Online Consumer Data Collection and Data Privacy

October 31, 2022

Congressional Research Service
https://crsreports.congress.gov
R47298

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Online Consumer Data Collection and Data Privacy

SUMMARY

R47298

October 31, 2022

Clare Y. Cho
Specialist in Industrial Organization and Business Policy

Ling Zhu
Analyst in Telecommunications Policy

Large amounts of consumer data can be collected, processed, and analyzed by operators of websites and mobile applications (apps) and *third parties*, which are entities other than the website or app primary operator (e.g., data brokers). Operators collect data for multiple purposes, including providing services, selling user data to third parties, or sending targeted ads directed to specific individuals.

The value of consumer data often comes from identifying users and linking their data from various sources to a common identifier. Operators can identify individuals using their personally identifiable information (PII)—such as name, address, or date of birth—and other identifiers, such as those associated with a particular device. Some federal laws prevent entities from collecting or sharing specific types of PII or identifiers in certain circumstances. However, in recent decades, the ubiquity of non-PII (data not directly linked to an individual's identity, including anonymized or aggregated data) and the emergence of new data collection and tracking tools have made it easier to identify individuals.

Consumer data can be collected using various data collection and tracking tools, such as cookies, pixels, device and browser fingerprinting, application programming interfaces (APIs), and software development kits (SDKs). These tools can continuously collect different types of data, including identifiers, even when the consumer visits a different website or app. Some of these tools are necessary for websites and apps to provide services, and others typically are used for online advertising. Some of these tools can be used to help develop a website or app and offer services provided by other operators, which can increase competition. They also can be used to collect large amounts of data, particularly by third parties, causing some to raise consumer data privacy concerns.

Although some intermediaries—such as web browsers and operating systems—offer anti-tracking tools allowing users to limit the data collected by websites, apps, and third parties, they can also make it difficult for individuals to access these tools. Most web browsers offer "private browsing" or "incognito" modes that allow users to refuse cookies, and some browsers ban third-party cookies. Apple released an iPhone operating system update that requires apps to ask for permission before tracking user activity. Google has restricted access to a consumer identifier in its advertising (ad) network and banned certain ad blocking apps, some of which were reinstated, from its app store. Intermediaries such as these may be able to obtain a competitive advantage if they are able to collect data that others cannot access.

The United States does not have a comprehensive federal data protection law, although multiple federal statutes create data protection obligations for particular types of information or for entities engaged in certain activities. For example, the Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§6501-6506) requires online services directed to children under 13 years of age that collect personal information to notify users about the data collection, receive parental consent, and maintain "reasonable procedures" to protect the data. COPPA is enforced by the Federal Trade Commission (FTC), which has brought enforcement actions against companies for their consumer data collection practices under its authority to prevent "unfair or deceptive acts or practices in or affecting commerce." For example, it has taken action against companies for allegedly handling personal information in a way that contradicts their privacy policies. The FTC is also considering whether it will implement new rules on data collection and security to protect consumers' data and privacy.

A comprehensive federal data protection law may have differential effects. For example, prohibiting the collection of consumer data would provide the highest level of data security but could also prevent some operators from providing their services or degrade the quality of their services. Prohibiting the transfer or sale of consumer data might provide some data protection, depending on the operators that consumers are willing to share their data with, but could also further entrench incumbents that have already collected large amounts of consumer data. Increasing transparency on the collection and use of consumer data—particularly if doing so would heighten public scrutiny of the operator—might incentivize operators to adjust their current practices but might not significantly alter operators' behavior if consumers continue to use the website or app.

Some Members of the 117th Congress have introduced bills to create a comprehensive data protection law. If Congress chooses to pursue legislative action, it may consider (1) if the legislation would broadly address consumer data collection or focus on specific types of data, (2) whether to implement requirements for operators or allow consumers to determine which

entities can receive their data, (3) if the legislation would preempt state laws, (4) whether to include a private right of action, and (5) potential unintended effects.

Contents

Figures

Contacts

Introduction

Over the past few decades, developments in information and communication technologies have enabled operators of websites and mobile applications (apps) and third parties to collect, process, and analyze large amounts of consumer data.[1] These developments have led to new products and services that collect and provide real-time information, including navigation services that update users with current traffic conditions and suggest faster routes, health-related services that can track physical activity or help users determine whether they are ovulating, and finance-related services that can help users analyze their spending habits.

Website and app operators may collect user data for multiple purposes, such as providing or improving their services, selling user data to third parties, or sending targeted advertisements.[2] Some data collection may benefit consumers when, for example, it allows consumers to access services at a cheaper price or for free. However, some consumers may be unaware that their data are collected and how that data are used.

The United States does not have a comprehensive federal data protection law, although multiple federal statutes create data protection obligations for particular types of information or for entities engaged in certain activities.[3] Some Members of the 117th Congress have introduced bills to create a comprehensive data protection law,[4] and five states have implemented their own comprehensive consumer data protection laws.[5] In October 2022, the White House Office of Science and Technology Policy (OSTP) released "Blueprint for an AI Bill of Rights,"[6] which includes recommended data privacy protections for all Americans.[7] Although OSTP does not have regulatory or enforcement authority, it notes, "where law or policy does not already provide guidance, the *Blueprint* should be used to inform policy-making to fill those gaps."[8]

[1] In this report, *consumer data* includes any data about an individual, including personally identifiable information (PII), demographic data, behavioral data (e.g., search history, buttons clicked on a website), and purchase data. *Operator* is used to describe the entity—such as a firm, nonprofit organization, or individual—that controls and operates the website or app. *Third parties* are entities other than the primary operator of the website or app; see text box in "Identifying and Linking Consumer Data."

[2] In this report, *targeted ads* are ads sent to a specific individual using their data. For more information about targeted advertising, see Organisation for Economic Co-operation and Development, *Competition in Digital Advertising Markets*, 2020, at https://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf; and Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, Federal Trade Commission (FTC), January 2020, at https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf.

[3] CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[4] For example, see the American Data Privacy and Protection Act (H.R. 8152) and the Consumer Online Privacy Rights Act (S. 3195). For comparisons of some of these bills, see CRS Legal Sidebar LSB10776, *Overview of the American Data Privacy and Protection Act, H.R. 8152*, by Jonathan M. Gaffney, Eric N. Holmes, and Chris D. Linebaugh.

[5] The five states are California, Colorado, Connecticut, Utah, and Virginia.

[6] White House, Office of Science and Technology Policy (OSTP), "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People," October 4, 2022, at https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[7] White House, OSTP, "Blueprint for an AI Bill of Rights: Data Privacy," October 4, 2022, at https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/.

[8] White House, "FACT SHEET: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public," October 4, 2022, at https://www.whitehouse.gov/ostp/news-updates/2022/10/04/fact-sheet-biden-harris-administration-announces-key-actions-to-advance-tech-accountability-and-protect-the-rights-of-the-american-public/.

This report provides a brief overview of methods for consumer data collection on websites and mobile apps.[9] It then discusses some efforts to limit consumer data collection and considers the potential effects of a comprehensive federal data protection law on website and app operators, which may be applicable to other types of data collection as well.

How Consumer Data Are Collected Online

Each day, individuals interact with digital technologies that collect vast amounts of their data—including self-reported personal information and online behavioral data—without their knowledge. Website and mobile app operators, as well as third parties (see text box), use these data to make inferences and decisions, inform machine learning models, and build detailed user profiles for targeted advertising or personalized content, among other purposes. This section discusses some of the tools used to collect consumer data and track individuals online.

Sources of Data Collection: First vs. Third Party

In this report, *first-party data* refers to data that the primary operator of a website or app collects directly from its users.[10] Some first-party data may be self-reported, that is, actively provided by the individual creating an account (e.g., name, age) or uploading content. *Third-party data* are collected by entities other than the primary operator of a website or app.[11] Some data collection tools can blur the distinction between first and third parties. For example, some providers of online advertising (ad) services embed code on websites that use their services; the ad service would be considered a third party in this report because it is not the website's primary operator.

First- and third-party data collection can raise different concerns. First-party data may be collected without a user's express consent or knowledge; this is nearly always the case with third-party data unless the user resides in a state or country that requires entities to obtain consumer consent.[12] Additionally, some website and app operators might supplement their first-party data with third-party data. For example, an operator might purchase or exchange user data with third parties; a firm could also acquire another firm to obtain its consumer data.

Nearly all of the most popular apps and websites provide data to third parties. One study found that the top one million websites send data to at least 34 third parties on average.[13] Another study found that nearly one million

[9] This report does not discuss data collected by internet service providers (ISPs) or other internet-connected devices, such as smart devices, that may present similar data privacy concerns. For more information, see FTC, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, Staff Report, October 21, 2021, at https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers; and CRS In Focus IF11239, *The Internet of Things (IoT): An Overview*, by Patricia Moloney Figliola; and CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Patricia Moloney Figliola.

