MERCATUS CENTER
George Mason University

POLICY BRIEF

Privacy Policy and the Future of the Online Economy: How Changes in Policy May Affect Digital Advertising and the Market for Online Services

Tracy Miller

May 2023

INTRODUCTION

Personal data play a critical role in the digital economy, providing information that is used for online advertising, which is the primary source of revenue for many online service providers. The importance of government policy on privacy of online consumers' data has increased correspondingly, sparking debate in state and federal legislative bodies and attracting the attention of regulatory agencies, particularly the Federal Trade Commission (FTC). In 2022, Congress voted an important piece of privacy legislation, the American Data Privacy and Protection Act, out of committee, but the act failed to move further. Congress may again consider federal privacy legislation this year.

In the coming years, privacy policy and the online economy will have different features depending on whether federal legislation is passed and whether that legislation preempts existing state laws. Existing and proposed privacy legislation, along with public opinion, has also influenced decisions of major tech platforms, such as Apple and Google, to change their privacy policies. What kinds of changes in the digital economy are expected as online firms and website users adjust their practices in response to recently enacted or proposed legislation, FTC regulation changes, and tech companies' changes in policies and practices in response to regulation and pressure to satisfy privacy proponents?

Many goods and services available online are funded largely or exclusively by revenues earned from digital advertising. The digital advertising ecosystem relies largely on data that is collected from users of online services and used to decide what to advertise to each user. To the extent that

online service providers' ability to collect personal data from users is restricted, the market for online services will decline, particularly for information of various kinds, especially news.

Legislation, regulation, and changes in privacy policies of some platforms affect the ability of online service providers to earn advertising revenue. These policy areas include (a) laws or regulations that prohibit collecting, processing, or sharing certain kinds of personal data and (b) rules that require opting in or that make it easier for users to opt out of data collection, sharing, or processing, whether enforced by government or imposed by online platforms. This paper begins by considering the status quo in terms of government policy and companies' practices that influence privacy and the collection and processing of personal data online. Existing legislation includes the General Data Protection Regulation in Europe (GDPR) and the California Consumer Privacy Act (CCPA), which is stricter than omnibus privacy laws that have been enacted in several other states. Following that summary is a discussion and analysis of recent and proposed changes in policy and their likely influence on the functioning of the online economy and the welfare of publishers, advertisers, and consumers of online services. Those changes include possible federal privacy legislation and changes made or proposed by online platforms, such as Apple and Google. The concluding section summarizes how privacy policy changes might significantly reduce mutually beneficial exchanges of data for services and contribute to reduced competition in the online economy. It also acknowledges, however, that entrepreneurs may be able to devise creative ways to combine greater transparency and more options for consumers to enhance their privacy with little or no harm to the online ecosystem that is based on exchanging data for services.

THE STATUS QUO AND RECENT CHANGES

To do personalized advertising, marketers use data collected about consumers of online services to choose which ads to show to them depending on their demographics and interests. Marketers try to ascertain users' interests by capturing what other websites they visit while online and by gaining other information that users may disclose about themselves. They can also use data to reengage users who have already expressed an interest in a product or service and to identify potential customers by comparing users with existing customers.[1]

In addition to targeting advertising to users, online marketers collect data about who is shown ads for certain products to cap the frequency in which a user encounters an ad for a particular product. The marketers also use data to measure how many users who were exposed to their ad campaign performed the desired action (such as making a purchase). Besides data on user demographics and interests, advertisers collect and use data about users' behavior after users are exposed to a particular ad.

The online economy in the United States relies heavily on online behavioral advertising.[2] Privacy regulation threatens its continuing viability. The case for online behavioral advertising enhanc-

ing economic welfare is a straightforward one. By using information to target their advertising, publishers can direct specific advertising to those users most likely to be interested so as to maximize earnings from advertising. Although it need not be the case that publishers earn more by using targeted advertising, the joint payoff between the publisher and the advertiser is likely to be higher.[3] If users voluntarily allow their data to be collected for online advertising, then behavioral advertising likely enhances their welfare as well.[4] If targeting is effective, a larger percentage of the ads that users are exposed to will be for products that are of interest to them.

