

Seton Hall University

eRepository @ Seton Hall

Law School Student Scholarship

Seton Hall Law

2021

The California Consumer Privacy Act and its Impact on the Use of Data

Tyler Pewitt

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship



Part of the [Law Commons](#)

Tyler Pewitt

Introduction

In order to achieve success, modern-day firms must leverage all available resources to reach their goals. One such resource is data. Data may be used in a variety of contexts, from expanding marketing outreach to new clients to improving web site layouts. The expansion of data usage, however, poses significant risks to all companies small and large. These risks include hackers attempting to collect sensitive personally identifiable information (PII) to employees unintentionally disclosing client information.

In 2018, Alastair Mactaggart created the California Consumer Privacy Act (CCPA) Ballot referendum.¹ Signed by 629,000 Californians, the ballot initiative would provide comprehensive privacy rights to all Californians.² Before the ballot initiative could be voted on, the California state legislature responded by passing the California Consumer Privacy Act.³

The passing of the CCPA reflects a substantial increase in data protection legislation throughout the world, with the General Data Protection Regulation (GDPR) being most notable predecessor. The GDPR provides comprehensive privacy rights to all European Union citizens,

¹ See <https://oag.ca.gov/initiatives> (Last visited March 8th, 2020).

² In California, once a ballot initiative reaches the required threshold of signatures, it goes on the subsequent November ballot to be voted on by California voters.

³ California Consumer Privacy Act of 2018 (CCPA), AB 375.

such as consent requirements to process the PII of data subjects, the ability to delete any PII collected by a covered entity, and the right to access and correct any collected PII.⁴

Europe has long adopted a “comprehensive” approach to data protection. That is, the GDPR and its predecessors have applied to a wide variety of contexts such as health data, financial data, and workplace records. Under the GDPR, the collection and use of this information falls under its provisions.

The United States has adopted an entirely different approach to data protection. Known as the “sectorial” approach, the regime consists of industry-specific statutes. To illustrate, the Health Insurance Portability and Accountability Act (HIPAA) applies to the collection and disclosure of personal health information (PHI) by covered medical providers, insurers, and clearinghouses.⁵ The Fair Credit Reporting Act (FCRA) applies to the accurate reporting of consumer credit information by Consumer Reporting Agencies.⁶ The Electronic Communications Privacy Act (ECPA) governs law enforcement access to wire, oral, and electronic communications.⁷

At the state level, legislatures are now recognizing broadly defined privacy rights for internet users. In addition to California, states such as Washington, Nevada, New Jersey, New York, and New Mexico have all enacted or are in the process of enacting comprehensive data privacy laws.⁸ While no federal legislation has officially passed, members of Congress have submitted numerous proposals.⁹

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

⁵ Health Insurance Portability and Accountability Act, 42 U.S.C. §1320.

⁶ Fair Credit Reporting Act, 15 U.S.C. § 1681.

⁷ Electronic Communications Privacy Act, 18 U.S.C. § 2518.

⁸ Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, International Association of Privacy Professionals (Apr. 18, 2019), <https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/>.

⁹ One recent proposal called for a national consumer right to data minimization, security, correction, and deletion. Consumer Online Privacy Rights Act, 116th Cong. (2019).

While the data practices of large technology companies such as Google, Facebook, and Amazon have been the driving force behind these legislative efforts, these companies are not the only entities affected. Businesses small and large that collect high amounts of PII may also be obligated to spend significant capital to comply with the upcoming flurry of state privacy laws. The goal of this project is to provide a general overview of the CCPA and how the new legislation will impact the data collection and storage practices of covered entities.

In sum, this paper will discuss the following three topics: (1) an overview of the CCPA, including what consumer information is protected and what rights are provided to Californians with respect to their PII; (2) the CCPA's impact on data collection; and 3) the CCPA's impact on data storage.

An Overview of the California Consumer Privacy Act

a. Covered Entities and Protected Data

To qualify as a covered entity under the CCPA, the entity must do business in California and must fall under one of the following three categories: (1) The business has an annual gross revenue exceeding twenty-five million dollars; (2) alone or in combination, annually buys, sells, shares, or receives (for commercial purposes) the PII of 50,000 or more Californian consumers, households, or devices; or (3) receives 50% or more of its annual revenues by selling consumer PII.¹⁰

Protected PII under the CCPA is “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly, or indirectly, with a particular consumer or household.”¹¹ Examples include, but are not limited to, real names, social

¹⁰ CCPA, Cal Civ. Code 1798.140(c)(1).

¹¹ Id. at 1798.140(o).

security numbers, email addresses, Internet Protocol addresses, biometric information, and geolocation data.¹²

b. The Right to Notice

Any business that collects consumer PII must, at or before the point of collection, inform consumers of the categories of PII collected in addition to the purposes for collecting those categories.¹³ Should the business use either additional categories of PII or use the PII for additional purposes, the business must furnish notice to the consumer.¹⁴

c. The Right to Opt-Out

Californians may request that covered entities that sell¹⁵ their PII to third parties stop the practice entirely,¹⁶ otherwise known as the right to “opt-out.” In order for covered entities to comply with this provision, a business’s webpage must display a hyperlink entitled “Do Not Sell my Personal Information.”¹⁷ Once an opt-out request is received, businesses must honor the choice for at least 12 months. Once this period has expired, a business may make a request to the consumer to authorize the sale of PII.¹⁸

¹² Id.

¹³ Id. at 1798.100 (b). To illustrate in the context of cookie-based data collection, websites often use “cookie banners” to provide notice to users regarding the data collection as soon as they visit the site. See Dan Storbaek, *CCPA and Cookies. What do I need to know?*, Secure Privacy (June 24, 2019), <https://secureprivacy.ai/ccpa-and-cookies-what-do-i-need-to-know/>. This would be considered notice “at or before the point of collection.”

¹⁴ Id.

¹⁵ The CCPA defines a “sale” of PI to include “releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally . . . [to a] third party for monetary or other valuable consideration.” CCPA, Cal. Civ. Code 1798.140(t)(1).

¹⁶ Id. at 1798.120(a).

¹⁷ CCPA, Cal Civ. Code 1798.135(a)(1).

¹⁸ Id. at 1798.135(a)(B)(5).