[10] Some data protection regulations use different terms for first-party data collection. For example, the European Union's (EU's) General Data Protection Regulation (GDPR) uses the terms *controller* and *processor* for data collection methods that would be considered first party in this report. See Article 4(7, 8) of the GDPR, at https://gdpr-info.eu/art-4-gdpr/.

[11] The EU's GDPR defines *third party* as "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data." See Article 4(10) of the GDPR, at https://gdpr-info.eu/art-4-gdpr/.

[12] For example, the EU's GDPR requires the controller to demonstrate that the data subject has consented to processing of his or her personal data. For the definition of *consent*, see Article 4(11) of the GDPR, at https://gdpr-info.eu/art-4-gdpr/. For the definition of *conditions for consent*, see Article 7 of the GDPR, at https://gdpr-info.eu/art-7-gdpr/.

[13] Steven Englehardt and Arvind Narayanan, "Online Tracking: A 1-Million-Site Measurement and Analysis," presented at the 23rd ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 2016, at https://doi.org/10.1145/2976749.2978313 (hereinafter Englehardt and Narayanan, "Online Tracking").

mobile apps send data to 10 third parties on average.[14] Google and Meta (formerly Facebook)[15] dominate third-party data collection. A 2018 study of nearly one million apps available on the Google Play Store found that Google's trackers were present in more than 88% of all apps and Facebook's trackers in more than 42% of all apps.[16] Additionally, according to some estimates, Google Analytics trackers are present on approximately 75% of the top 100,000 websites.[17]

Data brokers—entities that collect, compile, and sell consumer data—rely primarily on third-party data.[18] The federal government does not regulate data brokers as an industry. However, two states—Vermont and California—have passed laws that implement requirements for data brokers, such as registering with the respective state annually.[19] Data brokers offer services—including direct marketing, marketing analytics, identity verification, fraud detection, and people searches—to clients in various industries. They collect data from clients, publicly available sources, commercial sources, and online tracking—often for a particular industry or niche market—and trade data with other data brokers to obtain a wide range of data. Data brokers may collect data across services and entities, de-anonymize the data, and link it to specific users using a variety of methods.

Identifying and Linking Consumer Data

The value of consumer data often comes from identifying users and combining their data from various sources. This is possible, in part, through the ubiquity of personally identifiable information (PII) and unique identifiers, as well as identifying individuals from non-PII, such as aggregated or anonymized data. The ability to identify users enables website and app operators to combine data and track user activity across devices.[20]

Personally Identifiable Information

PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[21] Examples of PII include names, addresses, dates of birth, telephone numbers, Social Security

[14] Reuben Binns et al., "Third Party Tracking in the Mobile Ecosystem," presented at the 10th ACM Conference on Web Science, Amsterdam, Netherlands, May 2018, at https://doi.org/10.1145/3201064.3201089 (hereinafter Binns et al., "Third Party Tracking").

[15] On October 28, 2021, CEO Mark Zuckerberg announced that Facebook, Inc. would be renamed Meta Platforms, Inc. to reflect the company's focus on the metaverse (see Meta, "Introducing Meta: A Social Technology Company," October 28, 2021, at https://about.fb.com/news/2021/10/facebook-company-is-now-meta/). For more information about the metaverse, see CRS Report R47224, *The Metaverse: Concepts and Issues for Congress*, by Ling Zhu.

[16] The study on Google's trackers included its advertising services DoubleClick, Admob, and Adsense, and the study on Facebook's trackers included Facebook, Liverail, and Lifestreet. See Binns et al., "Third Party Tracking."

[17] U.K. Competition and Markets Authority (CMA), "Appendix F: The Role of Data in Digital Advertising," *Online Platforms and Digital Advertising*, last updated July 1, 2020.

[18] For a more in-depth discussion of selected data brokers, see FTC, *Data Brokers: A Call for Transparency and Accountability*, May 2014, at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[19] 9 V.S.A. §§2446, 2447; see Vermont General Assembly, "The Vermont Statutes Online," at https://legislature.vermont.gov/statutes/section/09/062/02446. Title 1.81.48; see CaseText, *California Civil Code*, at https://casetext.com/statute/california-codes/california-civil-code/division-3-obligations/part-4-obligations-arising-from-particular-transactions/title-18148-data-broker-registration.

[20] Consumer Council of Norway, *Out of Control: How Consumers Are Exploited by the Online Advertising Industry*, January 14, 2020, at https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.

[21] Paul A. Grassi, Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, National Institute of Standards and Technology (NIST), Special Publication 800-63-3, June 2017, at https://doi.org/10.6028/NIST.SP.800-63-3.

numbers, precise location information, and biometrics.[22] Multiple federal statutes regulate the use of specific types of PII in certain circumstances.[23]

The proliferation of non-PII and its widespread collection have raised additional privacy concerns. For the purposes of this report, non-PII is all other kinds of data not directly linked to an individual's identity, including anonymized or aggregated data. The emergence of new data tracking tools, data analysis, and statistical techniques in recent decades has made it possible to identify individuals with a high degree of accuracy from non-PII.[24] For example, one study found that four approximate location data points are sufficient to identify 95% of individuals in a dataset of one and a half million people.[25] The Federal Trade Commission (FTC) has said, "the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data."[26]

Persistent Identifiers

In the context of online tracking, a persistent identifier—also called unique identifier—links a specific device or user with a unique ID.[27] A persistent identifier can detect a specific device or user across different websites or online services and target content or advertisements to specific users. Companies may also use persistent identifiers to share and combine user data with one another. Some persistent identifiers may be necessary to provide certain online services or functionalities, such as retaining unpurchased items in an online shopping cart. Persistent identifiers are intended to be long-lasting and track users over time. Some may reset or expire after a certain period, while others can identify users over a number of years.

Examples of persistent identifiers include device identifiers, such as Media Access Control (MAC) addresses,[28] and web-based identifiers, such as IP addresses;[29] third parties can also assign their own identifiers to users.[30] Mobile advertising IDs (MAIDs) are popular persistent identifiers consisting of a long string of numbers and letters that uniquely identify a user's mobile device

[22] While PII typically includes these forms of data, it may include other types of data. Shaun Donovan, *Preparing for and Responding to a Breach of Personally Identifiable Information*, Executive Office of the President, Office of Management and Budget, M-17-12, January 3, 2017, at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.

[23] For example, the Gramm-Leach-Bliley Act prohibits financial institutions from sharing "nonpublic personal information," and the Health Insurance Portability and Accountability Act prohibits "covered entities" from using or sharing "protected health information," which includes "individually identifiable health information." For more information about these laws, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[24] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, vol. 57 (2010), at https://www.uclalawreview.org/pdf/57-6-3.pdf.

[25] Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The Privacy Bounds of Human Mobility," *Scientific Reports*, vol. 3 (March 25, 2013), Article 1376, at https://doi.org/10.1038/srep01376.

[26] FTC, *Self-Regulatory Principles For Online Behavioral Advertising*, Staff Report, February 2009, at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (hereinafter FTC, *Self-Regulatory Principles*).

[27] Persistent identifiers may also refer to long-lasting references to digital resources, often used in library science and archival research.

[28] A *Media Access Control (MAC) address* is a long string of numbers and letters that uniquely identifies every device connected to a network and typically does not change.

[29] An *IP address* is a numerical identifier assigned to a computer or device that connects to the Internet. IP addresses can be used for location tracking by linking an individual IP address to a particular device that is associated with a specific individual. See FTC, *Self-Regulatory Principles*.

[30] Farhad Manjoo, "I Visited 47 Sites. Hundreds of Trackers Followed Me," *New York Times*, at https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html.

through its operating system.[31] Apple's iPhone operating system (iOS) uses an "Identifier for Advertisers" (IDFA) as its MAID, and Google's mobile operating system (Android) uses "Google Advertising ID."[32] MAIDs enable targeted ads to be sent to a specific device based on data collected about the user. Some data brokers have also used MAIDs to identify and sell user data, linking MAIDs to PII or other persistent identifiers.[33]

Persistent identifiers can constitute PII in certain circumstances. For example, in 2013, the FTC published an amended rule adding "persistent identifier" to the definition of *personal information* in the Children's Online Privacy Protection Act (COPPA).[34] In 2016, then-FTC Chair Edith Ramirez stated, "as a result of the increased ability to identify consumers, we now regard data as personally identifiable when it can be reasonably linked to a particular person, computer, or device. In many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers meet this test."[35]

Selected Data Collection and Tracking Tools

Website and app operators use various tools to collect consumer data. Some of these tools can continuously collect data, even when the user visits a different website or app.

This section discusses selected examples of data collection tools, including cookies, pixels, fingerprinting, application programming interfaces (APIs), and software development kits (SDKs). **Figure 1** provides an overview of these tools. This list is illustrative, not exhaustive.[36] Each tool can collect various types of data, including persistent identifiers.