Existing Legislation

Privacy advocates, such as the Electronic Frontier Foundation, Privacy International, and Electronic Privacy Information Center, have been pushing for the enactment of legislation to limit the collection of personal data for commercial purposes and to regulate how those data are processed, used, and shared. The General Data Protection Regulation in the European Union (EU) has already had a significant effect on how data are collected and used in EU countries. In the United States, state legislation such as the California Consumer Privacy Act has also influenced how platforms collect and use personal data.

The GDPR, which became effective in 2018, requires a data controller—the person or organization that determines how and why data will be processed—to provide much specific information, including purposes and legal bases for collecting and processing personal data and third-party recipients of the data. To collect and process personal data, the controller must obtain opt-in consent from the data subject. The data controller must inform the data subject if automated decision-making or profiling is used and must give "insight into the 'logic' behind the profiling."[5] The GDPR includes an access right so that individuals have the right to know whether a data controller is processing their personal data, to request and receive access to the data, and to know details about the processing.[6]

In addition to the GDPR, the EU recently enacted the Digital Services Act, which affects personal data collection and online advertising.

California was the first US state to enact comprehensive privacy legislation, the CCPA, which took effect at the beginning of 2020. The CCPA has much in common with the GDPR. Both give individuals a right to access and a right to delete personal information collected about them. The GDPR requires that controllers obtain opt-in consent from data subjects unless controllers have "compelling legitimate grounds for processing," whereas the CCPA requires that controllers give data subjects the option to opt out of data collection, processing, and sharing.[7]

An important provision of the CCPA is its antidiscrimination requirement. The CCPA says that firms cannot discriminate against consumers who exercise their privacy rights by denying them

goods or services, charging them different prices, or providing a different quality of service, unless the price or difference is "reasonably related to the value provided to the consumer by the consumer's data."[8] But firms will not want to provide the same services to consumers who opt out of data collection without charging them higher prices. To earn enough revenue to cover their costs and stay in business, they may need to treat such consumers differently.

In enforcing this nondiscrimination provision, how is the state going to determine whether a price difference is reasonably related to the value of a consumer's data? How much leeway will firms have in deciding how to set prices or quality differences for those who opt out of data collection? Will the provision require companies to defend the price they charge with an explicit formula? One possibility is that companies could be required to report on a quarterly or an annual basis how much they receive from the sale or sharing of consumer data.[9]

The GDPR does not have a provision that is equivalent to the CCPA's antidiscrimination provision. But the EU treats the right to privacy as a fundamental human right, which implies that it would be invalid for a service provider to require "a data subject to waive their GDPR rights as a condition to use a service."[10] In other words, the EU principle means that online services cannot refuse to serve someone because the person does not provide personal information—unless processing that information "is necessary for the purposes of the legitimate interests pursued by a controller or third party" and such interests are not "overridden by the interests or fundamental rights and freedoms of the data subject."[11] In contrast to the CCPA, the GDPR does not limit an online firm's freedom to decide how much to raise the price or lower the quality of a service that the firm provides to users who opt out of data collection.

The GDPR affects privacy policy in the United States, partly because many US companies have extensive operations in Europe, but also because recent and proposed legislation shares some features in common with the GDPR.

Tech Company Initiatives

An important element of online advertising is how advertisers identify users. In the past, online advertising has relied on cookies, which track users across sites. But concern about privacy has given online service providers an incentive to limit how users are tracked. Firefox led the way in protecting users of its browser from tracking, including social media trackers, cross-site tracking cookies, and cryptominers.[12] Beginning with release 69, the Firefox browser blocks tracking cookies by default.[13] Apple made similar changes to stop the using of tracking cookies by its Safari browser.