Notwithstanding this opt-out provision, businesses may, under certain circumstances, be obligated to comply with opt-in requirements, similar to that found in the GDPR.¹⁹ If a business has actual knowledge that a consumer is younger than 16 years old, the business is prohibited from selling the consumer's PII.²⁰ For consumers between the ages of 13 and 16, covered entities must receive express consent to engage in the sale of consumer PII. For consumers less than 13 years old, the consumer's parent or guardian must opt-in to the transaction.²¹

*d. The Right to Disclosures*²²

Californians have the right to request a number of disclosures from covered entities under the CCPA. These disclosures include: (1) the categories of PII collected by the business; (2) categories of sources from which the PII was collected from; (3) the business or commercial purpose for collecting or selling the PII; (4) categories of third parties who have received the consumer's PII; and (5) specific pieces of PII that the business has collected on the consumer.²³ These disclosures may only be made by the covered entity upon receiving a verifiable request from the consumer.²⁴ Once the consumer is identified as the owner of the information, businesses must respond to the consumer within a 45-day period.²⁵ This period can be extended to an additional 45 days so long as the business furnishes notice and provides an explanation to the consumer as to why an extension is necessary.²⁶

e. The Right to Deletion (or the Right to be Forgotten)

¹⁹ General Data Protection Regulation, Art. 7 (2016).

²⁰ Id. at 1798.120(d).

²¹ Id.

²² This is distinguished from Section B, where notice is required irrespective of any consumer action. In comparison, rights to CCPA disclosures require a consumer request.

²³ Id. at 1798.115.

²⁴ CCPA, Cal Civ. Code 1798.135(a)(2).

²⁵ Id.

²⁶ Id.

Businesses must notify consumers of their right to delete any collected PII within the text of a business's privacy policy.²⁷ In order to have collected PII deleted by a business, a consumer must first submit a verifiable request.²⁸ Upon receipt of a verifiable request, both the business and any service provider holding the PII must delete the information. Notably, the right to deletion contains a number of significant exceptions. For example, to the extent that a business must fulfill its contractual obligations with the consumer, the business need not delete any PII necessary to fulfill the obligation.²⁹ If the business is utilizing the PII for an internal use, the business is not required to delete the PII upon request so long as the PII used is "reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."³⁰ Lastly, PII does not have to be deleted if used "in a lawful manner that is compatible with the context in which the consumer provided the information."³¹

f. The Right to Non-Discrimination

Should a consumer exercise any rights provided under the CCPA, she is nevertheless entitled to equal service and price.³² For example, any consumer that requests deletion of collected PII is entitled to the same quality of a particular good or service that any other consumer would be offered. However, a number of exceptions apply. For example, should a business delete the consumer's PII upon request, the business may offer a different quality of a good or service if the difference is reasonably related to the value of the consumer's data.³³

²⁷ Id. at 1798.105(b).

²⁸ Id. at 1798.105(c).

²⁹ Id. at 1798.105(d)(1).

³⁰ Id. at 1798.105(d)(7). This exception has also been referred to as the "legitimate interest" exception. Instead of deleting the consumer's PII, the business may instead limit its use to the specified purpose for which it was collected. Upon receiving a deletion request, the business may subsequently refrain from using that PII for additional, undisclosed purposes. *What Data is Exempt from Deletion under the CCPA?*, Sixfifty, <https://www.sixfifty.com/ccpa-exemptions/> (last accessed Apr. 2020).

³¹ Id. at 1798.105(d)(9).

³² CCPA, Cal Civ. Code 1798.125(a)(1)(A).

³³ Id. at 1798.125(a)(2).

g. Private Right of Action

The CCPA's private right of action is applicable in situations of "unauthorized access and exfiltration, theft, or disclosure" of the consumer's PII.³⁴ Should a business fail to properly notify a consumer of her CCPA privacy rights, refuse a deletion request, or otherwise fail to fulfill disclosure obligations, no private right of action is available against the violator.³⁵ Once the consumer identifies an unauthorized access and exfiltration, theft, or disclosure, the consumer must provide notice to the business of the specific CCPA provisions that have been violated.³⁶

However, the business is not immediately subject to a consumer's private right of action upon notification. Once the business is notified of the alleged CCPA violation, it has a total of 30 days to cure the violation and subsequently notify the consumer that the violation has been corrected.³⁷

With respect to damages, consumers may recover amounts not less than \$100 and no greater than \$750 per consumer per incident or actual damages, whichever total is greater. The consumer may also be entitled to injunctive or declaratory relief, or any other relief deemed proper.³⁸

CCPA's Impact on Data Collection

A firm with operational or financial goals will need a steady flow of data to properly measure the firm's progress.³⁹ In the aggregate, this data can provide a company with an

³⁴ Id. at 1798.150(a)(1).

³⁵ Private rights of action in light of data breaches are nothing new, insofar as state legislation is concerned. See Haw. Rev. Stat § 487N-1-4 (2006). See also 815 Ill. Comp Stat. Ann. 530/1-/30 (2006). No federal data breach law has been passed.

³⁶ CCPA, Cal Civ. Code 1798.150(b)(1).

³⁷ Id.

³⁸ Id.

³⁹ Dale Chang, *How Startups can use Data to grow Smarter*, (2016) <https://techcrunch.com/2016/10/15/how-startups-can-use-data-to-grow-smarter/> ("Based on my experience advising portfolio companies and consulting, I believe data-driven operations is the new table stakes for survival today.").

informative picture of the firm's growth and enable comparisons with other firms. Data is critical to applying contemporary management principles. From a housekeeping perspective, data sets help firms track employee performance and compensation, as well as other relationships between revenues and expenditures. Perhaps most notably, data collection may help in optimizing customer acquisition and retention as well as refining products.

Recall how the CCPA defines covered entities: any entity doing business in California that 1) has an annual gross revenue exceeding twenty-five million dollars; (2) alone or in combination, annually buys, sells, shares, or receives (for commercial purposes) the PI of 50,000 or more Californian consumers, households, or devices; or (3) receives 50% or more of annual revenues via the sale consumer PII. Even if a majority of firms fail to reach twenty-five million in gross revenue, many firms utilizing a data analytics program will nevertheless qualify under the second and third categories, respectively.