[31] NIST defines an *operating system* as "a program that runs on a computer and provides a software platform on which other programs can run." Karen Kent et al., *Guide to Integrating Forensic Techniques into Incident Response*, NIST, Special Publication 800-86, August 2006, at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

[32] Bennett Cyphers and Gennie Gebhart, "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance," Electronic Frontier Foundation (EFF), December 2, 2019, at https://www.eff.org/wp/behind-the-one-way-mirror (hereinafter Cyphers and Gebhart, "Behind the One-Way Mirror"). Google Advertising ID has also been referred to as Android Advertising ID.

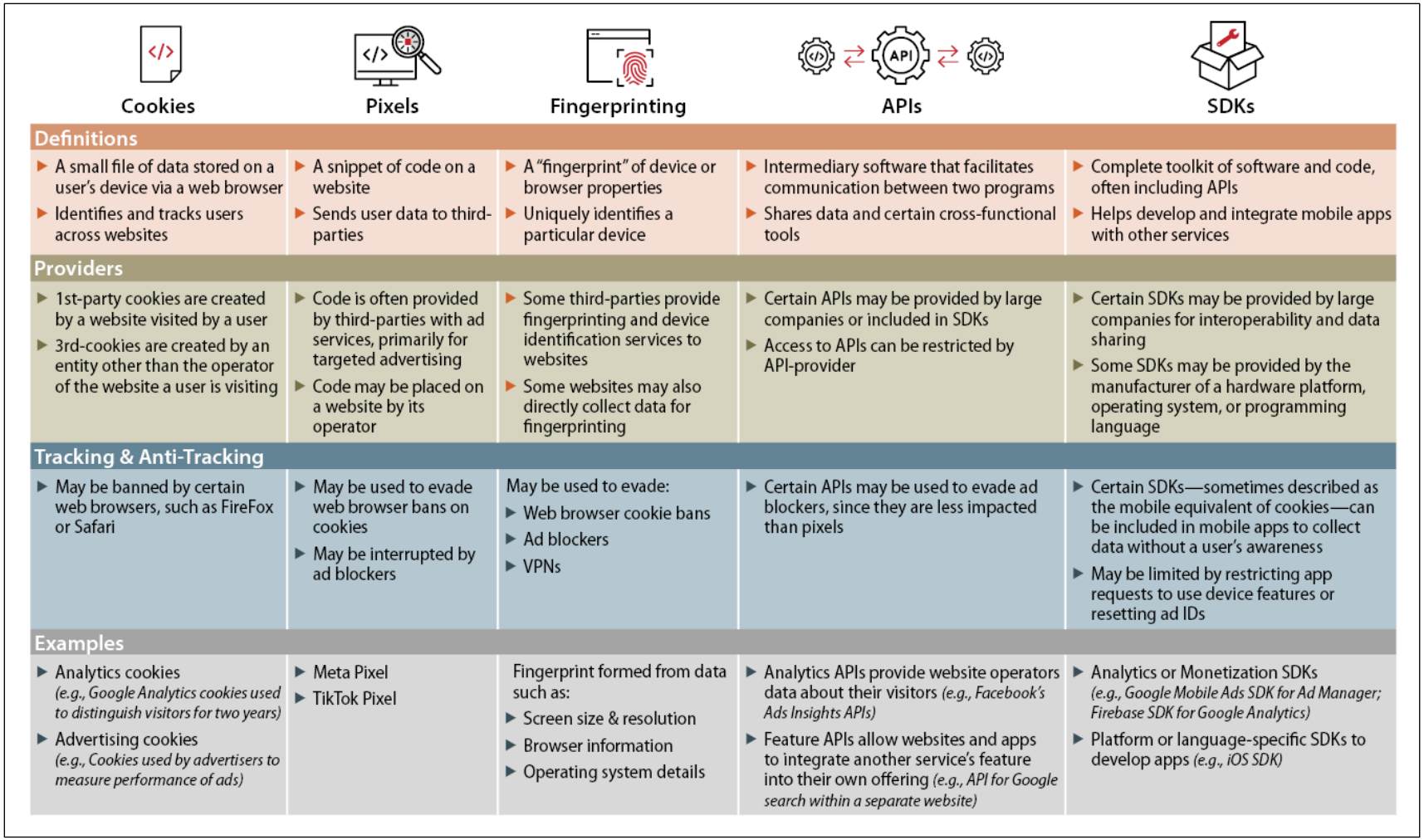
[33] Joseph Cox, "Inside the Industry That Unmasks People at Scale," *Motherboard: Tech by Vice*, July 14, 2021, at https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii.

[34] FTC, "Children's Online Privacy Protection Rule," 78 *Federal Register* 3972-4014, January 17, 2013, at https://www.ftc.gov/system/files/2012-31341.pdf. The Children's Online Privacy Protection Act (COPPA) created notice, consent, and security requirements for data collected by operators of online services directed to children under 13 years of age (15 U.S.C. §§6501-6506).

[35] FTC Chairwoman Edith Ramirez, "Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control," keynote address presented at the Technology Policy Institute Aspen Forum, Aspen, CO, August 22, 2016, at https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf.

[36] For example, this report does not discuss data collection through device sensors, such as motion or light sensors.

Figure 1. Overview of Selected Data Collection and Tracking Tools



Source: Congressional Research Service.

Notes: APIs = application programming interfaces; SDKs = software development kits; and VPNs = virtual private networks.

Cookies

A *cookie* is a small information file stored on a user's device when a user visits a website.[37] Cookies can store a wide range of information, including a persistent identifier known as a cookie ID.[38] The lifetime of a cookie can vary; some cookies are deleted as soon as the user leaves a website, while others remain on the user's device for a predetermined amount of time.

First-party cookies—created by a website visited by a user—can be used to personalize a website's features and may be necessary to provide certain services.[39] For example, a first-party cookie might save a user's preferred language setting or unpurchased items in a shopping cart. Data privacy concerns have focused primarily on third-party cookies, also called tracking cookies, which are created by an entity other than the operator of the website a user is visiting.[40] For example, if a user visits a website using a third-party advertising (ad) network, the third party can place cookies on the user's browser. Third-party cookies enable advertisers and websites to track user behavior and build user profiles in order to serve personalized ads.

Many websites serve ads from different ad networks, meaning multiple third parties can use and compare their cookies by combining data using cookie IDs.[41] This process, known as "cookie syncing," enables third parties that track users' online activities to merge data without users' knowledge.[42] Some studies have found that the majority of such third parties are involved in cookie syncing.[43]

Tracking Pixels

A *tracking pixel*—also called a pixel, marketing pixel, image tag, or tracking code—is a small piece of code that an operator can add to its website to collect and send data to a third party, typically an ad network that provides the pixel code. The code creates an "image" the size of a single pixel, the smallest unit of a digital image or graphic, that is not visible to users.[44] When a user visits a web page, their actions automatically trigger the pixel to send data to the pixel provider's servers. Pixels can be embedded in websites, ad banners, and emails.

Typically, Pixels are used for online advertising to collect data on each website user, including user behavior, such as clicks or searches, IP address, and device model and browser information.

---

[37] Mozilla, "Cookies - Information that Websites Store on Your Computer," at https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer; and CloudFlare, "What Are Cookies? Cookies Definition," at https://www.cloudflare.com/learning/privacy/what-are-cookies/.

[38] Ibid. and FTC, "Internet Cookies," at https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies.

[39] Aaron Cahn et al., "An Empirical Study of Web Cookies," presented at the 25th International World Wide Web Conference, Montréal, Québec, Canada, 2016, pp. 891-901, at https://doi.org/10.1145/2872427.2882991.

[40] Steven Englehardt et al., "Cookies That Give You Away: The Surveillance Implications of Web Tracking," presented at the 24th International World Wide Web Conference, Florence, Italy, May 2015, at https://doi.org/10.1145/2736277.2741679.

[41] Cyphers and Gebhart, "Behind the One-Way Mirror."

[42] Steven Englehardt and Arvind Narayanan, "Online Tracking."

[43] Ibid.

[44] Techopedia, "Pixel," last updated August 31, 2020, at https://www.techopedia.com/definition/24012/pixel. For the remainder of this report, references to "pixel" are "tracking pixels." "What Is a Tracking Pixel and Can Strangers Really Spy on Me Through Email?," *The Verge*, July 3, 2019, at https://www.theverge.com/2019/7/3/20681508/tracking-pixel-email-spying-superhuman-web-beacon-open-tracking-read-receipts-location.

Data are sent to the provider of the tracking pixel (e.g., Meta Pixel, TikTok Pixel),[45] which can be used to target ads to specific users and obtain metrics on the efficacy of ads.

Pixels are often used in combination with other data collection and tracking tools, such as first- and third-party cookies. For example, Meta has stated that its pixel relies on Facebook cookies, which enable Meta to match a company's website visitors to their respective Facebook accounts.[46] Additionally, if Meta Pixel is present on a website, Meta can then place a first-party cookie on the user, expanding its data collection tools.[47] Web browsers cannot disable pixels easily, unlike cookies, because they send data directly to the pixel provider's servers.