Apple took a major step in promoting privacy on its mobile operating system when it introduced its App Tracking Transparency (ATT) privacy policy in April 2021. ATT requires app users to opt

in for iOS app developers to be able to track their users beyond the app in use.[14] Such tracking can be accomplished through a mobile advertising identifier, which on iOS is the Identifier for Advertisers (IDFA). The IDFA makes it possible to track users across multiple sessions of an app and across apps. With the ATT policy in place, if an Apple mobile operating system (iOS) user asks an app not to track, then the app can no longer access the IDFA. Before Apple implemented this new policy, users could opt out from the use of IDFA, but tracking was the default and the option to opt out was "not very visible in the system settings of iOS devices."[15]

Google announced a plan to stop using cookies to track users of its Chrome browser, now projected to take effect in 2024. To bring this effort to fruition, it created an open-ended development environment, referred to as a Privacy Sandbox.[16] Google is developing alternatives to third-party cookies to achieve goals of improving user privacy while preserving an online ecosystem where free online content is funded by advertising. Google is carrying out this effort in collaboration with the rest of the industry, including publishers, developers, and advertisers.[17] Per Google, the following changes are anticipated:

- Instead of tracking individuals across the web to find out their interests, the browser will share the observed topics of recently visited sites without any connection to an individual.
- Instead of having companies collect people's information in the course of showing them ads, that information can be kept on each person's device so that it stays private.
- Instead of measuring how people respond to ads in a way that could reveal their identity, individuals can be kept anonymous by limiting how much data can be shared about them.[18]

Rather than third-party cookies tracking the websites a user visits, the new approach uses the web browser to determine up to three topics that represent a user's top interests for the current week. This technique will mean that "a person's specific browsing information never leaves their devices."[19]

Google is also planning to phase out the Android Ad ID, which works in a similar way to Apple's IDFA, and it has given developers at least two years' notice of its plans.[20] It has offered a public commitment not to give preferential treatment to Google's ads, products, or sites.[21]

Other firms in the advertising technology, or ad tech, industry are exploring other open-source proposals. These include the Secure Web Addressability Network (SWAN) and Unified ID 2.0. With SWAN, when users visit a website, they can choose whether to permit all publishers that use SWAN to show them ads.[22] They can revoke this permission at any time and should also have access to a list of all organizations that receive their data.[23]

Unified ID 2.0, a new kind of online identifier, was developed by the Trade Desk, a digital advertising company. This identifier relies on email addresses, which are anonymized through encryption, to create profiles for users.[24] The identifier is an alternative to collaborating with walled gardens—platforms that control a user's access to applications, content, or media, such as Google and Facebook.

HOW THE ONLINE ECONOMY IS CHANGING IN RESPONSE TO NEW POLICIES AND PRACTICES

In addition to legislation, technology platforms have been changing their policy and practices to better promote privacy. The GDPR had a major impact on the online economy after it was enacted. Changes in policy and practices by tech platforms, such as Apple, have also already had an important impact. Tech companies are changing their policies and practices in response to GDPR, state legislation, and pressure from privacy advocates.

Evidence on the Impact of GDPR and CCPA

In the first year after passage of the GDPR, an estimated 1,000 news sources, including the *Los Angeles Times* and *Philadelphia Inquirer*, blocked EU readers because the news sources were not in compliance with GDPR provisions. Companies that wanted to continue collecting online data in Europe spent billions of dollars preparing to be compliant with the GDPR. UK companies spent $1.1 billion and US companies an estimated $7.8 billion between the implementation of the GDPR and the end of the first year it took effect.[25]

The implications of the GDPR for online behavioral advertising are still not completely clear. In light of provisions such as purpose limitation and specific consent, behavioral advertising is problematic. It is questionable whether data subjects provide specific, informed consent, because the nature of correlating identified interests with a willingness to purchase a particular good or service makes it "inherently impossible to establish ex ante what data will be collected and what processing activities will take place."[26] Consider the requirement that data controllers explain the logic of profiling to data subjects. It is not clear whether it is possible that information could be provided to typical users that would be meaningful and would enable them to understand how their clicks and search queries led to the ads they are being shown.[27]

A large share of online advertising is programmatic, involving multiple advertisers bidding for each online advertising slot. As the GDPR was being implemented, an innovative way emerged to obtain consent from data subjects when multiple firms are involved in processing and using the data. That innovation was consent management platforms (CMPs). CMPs are embedded within web pages and sometimes within apps and enable a large number of third parties to "simultane-

ously seek consent from a data subject in one action."[28] This tool usually results in consent being sought for hundreds of vendors at once.[29]

Even with all the information rights included as part of the GDPR, it is difficult for a consumer to "attain a working knowledge of the data being processed," especially when complex advertising networks are involved.[30] Many of the firms involved in the targeted advertising market do not interact directly with the consumer. Consumers may be familiar with Google's advertising network, but most are not familiar with many other ad networks that collect their data on some of the websites they visit.

