Dec 30 2019

California Privacy Regulation

Brief #18: The CA privacy law effective Jan 1 will set the tone for US regulation

17 min read

What's Happening

With the **California Consumer Privacy Act (CCPA) about to take effect on Jan 1 2020**, companies across the world are scrambling to prepare for the requirements of the new data privacy law. Given the size of California (the most populous US state) as well as the number of companies residing in the state, **CCPA applies to a significant portion of US and large global businesses** (though not to nonprofits or government agencies). In the US alone, an estimated 500K organizations will be impacted. The **cost of compliance for each business in scope could be $50K to $2M**, with companies expected to spend a total of $55B to prepare for CCPA (not including the follow-on costs to maintain compliance).

Most of the big tech players – including Google, Twitter, Microsoft, and Facebook – are making moves to comply while lobbying for federal regulation. The advertising ecosystem – including advertisers and publishers who may be disproportionately affected – is bracing for the impact of the coming rules and waiting to understand how they will be enforced.

Privacy regulation could upend the advertising business model and shake up even the largest tech firms. Consumer trust will be critical in gaining consent for use of their data.

Jump to **What It Means**

Overview of the CCPA

What is the CCPA: Passed in Jun 2018, the California Consumer Privacy Act requires that certain companies **"doing business" in California** (e.g. users, customers or employees in California) – regardless of whether the business has a physical presence there – comply with rules governing how they collect, manage, and use personal data, both online and offline. While CCPA goes into effect on Jan 1 2020, it **will not be enforced until Jul 1 2020** (though noncompliance that dates back to Jan 1 could still be liable to a lookback). Finalized regulations from the CA attorney general have yet to be released but are expected to be similar to the proposed version.

CCPA specifically applies to businesses that meet **at least one of the following** criteria:

- **$25M+ in annual gross revenue**
- Handles data on **50K+ consumers or devices**
- Derives **50%+ of revenue from selling consumer data**

Rights of consumers: The law gives California consumers the right to:

- **Request disclosure of business practices** related to their data, such as what is collected, how it's used, and who it's shared with
- **Know all of the information collected** on them for the 12 months preceding a request, including any inferences drawn about the consumer (e.g. characteristics, preferences, segmentations); with exceptions for high-risk information such as Social Security numbers and bank accounts
- **Delete their data**, including from service providers (with certain broad exemptions such as to abide by other legal obligations, for essential security functions, or for internal uses aligned with consumer expectations)
- **Opt out from their data being sold** (children under 16 must opt in, with a parent/guardian opting in for children under 13)
- **Not be discriminated against** for exercising the rights above – e.g. being denied goods or services, different pricing or service levels (unless the difference is "reasonably related" to the value of the consumer's data)

Businesses must **notify consumers at or before data collection** (e.g. use of cookies), such as a plain-language notice and CCPA-compliant privacy policy describing the business

purposes for which the data will be used. They also have to **establish processes to receive and handle requests**, including "**reasonably verifying" each requestor's identity** with consideration to the sensitivity of data being requested. Businesses receiving a request to know or delete must confirm receipt within 10 days and **provide an individualized response within 45 days** (unless they provide a reason for needing a 45-day extension). With respect to the right to opt out from personal data being sold, businesses must offer an opt-out button, take action within 15 days of a request, and notify third parties to whom they have sold the data within 90 days.

Role classifications: CCPA defines 3 different role classifications – **businesses, service providers, and third parties** – each with its own set of requirements and allowances. For instance, businesses are required to disclose to requesting consumers how they are sharing personal information with a third party. They also may need to notify service providers and third parties upon receiving a relevant consumer request – e.g. request to delete or opt-out of sale. Service providers are an advantageous classification because they can collect personal data from a business for a business purpose covered in a contractual agreement (though service providers are restricted from using the data for any other purpose). Conversely, businesses that provide consumer data to service providers (as opposed to third parties) are generally not considered to be "selling" that data – which means the consumer right to opt out of their data being sold would not apply in this case.

Definition of "selling data": The CCPA defines "selling" a consumer's personal information as providing it to a business or third party for "monetary or other valuable consideration." The ambiguity of this definition has resulted in controversy, with variance in how it has been interpreted by different companies. Facebook (see below), for example, is contending that receiving and sharing user data collected on other websites is exempted as transfers to "service providers," rather than "selling data." Other industry watchers are saying, however, that the law was expressly intended to address how Facebook collects and uses consumer data.