In recent years, pixels have become increasingly popular as an alternative to tracking cookies. In 2018, Meta CEO Mark Zuckerberg testified that there were more than two million of its pixels installed on websites;[48] the number has likely grown since. One investigation found that 30% of the 100,000 most popular websites embed Meta Pixel.[49]

Privacy advocates have criticized the use of pixels for sharing sensitive user information without users' knowledge and potentially violating data privacy laws.[50] For example, in 2022, the news outlet *MarkUp* found that Meta collects sensitive user data through Meta Pixels embedded in the websites of hospitals, crisis pregnancy centers, and federal government agencies.[51] Another investigation found that Meta Pixel and TikTok Pixel collect data from thousands of popular websites before a user submits information to the website via an online form, such as signing in or signing up for a service.[52] These pixels collected personal information, including email addresses and passwords, even if the user never submitted the form or provided consent.[53]

Device and Browser Fingerprinting

Device and browser fingerprinting is a process to collect and combine a variety of data (e.g., device or browser properties) to uniquely identify and track a particular device, thereby tracking

[45] Meta, "What Is Meta Pixel," at https://www.facebook.com/business/tools/meta-pixel; TikTok, Business Help Center, "About TikTok Pixel," at https://ads.tiktok.com/help/article?aid=9663; and Google Developers, "Tag Setup Guides: Overview," at https://developers.google.com/tag-platform/devguides.

[46] Meta for Developers, "Get Started," at https://developers.facebook.com/docs/meta-pixel/get-started; and U.K. CMA, *Online Platforms and Digital Advertising*.

[47] Kerry Flynn, "WTF Are Facebook's First-Party Cookies for Pixel?," *DigiDay*, October 9, 2018, at https://digiday.com/marketing/wtf-what-are-facebooks-first-party-cookies-pixel/.

[48] Senate Committee on Commerce, Science, and Transportation, "Facebook, Social Media Privacy, and the Use and Abuse of Data," April 10, 2018, at https://www.commerce.senate.gov/services/files/9d8e069d-2670-4530-bcdc-d3a63a8831c4.

[49] Surya Mattu and Aaron Sankin, "How We Built a Real-Time Privacy Inspector," *The Markup,* September 22, 2020, at https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector.

[50] Skye Witley, "Meta Pixel's Video Tracking Spurs Wave of Data Privacy Suits," *Bloomberg Law*, October 13, 2022.

[51] Todd Feathers et al., "Facebook Is Receiving Sensitive Medical Information from Hospital Websites," *The Markup,* June 16, 2022, at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites; Surya Mattu and Colin Lecher, "Applied for Student Aid Online? Facebook Saw You," *The Markup,* April 28, 2022, at https://themarkup.org/pixel-hunt/2022/04/28/applied-for-student-aid-online-facebook-saw-you; and Grace Oldham and Dhruv Mehrotra, "Pixel Hunt Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients," *The Markup*, June 15, 2022, at https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

[52] Lily Hay Newman, "Thousands of Popular Websites See What You Type—Before You Hit Submit," *Wired*, May 11, 2022, at https://www.wired.com/story/leaky-forms-keyloggers-meta-tiktok-pixel-study/.

[53] Asuman Senol et al., "Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission," presented at the 31st USENIX Security Symposium, Boston, MA, August 10-12, 2022, at https://homes.esat.kuleuven.be/~asenol/leaky-forms/leaky-forms-usenix-sec22.pdf.

the user.[54] In fingerprinting, a piece of code on a website typically collects user data—such as screen size, screen resolution, browser information, and operating system details—to identify and track users. A fingerprinting algorithm combines the data to create a "fingerprint" or identifier.[55] Commercial fingerprinting companies can provide the code to websites and store the results as a service.[56]

One study found that 80%-90% of desktop fingerprints and about 80% of mobile device fingerprints are unique, suggesting that the majority of users' browsers are uniquely identifiable.[57] Another investigation found that at least one-third of the 500 most popular websites collected details about user devices for fingerprinting.[58] Even when an individual uses "private browsing mode, a virtual private network (VPN), or clears third-party cookies, these websites were still able to successfully track users."[59] Unlike cookies or other data collection tools that can be "reset," fingerprints typically last as long as the user has the same hardware and software.

Application Programming Interfaces

An API is a piece of software that enables one software program to communicate and interact with another, typically to share data and make certain features or tools available.[60] Data communications between apps and operating systems, between apps and websites, and between apps often use APIs. APIs can connect the platforms and share data in a form that the developers of a separate website or app can easily use, sometimes for tracking users as they move across platforms.

Data collection and sharing user data with third parties, including advertisers, may use some APIs. For example, Meta and Google offer analytics APIs to help operators gain information about visitors to their websites based on their Google or Meta account and other data, allowing all the companies involved to build detailed user profiles for targeted advertising. Third parties can take advantage of APIs to extract consumer data deceptively. For example, in 2018, the company Cambridge Analytica collected user data through Facebook's API without users' knowledge or consent to build voter profiles (discussed later in "Federal Trade Commission Enforcement of Consumer Data Collection").

Operators of websites and apps have various incentives to use or provide certain APIs. Small operators might use APIs offered by large operators to improve their website or app and offer

[54] Information Commissioner's Office, "What Are Cookies and Similar Technologies?," at https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-cookies-and-similar-technologies; and Pierre Laperdrix et al., "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints," presented at the 37th IEEE Symposium on Security and Privacy, San Jose, CA, May 2016, pp. 878-894, at https://hal.inria.fr/hal-01285470v2.

[55] A fingerprinting algorithm inputs data and produces a shorter string that identifies the data.

[56] Nick Nikiforakis et al., "Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting," presented at the 34th IEEE Symposium on Security and Privacy, San Francisco, CA, May 2013, at https://doi.org/10.1109/SP.2013.43.

[57] Peter Eckersley, "How Unique Is Your Web Browser?," presented at the 10th Privacy Enhancing Technologies Symposium, Berlin, Germany, 2010, at https://doi.org/10.1007/978-3-642-14527-8_1.

[58] Geoffrey A. Fowler, "Think You're Anonymous Online? A Third of Popular Websites Are 'Fingerprinting' You," *Washington Post*, October 31, 2019, at https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/.

[59] Ibid.

[60] For example, apps use application programming interfaces (APIs) to access and send service requests to the operating system of a mobile device. Thus, all apps need these kinds of APIs to be compatible with an operating system. Cameron Russell et al., "APIs and Your Privacy," *SSRN*, February 5, 2019, at http://dx.doi.org/10.2139/ssrn.3328825.

special features, and large operators might offer APIs to expand their consumer data collection and integrate their services with others. For example, one of YouTube's APIs allows other developers to embed YouTube videos on their websites and apps.[61] Large companies may collect data and track users across different contexts through various APIs. Facebook, Google, and Apple offer login APIs that allow users to use their accounts with the respective companies to log in to a different website or app. These APIs may present privacy and cybersecurity concerns, as each company may be able to control user data and access to hundreds of other websites and apps.[62] APIs can also evade certain anti-tracking software. For example, Meta's Conversions API enables advertisers to share user data and online activity, even if a user has an ad blocker to block third-party cookie tracking.[63]

Through sharing data and functionality, APIs can enable interoperable and interactive online services, which may benefit competition but create privacy risks. Some APIs can increase competition by helping companies innovate and interoperate with other services.[64] Some large companies have been accused of stifling competition by revoking competitors' access to their APIs. For example, Facebook disabled Vine's (then owned by Twitter) access to a friend-finding API, which allowed users to find their Facebook friends on Vine; it also disabled Twitter's access to a cross-posting API, which allowed users to post on Facebook and Twitter simultaneously.[65] According to internal company documents released by the UK Parliament in 2018, Facebook executives, including CEO Mark Zuckerberg, intentionally severed Twitter's access to Facebook's friend-finding API.[66] Some researchers have argued that dominant companies that are vertically integrated, operating as a "supplier" and as a direct competitor, no longer have an incentive to provide potential competitors access to their APIs.[67]

Software Development Kits

An SDK is a set of software tools and code—often containing APIs[68]—that entities can use to develop and integrate websites and apps with other services.[69] This section focuses solely on SDKs found in mobile devices due to their increasing adoption to track users in mobile ecosystems. Google and Meta are two of the most popular SDK providers on both Android and

[61] Ibid.

[62] Ibid.

[63] Meta, Business Help Center, "About Conversions API," at https://www.facebook.com/business/help/2041148702652965?id=818859032317965.

[64] Becky Chao and Ross Schulman, *Promoting Platform Interoperability*, New America, Open Technology Institute, last updated May 13, 2020, at https://www.newamerica.org/oti/reports/promoting-platform-interoperability/ (hereinafter Chao and Schulman, *Promoting Platform Interoperability*).