This section will first assess the CCPA's impact on data collection with a specific focus on cookie-based data collection. The discussion will then shift to a case study on how the CCPA is impacting the data collection practices of a startup located in California. Although it is yet to be determined, the CCPA may force covered entities to fundamentally change their data collection practices.

a. Data Collection under the CCPA

Collection under the CCPA is defined as "buying, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."⁴⁰ This definition includes both active and passive data collection.

⁴⁰ CCPA, Cal Civ. Code 1798.140(e). The California legislature passed AB 25 to exempt personal information collected from job applicants, employees, and contractors. However, the exemption expires on January 1st, 2021. An act to amend Sections 1798.130 and 1798.145 of the Civil Code, relating to consumer privacy, AB 25.

Active data collection generally requires user consent. Common forms of active data collection include market research questions.⁴¹ There are several notable limitations of active data collection from a business standpoint. Specifically, this data gathering technique is limited by both response frequencies on the part of the user and the amount of information relayed by the user. Lastly, the information provided is more subjective compared to the information gathered via passive data collection.⁴²

In comparison, passive data collection does not involve affirmative consent by the user. Passive data collection may involve the use of software and websites to collect information on user experience over a prolonged period of time. To a privacy advocate, passive data collection may be considered more invasive than active data collection, insofar as users may not be aware of the information they are providing in the course of passive data collection.⁴³

An effective illustration of passive data collection is the use of cookies. Cookies originate on websites visited by users. While the user is visiting the site, the cookie proceeds to capture the user's activities on the site. This allows the website to track user activity and subsequently store the data. However, variations of cookies may be distinguished. "Session" cookies have already been described. Session cookies are limited to tracking user activity while the user is on the website. "Persistent" cookies are more evasive – they remain active even when a user closes her

⁴¹ Esomar World Research Codes & Guidelines, *Passive Data Collection, Observation and Recording*, (2009) https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR_Codes-and-Guidelines_Passive_Data_Collection-Observation-and-Recording.pdf.

⁴² Id.

⁴³ Nicole A. Maher, et al., *Passive Data Collection and Use in Healthcare: A Systematic Review of Ethical Issues* (2019) ("Because of the passive nature of the data, participants may not be aware of the type, amount, or implications of the data that is collected . . . the knowledge derived from passive data and the associated implications cannot always be foreseen.").

browser. Lastly, “flash” or “zombie” cookies are designed to stay on a user’s device on a permanent basis and may remain despite user deletion.⁴⁴

Under the definition of personal information, the CCPA includes “internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a *consumer’s interaction with an Internet Web site, application, or advertisement*.”⁴⁵ Thus, information collected via cookies is protected under the CCPA, whether the cookies are classified as session, persistent, or flash cookies. Furthermore, businesses that collect personal information via cookies must, *at or before the point of collection*, inform consumers of the categories of personal information to be collected as well as the purpose for collecting such categories of personal information.⁴⁶

With respect to the use of cookies, the aforementioned CCPA requirements may significantly impact the use of the tracking technology, particularly for host websites and marketers that receive the data. For those businesses that employ cookie technology at the onset of a user’s interaction with a website, the CCPA requires that users, at or before the point that the cookie begins collecting data, receive notice of the collection. As of this writing, it is unclear what sort of notice would comply with the CCPA under these circumstances.⁴⁷

Notwithstanding the CCPA’s impact on a host website’s use of cookies, online marketers may be significantly impacted as well. While businesses will be required to provide notice to consumers before cookies collect personal information, marketers that subsequently purchase this data may see a reduction in their consumer data stockpile. This is because the CCPA allows

⁴⁴ For an example of a class action lawsuit against several companies employing flash cookies, see *LaCourt v. Specific Media, Inc.*, 2011 U.S. Dist. LEXIS 50543 (C.D. Cal. April 28, 2011).

⁴⁵ CCPA, Cal Civ. Code 1798.140(o)(2)(F). (emphasis added).

⁴⁶ *Id.* at 1798.100(b). (emphasis added).

⁴⁷ Upon entering a particular website, hosts commonly employ “cookie banners” to notify users of cookie data collection. But as we will discuss, it is unclear what data collection activities, and by whom, these notices cover.

consumers to direct a business that sells personal information to third parties to cease the transactions. If states continue to pass legislation similar to the CCPA, the expansion of consumer control over PII may diminish marketers' access to individualized data. This necessarily means that marketers will have to explore alternative means of collecting personal information online.⁴⁸

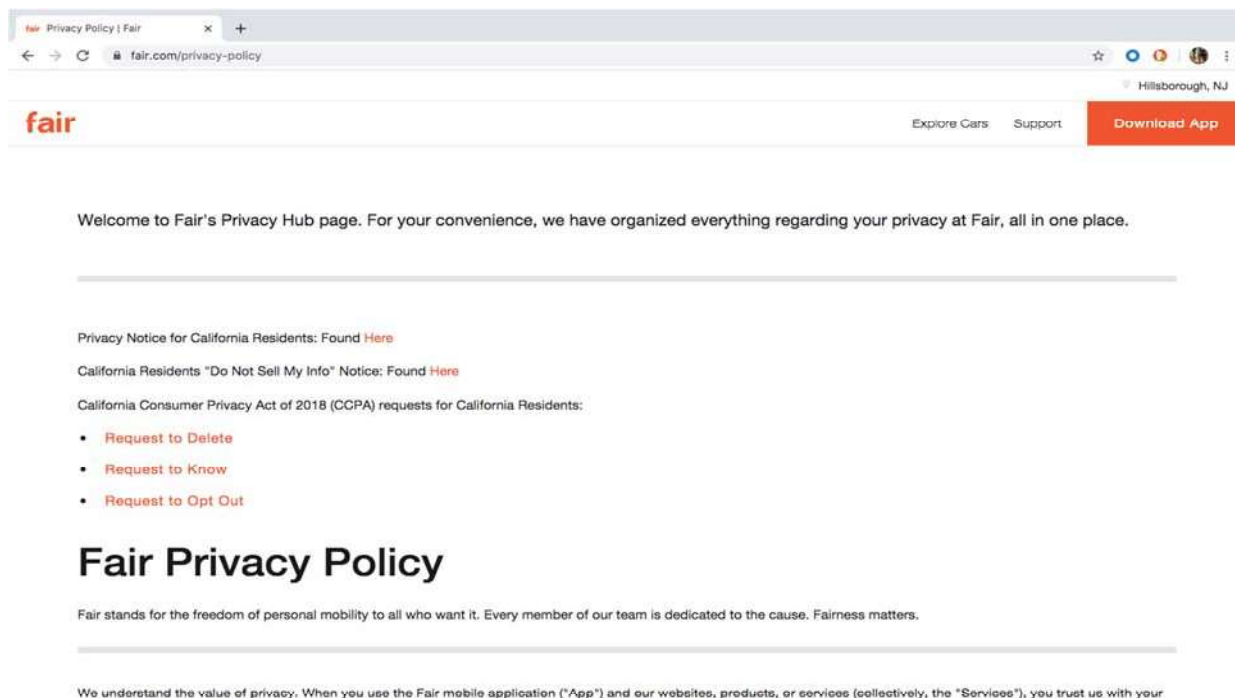
b. Fair and Cookie-Based Data Collection