The GDPR gives data subjects certain information rights, such as the right to access personal data collected about them. Large platforms, such as Google and Facebook, have developed procedures so that data subjects can download or view data that has been collected about them.[31] It is more difficult for users to invoke their right to data access when other ad networks are involved and they do not know which specific companies are receiving and processing their data.

Although some behavioral advertising may continue to be allowed, the way it is currently practiced will likely need to change in EU countries. In particular, real-time bidding, which involves many parties, may not comply with the GDPR in at least three ways. First, because of the large number of parties involved and the complexity of how data are processed, it is very difficult for all involved to get valid consent. Second, the requirement that controllers provide clear, plain, and intelligible information about what will happen to a subject's data is hard to comply with because the publisher does not know the identities of all parties that might collect data on its site and probably cannot explain real-time bidding to site visitors. Third, it is difficult to meet the requirement to provide adequate security in the form of protection against unauthorized or unlawful processing when multiple parties are involved.[32]

The recently enacted Digital Services Act (DSA) clarifies EU policy toward online advertising. It prohibits targeted advertising to minors and the use of sensitive data, including data on sexual orientation, political opinions, and racial or ethnic origin for targeted advertising.[33] The DSA requires that platforms provide users with meaningful information about how their data will be monetized, about who sponsors the ads users are shown, and about the "main parameters used" to decide which users to target.[34] It singles out very large online platforms and requires that they "maintain a repository of exposed ads, sponsor information, parameters used to target, and total exposures."[35]

The CCPA may have less effect on the online economy than the GDPR because it only requires that firms give users a choice whether to opt out of data processing and sharing. It restricts the selling of personal data but not its collection.[36]

Google as De Facto Privacy Regulator: Implications for Competition

An important question is the relationship between privacy policy and competition. One concern is that Google, because of its size and dominant role in online data collection and advertising, has become a de facto privacy regulator. By setting the standards for online advertising, Google may be able to gain an unfair competitive advantage. Google and Facebook already dominate the digital advertising market, capturing 51 percent of digital ad spending worldwide and 61 percent in the United States in 2019.[37] These two firms are dominant because they operate highly popular user-facing services.

Any regulation that makes it harder to track users, particularly via third-party data and cross-site tracking, favors highly integrated companies like Google and Facebook that have lots of internal sources of user information. By making it harder to share and process third-party data, the GDPR and some state privacy legislation limit third-party tracking that can be used to construct profiles for targeting online advertising. Google's plans to stop supporting third-party cookies by 2024, if implemented, would also tend to reduce cross-site tracking, which will favor publishers large enough to collect a variety of first-party data about users.[38]

Google's plan to phase out tracking cookies led to a backlash by influential players in the digital media ecosystem, such as ad tech firms that depend on cookies to collect information about users.[39] Google's stated intention is to provide an alternative way to track anyone who uses its Chrome browser and to work with publishers and ad tech firms so they can use that tracking data for ad targeting. In 2020, as part of its experimental Privacy Sandbox, Google announced plans to use a new technology, Federated Learning of Cohorts (FLoC), which would be driven by artificial intelligence. FLoC had several weaknesses, including the following:

- The data Google was planning to collect would make it possible to infer other data, some quite sensitive, about users.
- By sorting users into cohorts of a few thousand, FLoC would have made digital fingerprinting—a process by which information about a user's device or browser is used to identify the user—easier.[40]

Eighteen months later, in January 2022, Google announced that FLoC was to be dropped, with Google citing heightened ability to fingerprint users as a reason for FLoC's termination. FLoC was "replaced by a new system known as 'The Topics API' and another known as 'Fledge.'"[41] Because of this change, Google delayed phasing out cookies in 2022 as originally planned. Its latest plans are to wait until late 2024 to phase out tracking cookies.