[65] U.K. CMA, "Appendix J: Facebook Platform and API Access," *Online Platforms and Digital Advertising*, last updated July 1, 2020, at https://assets.publishing.service.gov.uk/media/5efb1dd2d3bf7f7699160dd6/Appendix_J_-_Facebook_Platform_and_API_access_v4.pdf.

[66] Ibid.; and Adi Robertson, "Mark Zuckerberg Personally Approved Cutting Off Vine's Friend-Finding Feature," *The Verge*, December 5, 2018, at https://www.theverge.com/2018/12/5/18127202/mark-zuckerberg-facebook-vine-friends-api-block-parliament-documents.

[67] Chao and Schulman, *Promoting Platform Interoperability*.

[68] For example, one of Meta's software development kits (SDKs) includes login APIs and cross-posting APIs.

[69] U.K. CMA, "Appendix F: The Role of Data in Digital Advertising," *Online Platforms and Digital Advertising*; and Linda Rosencrance, "Software Development Kit (SDK)," TechTarget, last updated July 2019, at https://www.techtarget.com/whatis/definition/software-developers-kit-SDK (hereinafter Rosencrance, "SDK").

iOS, according to a 2019 report.[70] Google had SDKs in over 85% of the most popular apps on Google Play Store, and Facebook had the second highest with SDKs in over 40% of these apps.[71]

Some SDKs are required to develop an app for a particular operating system. These SDKs are necessary for mobile ecosystems to function and not commonly used for mobile tracking. Other SDKs specifically track and collect user data across mobile apps, including users who have never accessed the SDK providers' consumer-facing products. Consumers are often unaware of the integration of third-party SDKs in apps or that they collect their data. When users interact with a mobile app, they may unknowingly share many kinds of data with all the third-party SDKs integrated in the app.

SDKs are extremely common, in part because they make it faster and easier to develop apps by reducing the amount of original code needed.[72] Developers can also use ad network SDKs to obtain revenue. For example, apps that use Meta's advertising SDK can send targeted ads to users based not only on the user's interaction with the app but also on data that Meta collects from other sources.[73] This benefit may incentivize developers to use Meta's SDKs while simultaneously expanding Meta's own data collection capabilities. Some app developers may be unaware of the data that third-party SDKs collect, particularly if the data are not essential for the app's functionality.[74] For example, a 2020 investigation found that Zoom's iOS mobile app was sharing users' data with Meta through one of the Facebook SDKs, even if the user did not have a Facebook account.[75] Zoom removed the Facebook SDK after learning that it was collecting device information that was unnecessary for Zoom's purposes.

Anti-Tracking Tools from Intermediaries

Some intermediaries—such as web browsers and operating systems—permit users to limit the data collected by websites, apps, and third parties. Most web browsers offer "private browsing" or "incognito" modes that allow users to refuse cookies. However, other tools can still track users, such as pixels, fingerprinting, and APIs. Some operating systems on mobile devices provide an "opt-out" setting that limits tracking on the device, but most users do not use this setting.[76] Nevertheless, some studies have found that most individuals would prefer to opt out of third-party cookies. One study found that when users are given the option to opt out of third-party cookies, less than 0.1% of respondents agreed to be tracked (i.e., 99.9% opt out) for personalization and advertising.[77]

---

[70] Cyphers and Gebhart, "Behind the One-Way Mirror."

[71] U.K. CMA, "Appendix F: The Role of Data in Digital Advertising," *Online Platforms and Digital Advertising*.

[72] Rosencrance, "SDK"; and Charlie Warzel, "The Loophole That Turns Your Apps into Spies," *New York Times*, September 24, 2019, at https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html (hereinafter Warzel, "The Loophole").

[73] Sara Morrison, "The Hidden Trackers in Your Phone, Explained," *Vox*, July 8, 2020, at https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

[74] Warzel, "The Loophole."

[75] Joseph Cox, "Zoom Removes Code That Sends Data to Facebook," *Vice*, March 27, 2020, at https://www.vice.com/en/article/z3b745/zoom-removes-code-that-sends-data-to-facebook.

[76] Thomas Germain, "What the New iPhone Tracking Setting Means, and What to Do When You See It," *Consumer Reports*, April 26, 2021, at https://www.consumerreports.org/privacy/what-the-new-iphone-tracking-setting-means-and-what-to-do-when-you-see-it-a8018618269/.

[77] Christine Utz et al., "(Un)informed Consent: Studying GDPR Consent Notices in the Field," presented at the 26th ACM SIGSAC Conference on Computer and Communications Security, London, U.K., November 11-15 2019, at https://doi.org/10.1145/3319535.3354212.

Some web browsers, including Firefox and Safari, have banned third-party tracking cookies. In 2019, Google announced plans to "develop new standards that advance privacy, while continuing to support free access to content" by replacing tracking tools, such as third-party cookies and fingerprinting, with a new set of tools for targeted advertising—collectively known as the Privacy Sandbox.[78] This proposal raised competition concerns from antitrust enforcers in the United States and Europe, who argued the Privacy Sandbox could disadvantage Google's ad competitors by denying them access to user data that Google still collects.[79] Google has delayed implementing the Privacy Sandbox until 2024.[80] Some commentators have argued that Google is delaying implementing its cookie ban because it could harm Google's advertising platform.[81]

Apple released an iOS update in April 2021 that required apps to ask for permission before tracking user activity.[82] Specifically, if users choose the option "Ask App Not to Track," their Apple IDFA would be withheld. An app analytics firm estimated that during the first month after the release of the update, the percentage of U.S. daily users who allowed apps to continue tracking them ranged from 2% to 6%.[83] Some commentators noted, however, that the update allows app providers to collect aggregated and "anonymized" data, such as a device's IP address,[84] and that Apple cannot prevent developers from tracking users with other identifiers, such as their email address or usage data.[85] Furthermore, some companies reportedly use other tools for data collection, such as device fingerprints, to circumvent the tracking permission requirement.[86]

---

[78] Google started exploring the possibility of phasing out third-party cookies from its Chrome browser in 2019. See Justin Schuh, "Building a More Private Web," Google, August 22, 2019, at https://www.blog.google/products/chrome/building-a-more-private-web. For Google's official announcement, see Anthony Chavez, "Expanding Testing for the Privacy Sandbox for the Web," Google, July 27, 2022, at https://blog.google/products/chrome/update-testing-privacy-sandbox-web/.

[79] European Commission, "Antitrust: Commission Opens Investigation into Possible Anticompetitive Conduct by Google in the Online Advertising Technology Sector," June 22, 2021, at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3143; U.K. CMA, "CMA to Investigate Google's 'Privacy Sandbox' Browser Changes," January 8, 2021, at https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes; and Mark MacCarthy, "Controversy over Google's Privacy Sandbox Shows Need for an Industry Regulator," Brookings, June 23, 2021, at https://www.brookings.edu/blog/techtank/2021/06/23/controversy-over-googles-privacy-sandbox-shows-need-for-an-industry-regulator/.

[80] Vinay Goel, "An Updated Timeline for Privacy Sandbox Milestones," Google, June 24, 2021, at https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/; and Kyle Wiggers, "Google Delays Move Away From Cookies in Chrome to 2024," *TechCrunch*, July 27, 2022, at https://techcrunch.com/2022/07/27/google-delays-move-away-from-cookies-in-chrome-to-2024/.

[81] See Sara Morrison, "Google's Plan to Get Rid of Cookies (Still) Isn't Going Well," *Vox*, July 27, 2022, at https://www.vox.com/recode/2021/6/24/22548700/google-cookies-ban-delay-floc-tracking.

[82] Apple, Apple Support, "If an App Asks to Track Your Activity," at https://support.apple.com/en-us/HT212025; and Apple, Apple App Store Developer, "User Privacy and Data Use," at https://developer.apple.com/app-store/user-privacy-and-data-use/.

[83] Estelle Laziuk, "iOS 14.5 Opt-In Rate - Daily Updates Since Launch," Flurry Analytics, April 29, 2021, at https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

[84] Patrick McGee, "Apple Reaches Quiet Truce Over iPhone Privacy Changes," *Financial Times*, December 8, 2021, at https://www.ft.com/content/69396795-f6e1-4624-95d8-121e4e5d7839; and Karl Bode, "Apple's 'Do Not Track' Button Is Privacy Theater," *TechDirt*, December 10, 2021, at https://www.techdirt.com/2021/12/10/apples-do-not-track-button-is-privacy-theater/.

[85] Thorin Klosowski, "We Checked 250 iPhone Apps—This Is How They're Tracking You," *New York Times*, May 6, 2021, at https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/.

[86] Sharon Terlep et al., "P&G Worked With China Trade Group on Tech to Sidestep Apple Privacy Rules," *Wall Street Journal*, April 8, 2021, at https://www.wsj.com/articles/p-g-worked-with-china-trade-group-on-tech-to-sidestep-apple-privacy-rules-11617902840.