Penalties for violation: Intentional violations can result in a **fine of up to $7,500 per impacted consumer** (unintentional violations will be subject to the preset $2,500 maximum). For a data breach specifically, individual consumers can also sue for $100-750 in statutory damages or the value of actual damages (if greater). There is a **"cure provision" that protects businesses from statutory damages** in individual and class-action lawsuits if they can fix the underlying issue behind the violation within 30 days, leaving them liable only to actual damages. The extent of enforcement remains to be seen – California has set aside $4.7M in funding and made 23 new hires to support enforcement.

Response from companies

The value of personal data used in advertising in California is estimated at $12B to $20B annually. Companies are beginning to recognize that CCPA – and its constraints on use

of personal data – may have **far-ranging business model implications as well as compliance costs**. In one survey of US businesses, **only 42% expected to be ready for CCPA** by the Jan 2020 date.

Tech firms such as Facebook, Google, Microsoft and Apple have been lobbying for **federal privacy regulation** since at least mid-2018, seeking a more consistent and coherent regulatory framework rather than a patchwork of state-level laws. Some of the companies impacted are also hoping to influence federal regulation, which **could override and loosen CCPA requirements**. In Sep 2019, 51 large-company CEOs (including Amazon) in the Business Roundtable signed an open letter asking the US Congress for federal privacy regulation, proposing their own consumer privacy framework. In Dec 2019, Walmart also expressed its support for a comprehensive federal privacy law, asking lawmakers to be wary of how the law will have unintended consequences on sectors outside of technology (such as retail). **Proposals in both houses of Congress are currently on the table** but lawmakers have yet to resolve their disagreements.

In the meantime, companies are working to adapt to the CCPA, which will go into effect very soon. Many companies including Walmart, Disney, Kohl's, Lyft, and Visa have updated their privacy policies to comply with CCPA, in some cases taking a conservative approach that pulls back on certain activities to ensure compliance. A handful of companies, both large and small, such as Microsoft and Starry (an ISP), have committed to **applying CCPA rules to all customers nationally**. A smaller subset of businesses are opting for a "wait and see" approach, holding off until they get clarity on the requirements and consequences.

Tech firms

- **Facebook**, which has been trying to rebuild user trust and its reputation, published a blog post on Dec 12 2019 describing its preparations for CCPA. In addition to updating its Data Policy and Privacy & Data Use Business Hub, Facebook also offered revised contractual commitments to its business partners clarifying it would only use partner data for business purposes described in their contracts. It also referenced an existing suite of tools developed to comply with the EU's GDPR (General Data Protection Regulation) that allows users to "access, download and delete their information." **Facebook's Pixel web-tracking tool has been a point of particular controversy**. Typically installed by businesses on their websites, Pixel sets cookies on visitor browsers, which helps Facebook link their activity to their Facebook profile and allows businesses to buy targeted ads on Facebook. According to a recent WSJ report, Facebook told advertisers it would not be making changes (e.g. adding opt-out) to Pixel, because it believes the data-sharing involved falls under the "service provider" exemption. Earlier this year, however, Facebook tested an Off-Facebook Activity tool in limited markets, allowing users to disconnect and delete data collected on them from outside websites.
- **Twitter** announced on Dec 2 2019 that it was launching the Twitter Privacy Center hub, in addition to updating its Terms and Privacy Policy. The Twitter Privacy Center outlines how it collects and manages user data as well as the options for users to control it, with dedicated

pages for CCPA, GDPR, and Global DPA (Data Processing Addendum). Twitter also announced it was moving accounts for international non-EU users from Twitter International to its US-based company, allowing it to experiment with different privacy tools and settings for EU and non-EU users.