An amended monopolization complaint against Google by a Texas-led coalition of state attorneys general includes allegations that Google's plan to terminate cookies on its Chrome internet browser is anticompetitive.[42] By making the browser the central player in the ad tech ecosystem,

Google's various Privacy Sandbox proposals will tend to favor Google because of its large browser market share. How this change affects Google's competitors in online advertising depends on their options. Without cookies, the publishers, marketers, and advertisers have three possible ways to compete with Google: (a) by contextual advertising, (b) by relying on first-party data for ad targeting, or (c) by using email-based identity solutions.[43] Small publishers do not have the same access to data and so may be better off relying on leading consumer-facing platforms such as Google and Facebook to decide how to target advertising on their sites. These decisions, in turn, may enhance Google's power in the market for ad tech services.

Pressure from antitrust regulators is influencing the steps Google is taking to replace cookies. The United Kingdom's Competition and Markets Authority (CMA) has been investigating Google's Sandbox proposals.[44] This investigation may be part of the reason Google has made a public commitment not to give preferential treatment to its own ads, products, or websites in the way it collects and uses personal information.[45] Google has sought to cooperate with the CMA, offering to make legally binding commitments involving CMA oversight of its Privacy Sandbox and related changes in functionality to address competition concerns.[46]

Competition between Online Platform Efforts to Enhance Online Privacy: Hype versus Reality

There is considerable uncertainty about when and whether Google will actually carry out its plan to phase out tracking cookies or how that action will affect online advertising. As noted, Mozilla Firefox and Apple have stopped the use of tracking cookies on their browsers, and ATT has made it harder to track app users on mobile devices. According to one estimate, 18 percent of Apple's mobile clients opted in to tracking as of April 2022.[47] That small number who allowed tracking is an important reason why Facebook experienced a decline in advertising revenue in 2022. Lack of access to IDFA limits the ability of apps to use targeted ads. The inability of tracking libraries to access IDFA has also reduced opportunities for data brokers.[48]

Several factors have limited how much ATT has been able to reduce tracking and bring about greater privacy. One factor is that Apple allows companies, such as Snap Inc. and Facebook, to "keep sharing user-level signals from iPhones, as long as that data is anonymized and aggregated" and not tied to specific users.[49] This policy allows Facebook and Snapchat to continue tracking users who have asked not to be tracked.[50] Apple continues to have access to user-level identifiers, which has enabled it to increase advertising revenue at the expense of others to whom its policy has denied such access. But Apple's ability to enforce ATT is limited. Apps are still able to widely use the "tracking technologies of large companies and send a range of user and device characteristics over the internet."[51] Apps are not allowed to fingerprint, according to the Apple Developer program license agreement, but Apple has not developed a technical solution to prevent apps

from fingerprinting users.[52] As a result, there is a discrepancy between the disclosed and actual data practices of many apps.

The Role of Federal versus State Privacy Legislation

Privacy law in the United States is fragmented across sectors and across states. The argument for omnibus federal legislation is that compliance costs will be lower if online firms do not face a variety of state privacy laws. How much federal legislation would reduce compliance costs depends on the extent to which federal law preempts state laws. A key issue that has made it difficult to pass federal privacy legislation is whether preemption should apply to state rules that are stricter than the federal law. Many privacy advocates favor an approach where federal privacy law serves as the baseline, with states having the option of adding stricter provisions. But some proponents recognize that federal legislation is more likely to pass if it preempts stricter state regulation. One possible compromise is for federal provisions that preempt stricter state provisions to sunset after a period of time, giving "Congress the opportunity to revisit any need for state laws to supplement a comprehensive federal privacy law."[53]

Proponents of federalism claim that front-runner states promote a race to the top in terms of data privacy regulation.[54] Because of its large size, other states often imitate California in their regulatory policy. Given the interconnectedness of the online economy, many online firms will likely choose to adhere to the requirements of the CCPA, such as giving consumers the choice to opt out of data collection, in their interactions with US users in the other 49 states.[55]

CONCLUSION

In light of trends, it appears that privacy legislation and the response of large platforms to legislation, regulation, and user preferences could lead to dramatic changes in the online economy, reducing opportunities to exchange personal information for online services. Entrepreneurs, however, have an incentive to find creative ways to facilitate information exchange, insofar as it is mutually beneficial, in a way that better protects user privacy.