In 2018, Google restricted ad buyer and ad agency access to its persistent identifier in its ad network DoubleClick ID, indicating that the identifier could be tied to sensitive user information.[87] However, restricting access to DoubleClick ID made it impossible to compare metrics from ads purchased in Google's ad network with those purchased from other intermediaries. In response, the U.K. Competition and Markets Authority (CMA) proposed mandating the creation of secure common user IDs to address competition concerns within digital advertising and to increase interoperability by ensuring adherence to common standards.[88] According to the CMA, market participants could assign a common digital ID to their own data for targeting and attribution purposes. The CMA also recognized potential privacy concerns that the proposal could raise, such as sharing data collected under the common user ID with third parties.

Some intermediaries can make it difficult for individuals to access anti-tracking tools. For example, Google has banned certain ad blocking apps and tracker blockers, some of which were reinstated,[89] from its app store for violating its policy prohibiting developers from interfering with, disrupting, or damaging devices and other apps.[90] In July 2022, Google announced updates to its app store policy, including allowing only VPN apps that use its proprietary VpnService interface and have VPN as its core functionality.[91] The updates prohibit VPN apps from collecting "personal and sensitive user data without prominent disclosure and consent," redirecting or manipulating "user traffic from other apps on a device for monetization purposes (for example, redirecting ad traffic through a country different than that of the user)," or manipulating "ads that can impact apps monetization."[92] These changes could increase user privacy but might also prevent some ad-blocking VPN apps.[93]

Intermediaries may be able to obtain a competitive advantage if they can collect data that others cannot access.[94] Some commentators have noted that a third-party cookie ban may have detrimental effects on competition in digital advertising by limiting the availability of data and

[87] U.K. CMA, "Appendix O: Measurement Issues in Digital Advertising," *Online Platforms and Digital Advertising*, last updated July 1, 2020, at https://assets.publishing.service.gov.uk/media/5fe495ede90e071205803986/Appendix_O_-_measurement_issues_in_digital_advertising_WEB.pdf.

[88] U.K. CMA, *Online Platforms and Digital Advertising*, last updated July 1, 2020.

[89] Colin Gibbs, "Google Boots Samsung-Backed Ad Blocker from Google Play," *Fierce Wireless*, February 4, 2016, at https://www.fiercewireless.com/wireless/google-boots-samsung-backed-ad-blocker-from-google-play; and Sarah Perez, "Google Reverses Its Decision to Ban Ad Blocking Apps from the Google Play Store," *TechCrunch*, February 9, 2016, at https://techcrunch.com/2016/02/09/google-reverses-its-decision-to-ban-ad-blocking-apps-from-the-google-play-store/.

[90] Google's Developer Distribution Agreement states, "You will not engage in any activity with Google Play, including making Your Products available via Google Play, that interferes with, disrupts, damages, or accesses in an unauthorized manner the devices, servers, networks, or other properties or services of any third party including, but not limited to, Google or any Authorized Provider." See Google Play, "Google Play Developer Distribution Agreement," effective as of November 17, 2020, at https://play.google.com/about/developer-distribution-agreement.html; and Google Play Console Help, "Device and Network Abuse," at https://support.google.com/googleplay/android-developer/answer/9888379?hl=en.

[91] Google Play, "Developer Program Policy: July 27, 2022 Announcement," at https://support.google.com/googleplay/android-developer/answer/12253906.

[92] Ibid.

[93] Ivan Mehta, "Google Announces New Play Store Policies Around Intrusive Ads, Impersonation and More," *TechCrunch*, July 28, 2022, at https://techcrunch.com/2022/07/28/google-announces-new-play-store-policies-around-intrusive-ads-impersonation-and-more/; and Craig Hale, "Google to Stop Android VPN Apps Blocking Ads," *TechRadar*, August 30, 2022, at https://www.techradar.com/news/google-to-stop-android-vpn-apps-blocking-ads.

[94] Ian Thomas, "Planning for Cookie-Less Future: How Browser and Mobile Privacy Changes Will Impact Marketing, Targeting, and Analytics," *Applied Marketing Analytics*, vol. 7, no. 1 (Summer 2021), pp. 6-16.

potential revenue from targeted ads for smaller competitors.[95] Smaller digital advertising platforms may need third-party cookies, while larger incumbents—such as Google and Facebook—may be able to rely on first-party data.[96]

Federal Trade Commission Enforcement of Consumer Data Collection

Although the United States does not have a comprehensive federal data protection law, the FTC has brought enforcement actions against companies for their consumer data collection practices under its authority to prevent "unfair or deceptive acts or practices in or affecting commerce."[97] The FTC's complaints have included allegations that companies handled personal information in ways that contradict their privacy policies, failed to adequately protect personal information from unauthorized access despite promises that that they would do so, and implemented default privacy settings that are difficult to change.[98] The FTC also enforces some laws related to data collection, such as COPPA.[99]

The FTC has taken enforcement actions against companies for allegedly using some of the data collection tools discussed in the "Anti-Tracking Tools from Intermediaries" section.[100] On August 29, 2022, it filed a complaint against the company Kochava, a data broker, for acquiring and selling consumers' precise geolocation data, allowing "entities to track consumers' movements to and from sensitive locations."[101] Other examples of complaints filed by the FTC that resulted in settlements include the following:

- In 2011, the FTC reached a settlement with ScanScout, an online advertiser, which allegedly misrepresented its data collection practices and consumers' ability to control collection of their data by deleting some cookies but continuing the use of others to track consumers.[102]
- In 2017, the FTC reached a settlement with Turn, a digital advertising company, for allegedly misrepresenting the extent to which it continued to track consumers online and through mobile apps after consumers opted out of such tracking.[103]

[95] Brian X. Chen and Daisuke Wakabayashi, "You're Still Being Tracked on the Internet, Just in a Different Way," *New York Times*, April 6, 2022, at https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html.

[96] House Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law, *Investigation of Competition in Digital Markets*, 2020, p. 230, at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf.

[97] 15 U.S.C. §45(a). For examples of enforcement actions taken by the FTC, see FTC, "Privacy and Security Enforcement," at https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[98] For more information, see CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[99] 15 U.S.C. §6501-6506. For enforcement actions the FTC has taken against companies for not complying with COPPA, see FTC, "Kids' Privacy (COPPA)," at https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa.

[100] See "Selected Data Collection and Tracking Tools."

[101] FTC, "FTC v Kochava, Inc.," last updated August 29, 2022, at https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc.

[102] FTC, "ScanScout, Inc., In the Matter of," last updated December 21, 2011, at https://www.ftc.gov/legal-library/browse/cases-proceedings/102-3185-scanscout-inc-matter.

[103] FTC, "Turn Inc., In the Matter of," last updated April 21, 2017, at https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3099-turn-inc-matter.

- In 2019, the FTC reached a settlement with data analytics company Cambridge Analytica, its then-CEO Alexander Nix, and app developer Aleksandr Kogan, who worked with Analytica. In its complaint, the FTC alleged that one of Facebook's APIs was used to deceptively collect data from millions of Facebook users without their permission.[104] The FTC also imposed a $5 billion penalty and additional requirements on Facebook for violating a settlement reached in 2012 that required Facebook obtain consumers' consent before sharing their data beyond its privacy settings.[105]
- In 2021, the FTC reached a settlement with Flo App, a women's health app, for disclosing millions of users' health information to various third parties using integrated SDKs.[106]

The FTC has also made statements and released reports regarding companies' uses of consumer data.[107] For example, in July 2022, after the U.S. Supreme Court issued its opinion in *Dobbs v. Jackson Women's Health Organization*,[108] the acting associate director of the FTC Division of Privacy and Identity Protection released a statement that location and information about consumers' health are among the most sensitive categories of data.[109] The statement warned companies that those "that make false claims about anonymization can expect to hear from the FTC" and that "the FTC does not tolerate companies that over-collect, indefinitely retain, or misuse consumer data."

On August 11, 2022, the FTC announced that it is "exploring rules to crack down on harmful commercial surveillance and lax data security."[110] It published an advance notice of proposed rulemaking and held a virtual meeting seeking public input, using that information to help

[104] FTC, "Cambridge Analytica, LLC, In the Matter of," last updated December 18, 2019, at https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter.

[105] FTC, "Facebook, Inc., In the Matter of," last updated April 28, 2020, at https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter. For more information about the settlement, see CRS Legal Sidebar LSB10338, *Facebook's $5 Billion Privacy Settlement with the Federal Trade Commission*, by Chris D. Linebaugh.

[106] FTC, "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations That It Misled Consumers About the Disclosure of Their Health Data," press release, January 13, 2021, at https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about.

[107] FTC, "Privacy and Security Enforcement," at https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[108] For more information about the case, see CRS Legal Sidebar LSB10768, *Supreme Court Rules No Constitutional Right to Abortion in Dobbs v. Jackson Women's Health Organization*, by Jon O. Shimabukuro.