- **Microsoft** announced in a Nov 11 2019 blog post that it would **honor the CCPA requirements for all of its customers nationwide** (similar to its prior announcement that it would extend the EU's GDPR rights to customers around the world). Microsoft also plans to continue to develop its privacy offerings and controls for users, including its core privacy dashboard. It is also working with enterprise customers to help them comply with CCPA as well. Microsoft has advocated for even stronger privacy regulations, with even more accountability placed on companies. Microsoft, unlike some of its big-tech peers, lacks a big digital-advertising business and has contractual relationships with most of the outside parties with which it shares data (i.e. largely under the "service provider" exemption).
- **Google** launched in Nov 2019 **"restricted data processing" features** for its advertising and analytics tools, to help advertisers and publishers comply with CCPA. The features make it easier for websites to restrict the sending and use of selected data – e.g. for consumers that have opted out. Google also updated its Privacy Compliance site with a CCPA section, and provided guidance for Google Cloud customers. Google has also been experimenting with **privacy features for its Chrome browser** such as better cookie controls and protections against browser "fingerprinting." In Aug 2019, Google launched a **Privacy Sandbox to experiment with personalization** while protecting user privacy.
- **Apple**, which has been one of the most vocal advocates for data privacy, announced in Jun 2019 the privacy-friendly "**Sign in with Apple**" service, allowing users to log into other websites and services on Apple devices without their data being used to sell ads. Apple was among the first to block cross-domain tracking in its Safari browser, and continues to work on anti-tracking features. It launched a revamped privacy page in Nov 2019, and also published a platform security guide in mid-Dec 2019 explaining how it protects data across its products and services. Apple has been actively hiring for an array of privacy-related roles in its legal and engineering departments.
- **Amazon**'s efforts around CCPA have largely been oriented around its Amazon Web Services (AWS) cloud business, particularly its data-related services used by thousands of enterprises. AWS has a dedicated CCPA compliance site with guidance on how to prepare, including whitepapers such as "Preparing for the California Consumer Privacy Act" (Jul 2019). Amazon CEO Jeff Bezos was among the 51 signatories of the open Business Roundtable letter advocating for federal privacy regulation.

Advertisers and publishers

Many advertising firms are taking a **preemptively cautious approach toward CCPA to ensure compliance**, despite the open questions regarding the definition of "sale" and how the law will be enforced. A few agencies have decided to avoid completely the targeting of California consumers, while some advertisers and adtech companies are imposing their own

measures for what they can do with user data. Contextual-advertising firm GumGum, for instance, is planning to be fully compliant, notifying consumers that it sells their data and providing tools to opt out.

Advertisers and ad tech companies are seeking to position themselves in advantageous roles – for instance, aiming for the "**service provider**" designation that would allow them to collect and process data shared by their business clients for specific business purposes, such as clients' own ad buys. However, the designation (which implies a bilateral contractual relationship) comes with restrictions on how the data shared can be used in other contexts and for other purposes, potentially hampering certain revenue streams. **For programmatic advertising, the multiple adtech companies involved in fulfilling a programmatic ad would likely have to all be "service providers" to share data**.

Advertisers are banding together and garnering **support from industry groups to help establish and promote standards**, as well as coordinate to minimize industry disruption. For instance, the Interactive Advertising Bureau (IAB) has developed a CCPA compliance framework and Limited Service Provider template contract to help advertising firms operate in a compliant way – specifically with companies "downstream" in the supply chain operating as service providers to publishers. Similarly, the Digital Advertising Alliance (DAA) recently released a set of CCPA opt-out tools and onboarding process for digital-advertising companies.

Some advertisers and publishers are concerned about the **implications if the current state of targeted and retargeted advertising becomes no longer viable** – e.g. if the CCPA takes on the strictest possible form and regulations and technology move toward a "post-cookie world." Retailers are already pressure-testing these extreme scenarios, while publishers like Meredith and Washington Post are working on forms of contextual advertising that are less reliant on cookies (e.g. that use the content the user is viewing on the page or the channel the visitor came from instead).

Privacy regulations beyond California

CCPA has been called "GDPR-US" by many regulatory observers, a nod to the **EU's General Data Protection Regulation** that went into effect in May 2018. CCPA is considered less burdensome than GDPR, which is a landmark data privacy law with far-reaching scope and scale affecting organizations of any size that do business in the EU, that target EU citizens as customers, or that engage with them more than occasionally.

While some of the requirements are the same – e.g. ability for consumers to view and delete data – **GDPR is more principles-based and CCPA leans towards a more rules-based approach**. Noncompliance with GDPR's principles can carry **sizable penalties – up to €20M or 4% of the company's global annual turnover, whichever is greater – without a cure provision**. Google ($57M), Marriott ($124M) and British Airways ($230M) are among the

companies that have faced sizable fines so far. Many of the **US companies that have already invested in GDPR compliance are leveraging that infrastructure for CCPA compliance**.