It has already been discussed how the CCPA may broadly impact data collection. Whether engaged in active data collection in the form of surveying customers and clients or extracting individualized user data via cookie technology, the CCPA will require firms to audit and evolve these programs. This reality may be most apparent in the context of a startup's data collection program. Machine learning and other artificial intelligence technologies allow startups to analyze massive amounts of data in a variety of contexts. This section will discuss one startup's adaptation to the CCPA's data collection requirements.

Fair is a California-based startup that allows users to subscribe to used vehicles of their choice on a mobile application. Users select the vehicle of their choice and are able to pick up the chosen vehicle at a local dealership. To complete the transaction, Fair collects a user's license information as well as insurance information. Fair also assesses the user's credit in determining how much to charge the user for the vehicle subscription. Users are able to obtain flexible subscription terms for their vehicles, often paying monthly fees between \$300 to \$400.⁴⁹ The following image contains Fair's privacy policy:

⁴⁸ For an argument that the CCPA and legislation like it means the end of cookies, see Chad Pollitt, *What Digital Marketers Need to Know About California's New CCPA Law*, (2020) at <https://www.socialmediatoday.com/news/what-digital-marketers-need-to-know-about-californias-new-ccpa-law/570356/>.


⁴⁹ See Sue Callaway, *Driven: Behind the Rise, Stumble, and Rebirth of Fair and its car-buying app*, Los Angeles Times (March 11, 2020), <https://www.latimes.com/business/story/2020-03-11/fair-car-buying-app>.



The presentation of this privacy policy is known as a “top layered” approach. Top layered privacy policies are essentially bifurcated. That is, the “top layer” of the policy includes short descriptions pertaining to how the company collects, discloses, and otherwise utilizes consumer PII. A more detailed layer follows, containing a more granular description of the firm’s privacy policy. The bifurcation aims at addressing cognitive constraints, providing something like an “executive summary” to help organize the topics covered by the privacy policy and enable an abbreviated review. Top layered privacy policies reduce dreaded legalese and are meant to clearly articulate the data practices of the company.

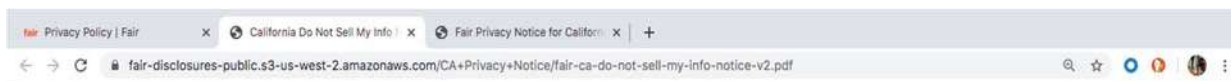
The first two links contain notice documents required by the CCPA while the last three links contain request forms for consumers to fill out. With respect to the last three links, each form is identical regardless of whether the consumer is requesting the deletion or disclosure of PII or opting out of the sale of PIII entirely. The consumer must provide her full name, her Fair account number, an email address associated with the account, a phone number associated with the account, and confirm the request by checking a box. Fair uses extensive cookie technology, as indicated by

the company’s specialized California privacy policy and its general privacy policy. Because cookie technology has already been discussed in some detail, we will assess how the CCPA has impacted the way in which Fair communicates its cookie practices to consumers. The following chart is contained in Fair’s California privacy policy:



Category	Examples	Collected?
Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))	A name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information. Some personal information included in this category may overlap with other categories.	Yes
Protected classification characteristics under California or federal law	Age (40 years or older), race, color, ancestry, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), veteran or military status.	Yes
Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Yes
Internet or other similar network activity	Browsing history, search history, information on interaction with a website, application, or advertisement.	Yes
Geolocation data	Physical location or movements.	Yes

The above chart is in compliance with the CCPA’s requirement that covered entities provide California consumers with categories of PII collected. With respect to covered cookie PII, this information would fall under the category “internet or other similar network activity,” which includes “browsing history, search history, information on interaction with a website, application, or advertisement.” The next image is Fair’s “Do Not Sell My Info” Notice:



California "Do Not Sell My Info" Notice

Effective January 1, 2020

There are certain services that you use of ours for which we do not charge. Instead, advertisers may pay us for allowing them to show you advertisements for their products and services online. Like many other online companies, we may use services provided by Google, Facebook, and others to help deliver interest-based ads to you.

California law may classify some cases of limited information sharing with advertising partners through the use of these services as a "sale" of personal information from which California residents have the right to opt-out. This is because the companies that provide these services and our advertising partners may collect some information from our users (e.g., cookies, advertising IDs, IP addresses, and usage activity) to help them understand how people interact with advertising content on and off of our services and content, and to serve ads that they think users may want to see based on their online activity.