[109] Kristin Cohen, "Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data," FTC, July 11, 2022, at https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use. For more information on laws protecting consumers' health information, see CRS Legal Sidebar LSB10797, *Protection of Health Information Under HIPAA and the FTC Act: A Comparison*, by Chris D. Linebaugh and Edward C. Liu; and CRS Legal Sidebar LSB10786, *Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview*, by Chris D. Linebaugh.

[110] For analysis of the advance notice of proposed rulemaking, see CRS Legal Sidebar LSB10839, *FTC Considers Adopting Commercial Surveillance and Data Security Rules*, by Chris D. Linebaugh. For the FTC announcement, see FTC, "FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices," August 11, 2022, at https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

determine whether new rules are necessary, the practices that might be addressed, and actions it might take to deter those practices.[111]

Potential Effects of Consumer Data Protection Requirements

The potential effects of a comprehensive federal data protection law would depend on how entities and consumers respond. For example, some bills introduced in the 117th Congress would require certain entities to inform individuals that their data are being collected and require entities to delete individuals' data if requested;[112] the effect of these requirements would depend on the number of users who request their data to be deleted.

This section discusses the potential effects of data protection requirements on website and app operators, specifically examining three possible scenarios: (1) prohibiting the collection of consumer data; (2) prohibiting the transfer, sale, or certain uses of consumer data; and (3) increasing transparency on the collection and use of consumer data.

Prohibit the Collection of Consumer Data

Prohibiting the collection of consumer data would provide the highest level of consumer data protection but could also prevent some operators from providing their services or degrade the quality of their services. For example, if data protection laws prohibit the collection of certain necessary location data,[113] navigation apps may no longer be able to provide real-time traffic information (e.g., notifying users that an accident has increased travel time and resulted in a faster alternate route). However, prohibiting the collection of nonessential data by navigation apps may have a minimal impact on navigation services.

Operators of existing navigation apps might be able to rely on historical data and analysis to continue providing some information—such as estimates for the time a route would take—that new entrants might be unable to provide. Thus, while prohibiting the collection of consumer data could encourage some operators to explore and develop other tools and technologies to obtain similar information from other sources, it also highlights the competitive advantage incumbents may have if consumer data is an integral component of developing their services.

Restricting data collection could have a significant effect on advertising. Some websites and apps collect consumer data to provide targeted ads, which often serve as a main source of revenue. Providers of targeted advertising services might experience a loss of revenue if they cannot offer other means of targeting ads. For example, the chief financial officer of Meta Platforms reportedly stated that the company expects to lose more than $10 billion in sales revenue because of Apple's "do-not-track" iOS update.[114]

[111] FTC, "Trade Regulation Rule on Commercial Surveillance and Data Security," 87 *Federal Register* 51273-51299, August 22, 2022; and FTC, "Commercial Surveillance and Data Security Public Forum," September 8, 2022, at https://www.ftc.gov/news-events/events/2022/09/commercial-surveillance-data-security-anpr-public-forum.

[112] For example, see the Online Privacy Act of 2021 (H.R. 6027) and the American Data Privacy and Protection Act (H.R. 8152).

[113] For example, GPS and other sensor data from a device may be necessary to determine a user's location.

[114] Daniel Newman, "Apple, Meta and the $10 Billion Impact of Privacy Changes," *Forbes*, February 10, 2022, at https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/.

Operators that rely on targeted advertising as their primary source of revenue might explore other options, such as charging users to access the app or using other forms of advertising. The potential effect on their revenue is unclear. An advertising technology company reportedly estimated that Facebook and Snap would lose about 13.2% of their revenue because of Apple's update, while YouTube and Twitter would lose 7.7% and 7.4%, respectively.[115] The estimated loss in revenue that Apple's update may cause might be partially due to advertisers potentially switching to platforms that would allow them to continue providing targeted ads; implementing a federal ban on the collection of consumer data might not have the same effect.

Some entities that stopped providing targeted ads in the European Union (EU) in response to the General Data Privacy Regulation (GDPR)[116]—the EU's comprehensive data protection law—did not experience a loss in revenue. For example, the *New York Times* reportedly started using contextual and geographical targeting,[117] rather than behavioral targeting,[118] and did not see a decline in revenue.[119] One study found that contextual advertising might be as cost-effective as behavioral targeted advertising.[120] Increased reliance on other forms of advertising, however, could increase competition to advertise on popular websites and apps, potentially making it difficult for smaller advertisers to gain visibility.

Prohibit the Transfer or Sale of Consumer Data

Prohibiting the transfer or sale of consumer data would provide users with greater control over which operators can access their data. It could discourage operators from collecting consumer data if they would not need it to provide their services. It might also provide greater data protection if it were to result in fewer operators having access to the data, although this would depend on various factors, such as the number of operators that consumers are willing to share their data with and the operators' level of data security.

Implementing restrictions on the transfer and sale of consumer data without restricting its collection and use could further entrench incumbents that have already collected large amounts of consumer data. It could encourage some of these incumbents to expand the markets they provide services in, potentially allowing these operators to obtain more data and expand the types of data they are able to collect. Furthermore, some consumers may be more willing to continue providing their data to a website or app for services they already use, rather than providing it to a new or

[115] Patrick McGee, "Snap, Facebook, Twitter and YouTube Lose Nearly $10bn After iPhone Privacy Changes," *Financial Times*, October 31, 2021, at https://www.ft.com/content/4c19e387-ee1a-41d8-8dd2-bc6c302ee58e.

[116] For more information, see CRS In Focus IF10896, *EU Data Protection Rules and U.S. Implications*, by Rachel F. Fefer and Kristin Archick;f and CRS Legal Sidebar LSB10846, *The EU-U.S. Data Privacy Framework: Background, Implementation, and Next Steps*, by Eric N. Holmes.

[117] *Contextual targeted advertising* describes ads targeted to an individual based on the content provided on a website or app.

[118] *Behavioral targeted advertising* describes ads targeted to an individual based on data about the individual's online behavior, such as the amount of time the individual was watching a video.

[119] Jessica Davies, "After GDPR, The *New York Times* Cut Off Ad Exchanges in Europe—and Kept Growing Ad Revenue," *Digiday*, January 16, 2019, at https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.

[120] Keach Hagey, "Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests," *Wall Street Journal*, May 29, 2019, at https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195.

unfamiliar one.[121] This could make it difficult for nascent websites and apps, as well as operators that currently do not have access to large amounts of data, to compete.[122]

Increase Transparency on the Collection and Use of Consumer Data

While some websites and apps provide general overviews of their data collection practices in privacy policies and other resources, detailed information—such as with whom data is shared or sold to—is typically not publicly available. Requiring operators and third parties to provide users with detailed information on their data collection and transfers—such as with a pop-up notification or a website that provides such information—could increase transparency about the collection and use of consumer data. Increased transparency could incentivize operators to adjust their current practices, particularly if it would heighten public scrutiny of the operators or discourage consumers from using the website or app.

Increasing transparency might not significantly alter consumer behavior, even if consumers must provide their consent before their data are collected. Most consumers do not read terms of service and privacy policies, in which operators provide general information about their data practices.[123] Some consumers may consider the services offered on a website or app valuable enough that they would continue sharing their data, even if they would prefer not to. Data privacy laws have led to a proliferation of notifications on websites providing users the opportunity to accept or reject cookies, causing some users to experience "digital resignation."[124] Even if operators provide additional information, such as with whom they share or sell a user's data, it might be difficult to track every entity that has access to that user's data. The aggregation and bundling of data, as well as the distribution of data to third parties, may present additional challenges for tracking user data.

Policy Considerations for Congress

Multiple federal laws create data protection obligations for specific types of information and entities. However, technological developments have enabled data collection that may provide similar information but are not be covered by existing laws. For example, operators of health-related websites and apps that are not associated with health care providers, health plans, or health care clearinghouses may not be subject to the data protection obligations required by the Health Insurance Portability and Accountability Act (HIPAA).[125] Similarly, operators of finance-related websites and apps that are not associated with banks may not be subject to the data protection obligations required by the Gramm-Leach-Bliley Act.[126]

[121] Alex Matthews and Catherine Tucker, *Privacy Policy and Competition*, Brookings, December 2019, at https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

[122] Ibid.

[123] U.K. CMA, *Online Platforms and Digital Advertising*, last updated July 1, 2020.

[124] *Digital resignation* is "the condition produced when people desire to control the information digital entities have about them but feel unable to do so." Nora A. Draper and Joseph Turow, "The Corporate Cultivation of Digital Resignation," *New Media & Society*, vol. 21, no. 8 (2019), at https://doi.org/10.1177/1461444819833331; and Joe Nocera, "How Cookie Banners Backfired," *New York Times: DealBook Newsletter*, updated January 30, 2022, at https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html.

[125] CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh.

[126] Ibid.; CRS Report R46333, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, by Andrew P. Scott; and CRS Report R47104, *Big Tech in Financial Services*, by Paul Tierno.

