with Audience Match*, MEDIAWEEK (Sept. 6, 2020), https://www.mediaweek.com.au/nine-announces-audience-match/.

255 *Id.*

256 Vishveshwar Jatain, *Programmatic Transparency and the Future of AdTech*, ADAGE (June 23, 2020), https://adage.com/article/industry-insights/programmatic-transparency-and-future-adtech/2263341.

the industry.[257] The standards were developed to "help reputable marketers, fundraisers and agencies better leverage data in a responsible manner, to enable the delivery of increasingly-relevant messages to consumers and donors and to improve the overall consumer experience with content and advertising . . ." and are meant to function like a "nutrition label" for the advertising technology industry.[258] The standards consist of four sections including: 1) data solution provider and distributor information, 2) an audience snapshot, 3) audience construction, and 4) source information, which was designed to inform market participants who are purchasing data about the set's "ingredients."[259] The IAB hopes that their Data Transparency Label will help to foster responsible data use while improving consumer experience and acting as "a driving force that improves data integrity, data quality, and the decisions that marketers and fundraisers make every day."[260]

C. Balancing the Standard of Service Provided by Targeting with the Privacy Consumers Deserve

At the center of the ad tech ecosystem is, of course, the consumer. While 67% of consumers feel they have little control of their data, many appreciate the personalized experience they receive thanks to advertising technology and recognize that data sharing as a "necessary evil."[261] Studies done by multiple advertising trade associations found that 70% of survey respondents "yearn for personalized ads," and 71% "were frustrated that their shopping experiences were too impersonal."[262]

Due to the industry's reliance on consumers, ad tech companies need to prioritize balancing consumer privacy, while continuing to provide the personalized experience many have come to expect. A 2020 report published by PricewaterhouseCoopers revealed that 84% of respondents would "take their business elsewhere if they don't trust how a company is handling their data . .

---

257 Press Release, IAB Tech. Lab., *Major Advertising Trade Bodies Unveil Data Transparency Label* (Oct. 1, 2018), https://iabtechlab.com/press-releases/major-advertising-trade-bodies-unveil-data-transparency-label/.

258 *Id.*

259 *Id.*

260 *Id.*

261 N.F. Mendoza, *Data Privacy: What Consumers Want Businesses to Know*, TECH REPUBLIC (Feb. 19, 2020), https://www.techrepublic.com/article/data-privacy-what-consumers-want-businesses-to-know/; *See* Ross Benes, *Do People Actually Want Personalized Ads?*, INSIDER INTELLIGENCE (Mar. 4, 2019), https://www.emarketer.com/content/do-people-actually-want-personalized-ads.

262 Benes, *supra* note 261.

."[263] Especially in light of the predicted reliance on first-party cookie data, and the fact that consumers have seemingly limitless options to choose from in determining which websites and platforms to frequent, consumer trust "is best viewed as a common resource that online entities work simultaneously to use and to preserve."[264] If companies fail to earn and maintain this trust, consumers will take their business elsewhere, or stop sharing personal information on the internet all together.[265] Therefore, in order to be successful in the near future, prioritizing transparency and promoting consumer trust will be essential for ad tech companies to keep consumers, buyers, and sellers happy and engaged.[266]

V. CONCLUSION

Don't count on digital advertising disappearing from the web any time soon. As technology continues to advance, and more people become reliant on the internet for work and school in the years following the COVID-19 pandemic, the online advertising industry will likely be worth more than ever. However, the way advertisers and publishers collect and utilize personal data will certainly being to change in major ways. As states, and potentially the federal government, follow the lead of California, Virginia, and Colorado and enact comprehensive privacy legislation, ad tech companies will need to adjust their practices in order to remain compliant with the laws of various jurisdictions. In a similar vein, as the biggest players on the internet close their proverbial walls to broader ad tech ecosystem, smaller advertisers and publishers will need to get creative, and employ practices such as utilizing first-party data, artificial intelligence, and industry collaboration. Above all, in the next decade, ad tech companies large and small will need to mindfully balance privacy concerns and consumer trust, while retaining the standard of service users have come to expect from targeted advertising. By incorporating changes such as the ones suggested in this article and by the technology industry broadly, ad tech will live on, even if its current practices do not.

---

263 Mendoza, *supra* note 261.

264 Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95, 98 (2019).

265 *Id.*

266 Mendoza, *supra* note 261.