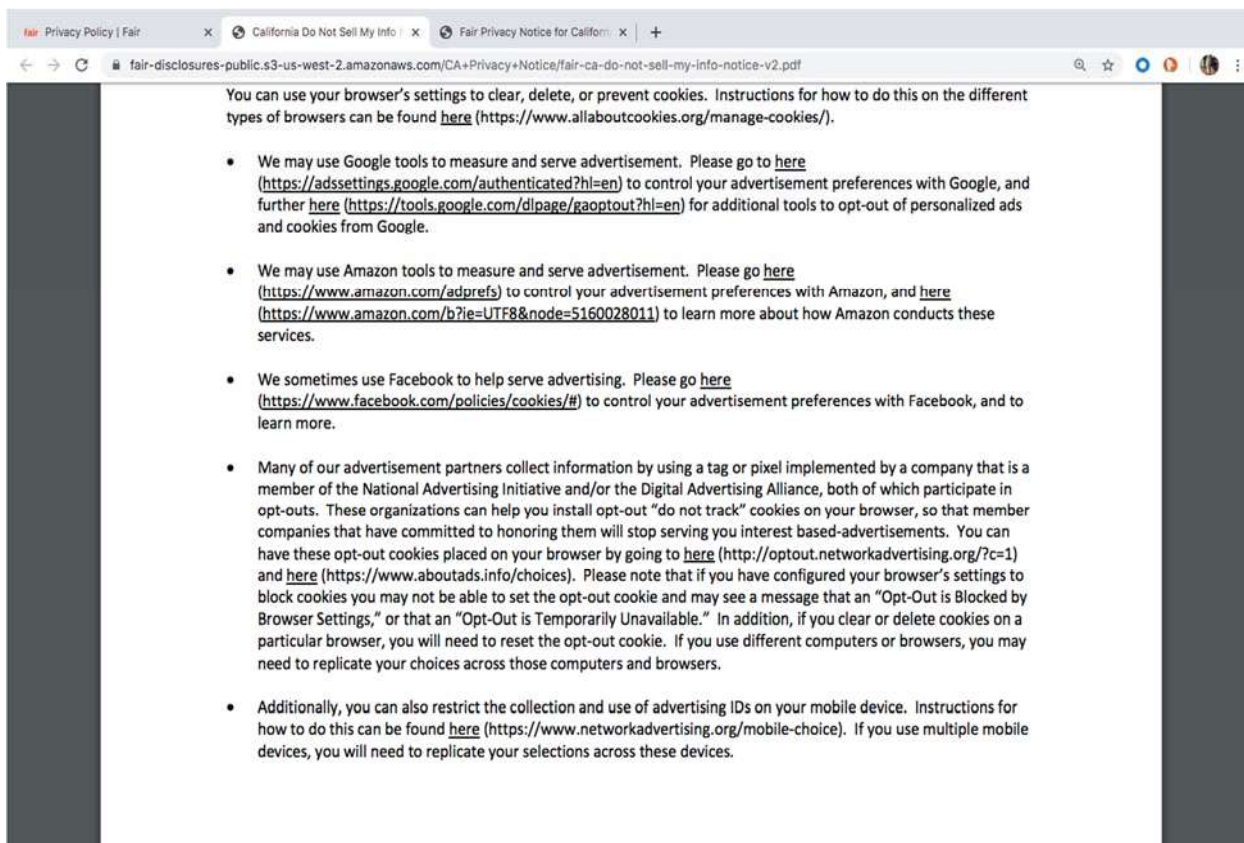
We wanted to take this opportunity to explain your choices regarding how to control the limited information that is shared. You have the ability to restrict this use of cookies and advertising IDs.

There are a few different ways you can do this for cookies:

You can use your browser's settings to clear, delete, or prevent cookies. Instructions for how to do this on the different types of browsers can be found [here](https://www.allaboutcookies.org/manage-cookies/) (<https://www.allaboutcookies.org/manage-cookies/>).

Under the CCPA, Section 178.120, "a business that sells consumers' [PII] to third parties shall provide notice to consumers . . . that this information may be sold and that consumers have the right to opt out of the sale of their personal information."⁵⁰ Hence, the notice above discloses that third parties provide compensation to Fair in order to show advertisements for their own products and services. The notice frames this disclosure in a manner characterizing these payments from third party advertisers as a substitute for Fair charging consumers additional amounts directly. The notice states that "sale" under the CCPA includes third party access to cookies and advertising IDs collected from Fair's users. The notice proceeds to provide the reader with ways in which to restrict the use of cookies and advertising IDs. Specifically, the notice provides links to Google, Amazon, and Facebook, stating all three are used by Fair to serve advertising:

⁵⁰CCPA, Cal Civ. Code 1798.120.



Notably, Fair’s advertising partners utilize both tag and pixel technology (otherwise known as “web beacons”) to collect information and instructs the user on steps to take to opt-out. The web beacons allow website operators to incorporate code in the website’s hypertext markup language (HTML) code. This allows the web beacons to harvest data such as a user’s activities during a session (similar to the functions of session cookies) as well as personal identifiers such as IP addresses.⁵¹

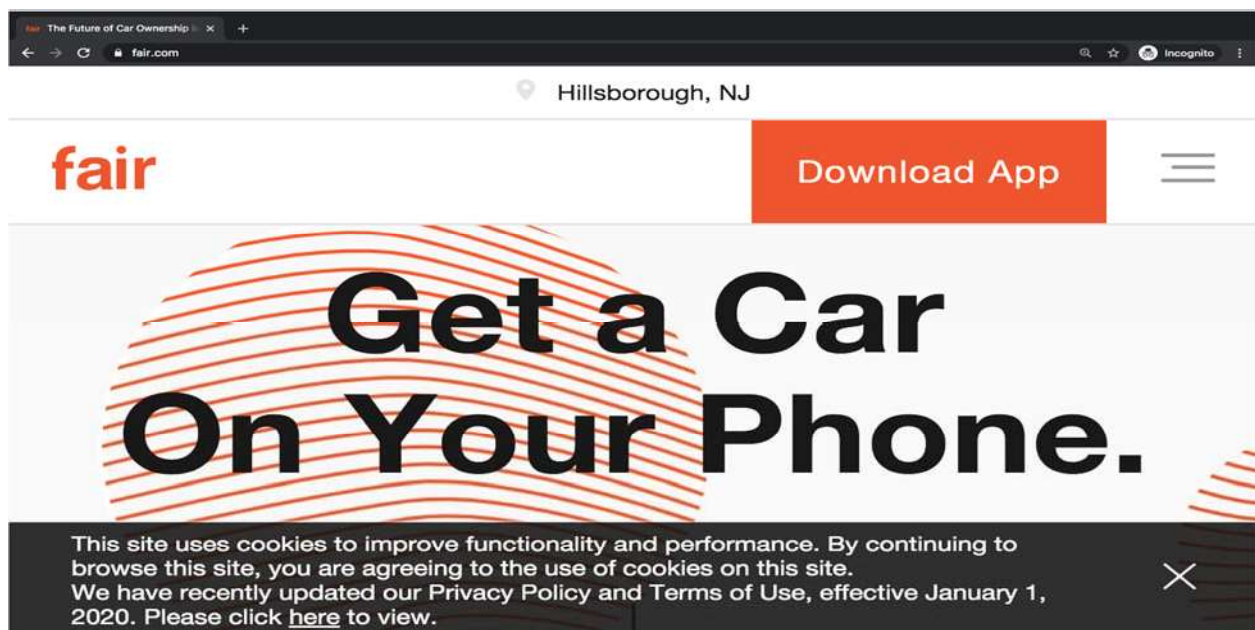
In light of the CCPA and enforcement regulations, some argue that it is still unclear whether covered entities must provide opt-outs of cookie-based advertising.⁵² In our illustration, Fair has

⁵¹ See *Tracking Pixel*, https://en.ryte.com/wiki/Tracking_Pixel (last visited April 9, 2020).