Some data protection regulations implemented by states and foreign countries govern the use of some data collection tools discussed in this report. For example, the California Consumer Privacy Act (CCPA) requires companies that conduct business in California and serve California residents to disclose the use of certain cookies in their privacy policies and, under certain circumstances, to allow users to opt out of the sale of their cookie-related data to third parties.[127] The CCPA does not mandate cookie disclosure banners or require user consent prior to the use of cookies.[128] The CCPA also specifies cookies and pixels in its definition of *unique identifier*, which is included in the definition of *personal information*.[129] The EU's GDPR and ePrivacy Directive include requirements for websites and apps that serve EU residents to notify users if they use cookies, allow users to opt out of receiving some or all cookies, and allow users to use the bulk of an online service without receiving cookies.[130] The results of studies examining the effect of GDPR on the use of cookies are mixed. Some studies find a decline in the use of cookies, while others find that few websites meet the minimum requirements.[131]

If Congress chooses not to pursue legislative action, then ongoing efforts by states, federal agencies, and intermediaries may determine standards for data protection in the United States, including the following:

- Five states—California, Colorado, Connecticut, Utah, and Virginia—have passed consumer data protection laws.[132]
- The FTC is considering whether it will implement new rules on data collection and security to protect consumers' data and privacy.[133]

[127] See the California Consumer Privacy Act of 2018, at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; and Amanda Lawrence et al., "Website Cookies and Privacy—GDPR, CCPA, and Evolving Standards for Online Consent," *Bloomberg Law*, November 14, 2019, at https://news.bloomberglaw.com/privacy-and-data-security/insight-website-cookies-and-privacy-gdpr-ccpa-and-evolving-standards-for-online-consent.

[128] David Zetoony et al., *California Consumer Privacy Act (CCPA): Answers to The Most Frequently Asked Questions Concerning Cookies and AdTech*, Bryan Cave Leighton Paisner LLP, February 2020, at https://ccpa-info.com/wp-content/uploads/2019/08/Handbook-of-FAQs-Cookies.pdf.

[129] Ibid.

[130] Richie Koch, "Cookies, the GDPR, and the ePrivacy Directive," GDPR.EU, at https://gdpr.eu/cookies/.

[131] Martin Degeling et al., "We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy," *Informatik Spektrum*, vol. 42 (2019), pp. 345-346, at https://doi.org/10.1007/s00287-019-01201-1; Adrian Dabrowski et al., "Measuring Cookies and Web Privacy in a Post-GDPR World," *Passive and Active Measurement*, vol. 11419 (2019), pp. 258-270, at https://doi.org/10.1007/978-3-030-15986-3_17; and Midas Nouwens et al., "Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence," presented at the CHI '20 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, April 25-30, 2020, at https://doi.org/10.48550/arXiv.2001.02479.

[132] See the California Consumer Privacy Act of 2018, at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; the Colorado Privacy Act, at https://leg.colorado.gov/sites/default/files/images/olls/crs2021-title-06.pdf#page=127; An Act Concerning Personal Data Privacy and Online Monitoring, at https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF; the Utah Consumer Privacy Act, at https://le.utah.gov/xcode/Title13/Chapter61/13-61.html; and the Consumer Data Protection Act, at https://law.lis.virginia.gov/vacode/title59.1/chapter53/.

[133] For more information about the FTC's rulemaking authority, see FTC, "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," revised May 2021, at https://www.ftc.gov/about-ftc/mission/enforcement-authority.

- Federal Communications Commission Chair Jessica Rosenworcel sent letters to the top 15 mobile providers requesting information about their data retention and data privacy policies and shared their responses.[134]
- The Consumer Financial Protection Bureau is considering rulemaking proposals to strengthen consumers' access to and control over their financial data.[135]
- Some intermediaries are implementing policies that limit data other entities can access.

If Congress chooses to pursue legislative action, it may consider the following:

- **Would legislation broadly address consumer data collection or focus on specific types of data?** Some bills introduced in the 117th Congress include additional requirements on data collection and use in sensitive categories, such as biometric data and PII.[136] Depending on the restrictions imposed, it may be possible to infer this information using other data that are seemingly less sensitive by using data collection and tracking tools.
- **Would legislation implement requirements for operators—such as restricting or increasing transparency of data collection, or prohibiting the transfer or sale of data—or allow consumers to determine which entities can receive their data?** Policymakers could create a privacy-by-default contractual regime that operators would need to follow—except in cases where consumers explicitly choose to provide their data—as suggested by the Biden Administration and other commentators.[137] Alternatively, operators could be required to allow consumers to "opt out" of data collection. If a limited number of consumers choose not to provide their data, they may benefit from operators improving their services using other consumers' information.
- **Would federal legislation preempt state laws and, if so, which laws and to what extent?** Without preemption, it may be difficult and costly for operators, particularly smaller and nascent ones, to comply, especially if some laws would create inconsistent regulations.[138] Several U.S. federal statutes related to privacy do not preempt state laws, and preemption could prevent states from

[134] Federal Communications Commission (FCC), "Rosenworcel Probes Mobile Carriers on Data Privacy Practices," July 19, 2022, at https://www.fcc.gov/document/rosenworcel-probes-mobile-carriers-data-privacy-practices; and FCC, "Rosenworcel Shares Mobile Carrier Responses to Data Privacy Probe," August 25, 2022, at https://www.fcc.gov/document/rosenworcel-shares-mobile-carrier-responses-data-privacy-probe.

[135] Consumer Financial Protection Bureau (CFPB), "CFPB Kicks Off Personal Financial Data Rights Rulemaking," October 27, 2022, at https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-personal-financial-data-rights-rulemaking/.

[136] For example, the American Data Privacy and Protection Act (H.R. 8152) includes biometric information, genetic information, and precise geolocation data under "sensitive data." Biometric information includes fingerprints, iris or retina scans, and facial or hand mapping.

[137] Stigler Committee on Digital Platforms, 2019; and White House, OSTP, "Blueprint for an AI Bill of Rights: Data Privacy," October 4, 2022, at https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/.

[138] Peter Swire, "U.S. Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws," IAPP, January 9, 2019, at https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/ (Swire, "U.S. Federal Privacy"); and Cameron Kerry et al., *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, Brookings, June 2020, at https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf (hereinafter Kerry et al., *Bridging the Gaps*).

implementing stricter laws and enforcement of existing privacy-related state laws.[139]

- **Would legislation include a private right of action?** Individuals filing suit could increase enforcement of the law, particularly for individual harms, since it may be difficult for a single federal agency to address every case in which an individual is harmed.[140] Including a private right of action could also lead to frivolous lawsuits, which may be particularly burdensome for small and nascent operators.[141] Some commentators have recommended a compromise, such as including a private right of action but incorporating a review of potential cases and limiting or setting tiers for damages, depending on the level of harm.[142]
- **What are the potential unintended effects?** One study estimates that the EU's GDPR led to over one-third of available apps on Google Play Store exiting and a 47.2% reduction in the rate of entry of new apps.[143] Another study found that consumers made use of the opt-out capabilities provided by GDPR but that the consumers who chose to opt out were primarily those who used other data protection measures offered by browsers, such as cookie blockers and private browsing.[144]

[139] Swire, "U.S. Federal Privacy"; and Hayley Tsukayama, "Federal Preemption of State Privacy Law Hurts Everyone," EFF, July 28, 2022, at https://www.eff.org/deeplinks/2022/07/federal-preemption-state-privacy-law-hurts-everyone.

[140] Becky Chao, Eric Null, and Claire Park, *Enforcing a New Privacy Law: A Private Right of Action Is Key to Ensuring That Consumers Have Their Own Avenue for Redress*, New America, Open Technology Institute, last updated November 20, 2019, at https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress/.

[141] Neil Bradley, "U.S. Chamber Letter on National Privacy Legislation," U.S. Chamber of Commerce, May 31, 2022, at https://www.uschamber.com/technology/data-privacy/u-s-chamber-letter-on-national-privacy-legislation.

[142] Kerry et al., *Bridging the Gaps*; and Paula Bruening, "How to End the Deadlock on the Private Right of Action," IAPP, January 20, 2022, at https://iapp.org/news/a/how-to-end-the-deadlock-on-the-private-right-of-action/.

[143] Rebecca Janßen et al., *GDPR and the Lost Generation of Innovative Apps*, National Bureau of Economic Research (NBER), Working Paper 30028, May 2022, at http://www.nber.org/papers/w30028.

[144] Guy Aridor, Yeon-Koo Che, and Tobias Salz, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, NBER, Working Paper no. 26900, May 2022, at http://www.nber.org/papers/w26900.

Author Information

Clare Y. Cho
Specialist in Industrial Organization and Business Policy

Ling Zhu
Analyst in Telecommunications Policy

Acknowledgments

Kristen E. Busch, former CRS Analyst in Science and Technology Policy, contributed to the original version of this report.

Disclaimer