Some of the policy changes that have already been implemented as well as some of those being considered have had a significant effect on the online behavioral advertising ecosystem, but more changes are likely to occur in the future. It is possible that if data collection and processing are done more transparently, advertisers will be able to continue to target users as effectively as they have in the past. Competition over privacy policy could not only lead to some improvements in privacy but also more concentration of data collection with fewer tech companies, as legislation and changes in the practices of large platforms make it harder for publishers to use traditional tracking technologies, such as cookies.

Despite being described by pejorative terms such as *surveillance capitalism*, most current commercial collection and processing of user information is comparatively benign. Those that are concerned about privacy have contributed to a backlash against the collection and processing of personal information that may have gone too far in some places. Devoting resources and political capital to policy and practices intended to enhance user privacy has opened the door for creative solutions that are likely to improve privacy, although risks to privacy and concerns about insufficient privacy are still a problem. Whether and how much the improvement in privacy from current and proposed changes in policy impairs the functioning of the online economy remains to be seen.

NOTES

1. Damien Geradin, Dimitrios Katsifis, and Theano Karanikioti, "Google as a De Facto Privacy Regulator: Analysing the Privacy Sandbox from an Antitrust Perspective," *European Competition Journal* 17 (2021): 625.
2. Behavioral advertising involves choosing which ads to display to which website users as a result of tracking the websites that users visit and the personal information they disclose online.
3. Jianquin Chen and Jan Stalleart, "An Economic Analysis of Online Advertising Using Behavioral Targeting," *MIS Quarterly* 38 (June 2014): 429–49.
4. Some privacy proponents would argue that users may be made worse off by giving up their privacy in exchange for online services. Evidence is mixed about whether online behavioral advertising makes users better off. See Kaan Varnalli, "Online Behavioral Advertising: An Integrative Review," *Journal of Marketing Communications* 27 (2021): 93–114.
5. Peter van de Waerdt, "Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market," *Computer Law and Security Review* 38 (2020): 7.
6. Bret Cohen, Britanie Hall, and Ryan Woo, "The Challenge Ahead: A Comparison of 10 Key Aspects of the GDPR and the CCPA," Hogan Lovells, October 3, 2018, https://www.engage.hoganlovells.com/knowledgeservices/news/the-challenge-ahead-a-comparison-of-10-key-aspects-of-the-gdpr-and-the-ccpa_1.
7. Cohen, Hall, and Woo, "The Challenge Ahead."
8. California Consumer Privacy Act. The full text of the act is available at https://ccpa-info.com/california-consumer-privacy-act-full-text/.
9. Jeeyun Baik, "Data Privacy against Innovation or against Discrimination: The Case of the California Consumer Privacy Act (CCPA)," *Telematics and Informatics* 52 (September 2020): 101431.
10. Cohen, Hall, and Woo, "The Challenge Ahead."
11. Michael Veale and Frederik Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law," *German Law Journal* 23 (2022): 226–56.
12. Barry Collins, "Why I'm Leading a Browser Double Life," *Web User* 504 (June 24–July 7, 2020): 74.
13. Barry Collins, "Has Firefox Found Chrome's Kryptonite?," *Web User* 485 (October 2–15, 2019): 74.
14. Manoj Balasubramanian, "App Tracking Transparency Opt-In Rate: Monthly Updates," *Flurry* (blog), May 2, 2022, https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/.
15. Konrad Kollnig et al., "Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels," ACM FAccT '22, June 21–24, 2022, Seoul, Republic of Korea, 2.
16. David Eliot and David Murakami Wood, "Culling the FLoC: Market Forces, Regulatory Regimes and Google's Mis(steps) on the Path Away from Targeted Advertising," *Information Polity* 27 (2022): 259–74.