⁵² Dan Storbaek, *CCPA and Cookies. What do I need to Know?*, Secure Privacy (Jun. 24, 2019), <https://secureprivacy.ai/ccpa-and-cookies-what-do-i-need-to-know/> (“In situations where a website deploys third-party tracking cookies (e.g. behavioral advertising network cookies), it is not clear how the business that owns and controls the tracking cookie will be able to provide [notice] ‘at or before the point’ of [collection].”).

answered in the affirmative. Fair discloses in its policies that it uses major platforms such as Facebook, Google, and Amazon to deliver interest-based advertising. The links to each of these sites, respectively, allow Fair’s website users to opt-out of receiving certain targeted ads.

Recall that the CCPA requires covered entities who collect PII to provide notice to consumers *at or before the point of collection*. Generally, websites provide a “cookie banner” to serve a dual purpose: 1) the notice should disclose the types of cookies utilized on the site; and 2) provides users notice of their right to opt-out of cookie-based data collection.⁵³ The following image contains Fair’s cookie banner:



Two related questions are raised by Fair’s cookie banner: 1) has the company complied with its disclosure obligations to inform consumers of the purposes for which the cookie data will be used; and 2) does this notice cover third-party cookie-based technology on Fair’s site?

⁵³ See *Why You Need a Cookie Banner on your Website*, <https://secureprivacy.ai/why-you-need-a-cookie-banner-on-your-website/> (last visited Apr. 9, 2020).

With respect to Fair’s disclosure obligations, it seems that the cookie banner has fallen short of disclosing *all of the purposes* for which cookies are used. Recall that Fair’s CCPA privacy policy states that third parties may use cookies on fair.com to serve users ads based on their online activity. Presumably, collecting revenues from the third parties whose advertising they enable is among the purposes for the cookies. While Fair’s cookie banner discloses use of cookies to maintain functionality of its platform, no disclosures are made with respect to third party activity. This raises the question of whether adequate notice has been provided to users “at or before the point of collection.”

The separate but related question is whether Fair’s cookie banner extends to third party use of web beacons, cookies, and other data collection technology on fair.com. Depending on the amount of third parties permitted to passively collect user data, it would seem impractical for the CCPA to require that all of these entities individually provide notice at or before the point of collection. Ultimately, a third party’s obligations will in all likelihood depend on whether it is engaged in a “sale” with Fair or is simply furnishing a service pursuant to maintaining the functionality of the site itself.⁵⁴ If the third party is passively collecting data to furnish a service to Fair, the CCPA requires a written contract that identifies the third party as a service provider⁵⁵ and specifies the business purpose for the third party receiving the data. This agreement

⁵⁴ Mary Costigan & Joseph Lazzarotti, *CCPA FAQs on Cookies*, JD Supra (Aug. 30, 2019), <https://www.jdsupra.com/legalnews/ccpa-faqs-on-cookies-94248/>, (“[I]t may be unclear if a third party cookie’s collection of personal information is strictly for the website’s business purpose or a sale subject to the right to opt-out.”).

⁵⁵ Defined as a “sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business . . . pursuant to a written contract, provided the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specified purpose of performing the services specified in the contract for business” CCPA, Cal Civ. Code 1798.140(v).

between the third party service provider and Fair would obviate the need for Fair to provide an opt-out right to consumers.

If the third party is engaged in a sale with Fair and is not otherwise classified as a service provider under the CCPA, then the question is raised whether a fair.com user is entitled to opt-out of not only Fair's cookie-based data collection, but all cookie-based data collection whether or not conducted by Fair or a third party.⁵⁶ Fair seemingly addressed this question in the negative. Fair's CCPA privacy policy explicitly states that some of the third parties that utilize cookie and pixel technology also participate in the National Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA).⁵⁷ Fair's notice provides its users instructions on how to opt-out of the targeted advertising of NAI and DAA members. This seemingly indicates that any opt-out request through Fair's *own channels* does not encompass third-party data collection for targeted advertising.

The classification or non-classification of third parties as service providers raises another important implication: service providers, in addition to the business receiving a deletion request directly, are obligated to delete the user's PII.⁵⁸ For third parties engaged in targeted advertising who otherwise have no service provider agreement with Fair, they are under no obligation to delete the user's PII. From Fair's perspective, the firm may be incentivized to utilize as many services as

⁵⁶ Although not specifically pertaining to third party use of cookies for targeted based ads, the CCPA does prohibit third parties from reselling consumer PI that they purchased from the business in contact with the user, except when the user has been notified and received an opt-out option. CCPA, Cal Civ. Code 1798.115. This seemingly implies that third parties engaged in resale of PI must comply with a user's opt-out request, but it is unclear whether this would apply to third party use of PI for targeted advertising.

⁵⁷ For an overview of the self-regulatory efforts of the NAI and DAA, see *NAI and DAA Self-Regulatory Principles Are Latest Effort to Address Mobile Privacy Concerns*, Crowell Moring (Aug. 21, 2013), <https://www.crowell.com/NewsEvents/AlertsNewsletters/all/NAI-and-DAA-Self-Regulatory-Principles-Are-Latest-Effort-to-Address-Mobile-Privacy-Concerns> ("It is clear that these self-regulatory organizations are well aware of the challenges mobile privacy presents; the question is whether they can, on their own, provide solutions that are satisfactory to governing bodies such that new regulations and laws are not needed.").

⁵⁸ CCPA, Cal Civ. Code 1798.105(c).

it can in-house to avoid the monitoring costs of ensuring outside service providers comply with deletion requests.

As the aforementioned discussion illustrates, Fair and many other firms covered under the CCPA may need to reassess and fundamentally change its data collection policies and practices. Given the lack of clarity regarding the CCPA's applicability to third-party data collection via web beacons, pixels, and cookies, host websites may have to devote substantial resources towards verifying the data collection practices of its service providers and other partners. This may ultimately impact the digital advertising ecosystem as a whole and the data collection practices that drive it.

CCPA's Impact on Data Storage and Transfer

Firms that store large data sets, whether located on an internal company server or a cloud-based data center, will inevitably be required to reassess and potentially revise their internal data storage practices. These audits may ultimately be necessary to ensure CCPA compliance. With respect to data storage under the CCPA, two consumer rights are implicated: the right to data portability and the right to deletion of collected data.

This section will explore how the CCPA will impact the internal data storage and transfer practices of covered entities. With respect to data portability, covered entities under the CCPA will be required to ensure that the collected information is readably available to transfer to the consumer upon request. The information must be easily transferable, or *portable*, in order for the consumer to transmit the information to other vendors. From a practical standpoint, such a requirement may

pose significant difficulty for firms who regularly anonymize data sets. For a firm's cybersecurity risk managers, this is not a welcomed development.⁵⁹

In addition to the right of data portability under the CCPA, the right to deletion is also implicated in the data storage context. Companies that store data sets across multiple platforms may face immense difficulties in properly fulfilling a consumer's deletion request.⁶⁰ Simply determining who is responsible for deleting the PII is in of itself a challenge.⁶¹

Effective compliance with the rights of data portability and deletion pose a variety of challenges in the data storage context. Both rights under the CCPA will require firms to correctly identify where data resides, who has access to it at any particular time, where the data was previously stored, and where it is being transferred. This necessitates the need for covered entities to effectively document a precise audit trail of company data. Thus, this section will also explore the potentially growing use of data inventories. Data inventories allow for the efficient and accurate tracking of data both in transit and storage. Whether the firm is responding to a request for consumer PII in a portable form or must delete collected PII, data inventories will allow firms to correctly identify the consumer's data as it progresses through its life cycle in the company.

a. The Right to Data Portability under the CCPA

⁵⁹ But see *Discussion Paper on Data Portability*, Personal Data Protection Commission (Feb. 25, 2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf>, ("From a competition perspective, data portability could lead to efficiencies for organisations, as organisations may find it easier to gain access to more varied data sets.").

⁶⁰ However, proposed CCPA regulations may allow for delays in deletion of information stored in archives or backup systems. See *Deletion Completion Under the CCPA*, Locke Lord Publications (Nov. 2019) <https://www.lockelord.com/newsandevents/publications/2019/11/deletion-completion-under-the-ccpa>.

⁶¹For firms utilizing cloud storage, the CCPA provides no clear answers as to who is responsible for deleting consumer PII - the cloud service provider or the firms using the storage. Maria Korolov, *CCPA and GDPR: The Data Center Pitfalls of the 'Right to be Forgotten'*, Data Center Knowledge (Feb. 4, 2020) <https://www.datacenterknowledge.com/regulation/ccpa-and-gdpr-data-center-pitfalls-right-be-forgotten>.

Once a business receives a verifiable request from a consumer for the PII the business has collected, the business must provide the requested PII in a “readily useable format that allows the consumer to *transmit this information from one entity to another entity* without hindrance.”⁶² This language indicates that any PII first collected by the business, and subsequently disclosed to the consumer upon request, must be portable. The right to data portability is also enumerated in the GDPR, which allows the consumer to receive her personal data in a “commonly used and machine-readable format and [has the right] to transmit those data . . . without hindrance.”⁶³

From a risk management perspective, the right of data portability presents a number of challenges. Firms that use widespread encryption on internal servers may have difficulties locating the correct PII requested by the consumer. It may be possible for firms to implement decryption tools on individualized sets of data. Moreover, firms could choose to assign select encryption keys to individualized data in order to increase accessibility. But firms could also conclude encryption may not be worth the cost of noncompliance and refrain from the practice entirely. In turn, this may present opportunities for bad actors to obtain portable PII with greater ease.

From a consumer’s perspective, holding portable data on an unsecured server will present a number of cybersecurity risks. These risks are heightened if the consumer is able to readily transfer her portable data to untrustworthy third parties.⁶⁴ Furthermore, it is unclear what data a consumer should have the right to obtain – i.e. what information belongs to the consumer and what belongs to another. This again presents a number of risks from a business’s perspective. If a

⁶² CCPA, Cal Civ. Code 1798.130. (emphasis added).

⁶³ General Data Protection Regulation, Art. 20 (2016).

⁶⁴ Gennie Gebhart, Bennet Cyphers, & Kurt Opsahl, *What We Mean When We Say “Data Portability”*, Electronic Frontier Foundation (Sep. 13, 2018), <https://www EFF.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability> (“Ported data can contain extremely sensitive information about you, and companies need to be clear about the potential risks before users move their data to another service.”).

business inadvertently discloses a consumer's portable data to the wrong consumer, this may lead to a private right of action against the business.

With respect to the storage of consumer PII, the right to data portability presents a number of risks from both the consumer's and business's perspective. Both sides of the transaction will have to grapple with a number of cybersecurity challenges that portable data will pose. As legislation similar to the CCPA becomes commonplace in the United States, lawmakers will have to balance the rights of consumers with respect to data ownership and the need to effectively safeguard PII from bad actors.