17. Google, The Privacy Sandbox, retrieved March 24, 2023, from https://privacysandbox.com/.
18. Chetna Bindra, "The Future of Privacy—and How You Can Prepare," August 2022, https://www.thinkwithgoogle.com/future-of-marketing/privacy-and-trust/privacy-sandbox/.
19. Bindra, "The Future of Privacy."
20. Allison Schiff, "Android Gets Its Own Privacy Sandbox—and Goodbye, Google Ad ID (in Two Years, Maybe)," AdExchanger, February 16, 2022.
21. Anthony Chavez, "Introducing the Privacy Sandbox on Android," *Google* (blog), February 16, 2022.
22. Naim Cinar and Sezgin Ates, *Data Privacy in Digital Advertising: Toward a Post-Third-Party Cookie Era in Privacy Algorithms and Society*, ed. Michael Filimowicz (London: Routledge, 2022).
23. SWAN Introduction, https://vimeo.com/549212557/43e5669a08.
24. Garett Sloane, "Everything Brands Need to Know about the Post-Cookie World," *Advertising Age,* October 4, 2021.
25. Rob Sobers, "A Year in the Life of GDPR: Must-Know Stats and Takeaways," *Varonis* (blog), February 2022.
26. Van de Waerdt, "Information Asymmetries," 12.
27. Van de Waerdt, "Information Asymmetries," 8.
28. Veale and Borgesius, "Adtech and Real-Time Bidding."
29. Midas Nouwens et al., "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence," *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, April 2020, 5.
30. Van de Waerdt, "Information Asymmetries," 7.
31. Van de Waerdt, "Information Asymmetries," 7.
32. Veale and Borgesius, "Adtech and Real-Time Bidding."
33. Eric Seufert, "Unpacking the DSA's Impact on Digital Advertising," Mobile Dev Memo, April 25, 2022.
34. Seufert, "Unpacking the DSA's Impact."
35. Seufert, "Unpacking the DSA's Impact."
36. Lengrui Liu, Umar Iqbal, and Nitesh Saxena, "Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy?," arXiv, 2022, https://arxiv.org/pdf/2202.00885.pdf.
37. Geradin, Katsifis, and Karanikioti, "Google as a De Facto Privacy Regulator."
38. Google originally announced plans to stop supporting cookies in 2022 but has delayed doing so. It announced in July 2022 that it will wait until 2024. See https://adtechbook.clearcode.cc/challenges-opportunities/.
39. Michael Applebaum, "How Brands Can Thrive in a World Without Cookies," Path to Purchase Institute, October 2021.
40. Eliot and Wood, "Culling the FLoC."
41. Eliot and Wood, "Culling the FLoC," 259.
42. Second Amended Complaint, Texas v. Google LLC, No. 20-CV-957, 2021 WL 2043184 (E.D. Tex. Aug. 4, 2021), 96–99.
43. Geradin, Katsifis, and Karanikioti, "Google as a De Facto Privacy Regulator," 661.
44. Matt Burgess, "Google's Rivals Are Fighting Back against Chrome's Big Cookie Plan," *Wired*, March 24, 2021.
45. Chavez, "Introducing the Privacy Sandbox."

46. Competition and Markets Authority, United Kingdom, "CMA Secures Improved Commitments on Google's Privacy Sandbox," press release, November 26, 2021.

47. Balasubramanian, "App Tracking Transparency."

48. Kollnig et al., "Goodbye Tracking?"

49. Patrick McGee, "Apple Reaches Quiet Truce over iPhone Privacy Changes," *Financial Times*, December 8, 2021.

50. Hartley Charlton, "Report: iOS Users Who Opt Out of App Tracking Continue to Be Tracked by Facebook and Snapchat," MacRumors, December 8, 2021.

51. Kollnig et al., "Goodbye Tracking?"

52. Allison Schiff, "It's Time for Apple to Stop Pointing Fingers at—and Start Enforcing Against—Fingerprinting," AdExchanger, June 15, 2022.

53. Cameron Kerry et al., "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," report, Brookings, June 2020, 7.

54. Bilyana Petkova, "The Safeguards of Privacy Federalism," *Lewis and Clark Law Review* 20 (2016): 595–645.

55. Catherine Barrett, "Are the EU GDPR and the California CCPA Becoming the De Facto Global Standards?," *Scitech Lawyer* 15 (Spring 2019): 24–29.