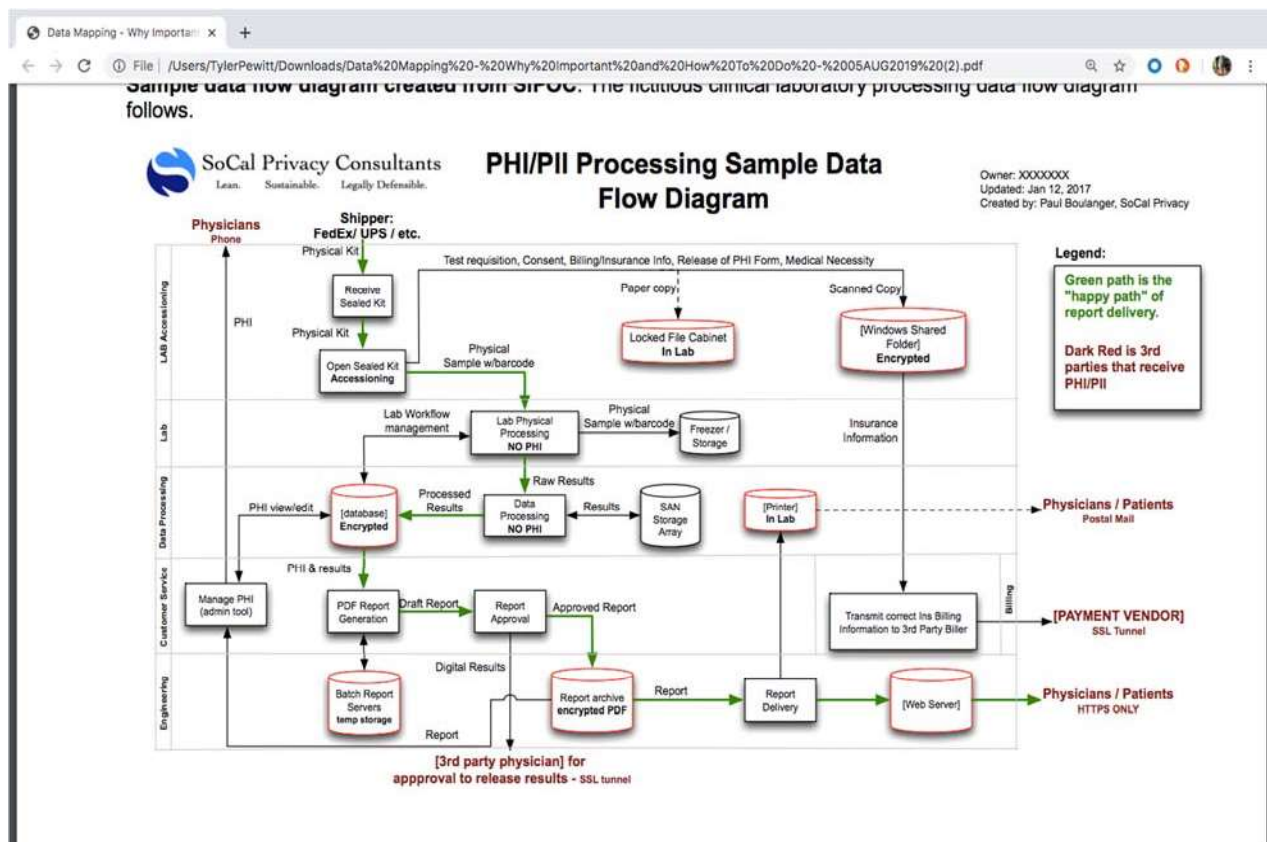
c. Right to Deletion

Assuming the consumer is entitled to the deletion of her collected PII,⁶⁵ covered entities must ensure their internal data storage and transfer policies permit compliance. For those firms holding exceptionally large amounts of data in storage, whether it be on a physical medium, cloud-based storage, or in a data center, a number of barriers may prevent the firm from complying with the deletion request. One example is encryption. If a firm employs encryption across an entire data center, deleting the requested information may prove difficult. As was the case under the right of data portability, firms may have to refrain from otherwise practical security measures for the sake of honoring requests for deletion. Ultimately, covered entities under the CCPA may have to weigh the costs of fundamentally changing their data storage practices and promptly responding to deletion requests.

d. Data Inventories

⁶⁵ The deletion right is not absolute. Businesses need not comply with deletion requests if the data is related to the following: 1) providing goods or services to the consumer; 2) detecting issues related to security; 3) complying with legal requirements; 4) research pursuant to the public interest; 5) the right to freedom of speech; and 6) internal uses of data that consumers may expect. CCPA, Cal Civ. Code 1798.105

Because of the rights to data deletion and portability, covered entities under the CCPA may be required to establish internal data inventory policies. Data inventories allow for the efficient identification of PII both in transit and in storage across multiple systems. Moreover, inventories promote sound data accountability principles, insofar as they clearly identify who is responsible for the data at a particular time in its life cycle. Finally, inventories allow for efficient categorization of data sets. The following image is an example of one firm's data inventory:



For those covered entities required to furnish portable PII or delete collected PII, the use of company data inventories may become commonplace.

As it pertains to covered entities required to furnish portable data to consumers, a data inventory will serve a three-fold purpose: 1) it will allow the covered entity to locate a suitable access point to extract the portable data; 2) it will reduce any costs associated with conducting

time-consuming audit trails of company data; and 3) the firm can identify the business units best equipped to furnish the portable data to the consumer.

This efficiency also translates when responding to requests for the deletion of consumer PII. The inventory will allow the firm to pinpoint the appropriate server to conduct the deletion. The inventory will ideally reflect those servers that contain readably accessible data and specify who may access the information to delete it. Ultimately, firms do not just have cost-incentives in ensuring they accurately fulfill deletion requests. Inadvertent deletion of PII may have substantial reputational costs for covered entities. Data inventories will allow covered entities to revise internal storage practices pursuant to full compliance with CCPA deletion requests.

Conclusion

At this point in time, it is largely unclear how the CCPA will change how companies collect and store personally identifiable information. From the consumer's standpoint, the CCPA provides controls over information never before available in the United States. Consumers now have the ability to request disclosures on what information a particular company has collected on them, request that companies cease selling the information, and even request the deletion of that very information under certain circumstances.

From the company's perspective, the CCPA may require the firm to closely scrutinize its relationships with digital advertisers and the contracts that shape those relationships. Covered entities may feel pressured to ensure that third parties with access to consumer PII adequately protect the information. Ultimately, changes in these relationships may fundamentally change the digital advertising ecosystem, a system largely fueled by cookie-based data collection.

The CCPA may also force covered entities to take another look at their internal data storage practices. A practical solution to this challenge should include the utilization of a data inventory.

Without tools necessary to locate the right data and successfully access it, covered entities stand little chance of complying with CCPA deletion requests and data portability requirements. These fundamental challenges will cause companies to closely scrutinize and ultimately adapt their business models.