Other countries are considering following the EU's lead in updating their privacy laws:

- **Brazil** passed in Aug 2018 its **General Data Protection Law (LGPD)**, which will go into effect Feb 2020. Similar to GDPR, the law is aimed at regulating the collection and use of personal information by both online and offline businesses, though the fines are less severe.
- **India** is now debating the **Personal Data Protection Bill 2019** that would require companies to give users more control over their data (e.g. consent, ability to delete), while simultaneously expanding the rights of the national government to store and use citizens' personal information such as biometrics and survey data.
- **Canada**'s prime minister Justin Trudeau released a **mandate letter in mid-Dec 2019 signaling a coming overhaul of data privacy rights** that parallels GDPR and CCPA, along with new elements such as data portability, proactive data security, and freedom from online discrimination and harassment.
- **Australia**'s prime minister announced in mid-Dec 2019 a **review of privacy laws**, as part of a broader effort by the competition authority to monitor the big tech platforms and establish a digital code of conduct.

In the **US**, which has lagged the EU in instituting federal privacy regulation, **other states are following in California's footsteps** with updated privacy laws – including Rhode Island, Massachusetts, New Jersey, Pennsylvania, Hawaii, New York, Washington, and Texas (proposed bills in Washington and Texas did not pass). In May 2019, **Nevada passed a significant amendment to its online privacy laws**, allowing Nevada consumers to opt out of the sale of their personal data (defined tightly as the exchange of data for monetary considerations).

What It Means

It's clear that the California Consumer Privacy Act will have **far-reaching impact beyond just California-based businesses**. In the near-term, it will impact 500K+ companies in the US that meet its size/scope thresholds and "do business" in California, and more beyond the US. **For some companies, the CCPA will effectively be treated as a "national law,"** similar to what happened with GDPR. In the medium-term, it will likely serve as **a touchstone for the federal privacy regulation** that has been looming. In the longer run, it may be an **impetus for a**

sweeping transformation of the advertising business model that powers some of the biggest tech firms.

How companies respond to CCPA depends on the resources they have available, their exposure to liability, and how forward-looking their leaders are. For instance, smaller companies with tight cash flow and limited exposure will likely take the less-advisable "wait and see" approach. On the other hand, **companies like Microsoft and Apple have been staking out early strategic positions as they track the market moving towards user privacy and trust**. If we believe that the broader trend towards more privacy regulation will continue, Microsoft and Apple's approach in playing to the highest and strictest standards may be more efficient than trying to address different pockets of regulation across the US and globally. Looking ahead, it also opens up avenues for gaining user trust and further entangling users in Microsoft and Apple's respective ecosystems (see Dec 13 2019 brief on tech players' expansion of their ecosystems into financial services).

Microsoft and Apple, not coincidentally, are also the big tech players that lack a large-scale digital advertising business. The other tech firms are generally no longer in denial and are investing in technological solutions. However, the efforts by these firms, particularly those with digital-advertising businesses, lag in public perception – partly because of the preexisting public-trust gap and partly because **privacy regulation goes to the heart of their data-based business models**.

While it's usually unwise to bet on a political process, **it's likely that we'll see a US national privacy law come to pass**. Many companies want federal privacy regulation that will supplant the CCPA and other state-level privacy laws, streamlining compliance and opening up the possibility of less stringent rules. There is both public and bipartisan support, not to mention several bills in play in both houses of Congress. CCPA, for instance, is very popular among California voters, with nearly 90% in favor. We may even see California privacy law become even more stringent under a recent initiative (as well as further progress on national privacy laws globally), putting further pressure on US Congress to get their act together. It wouldn't be the first time that California has served as a bellwether for national regulation.

Even if we see a less stringent federal privacy law, it will likely be anchored to GDPR and CCPA in its requirements. Many larger companies still have to comply with GDPR anyway, not to mention the swath of emerging privacy laws across the globe. The **costs of compliance** with these modern privacy laws can't be underplayed, stretching far beyond updates to privacy policies and cookie consent pop-ups. Sizable investments are needed to verify consumer requests (which could expose businesses to substantial risk); build tools to collect, view and delete personal data; enable users to opt out of sale; notify relevant service providers and relevant third parties; and deliver personalized responses within the statutory timeframe (e.g. 45 days). For many companies, adhering to the specific requirements around these consumer rights will mean **updates to legacy systems**. Tech and cloud firms also have to consider **how to help their customers/clients with compliance**, in addition to their own. Some countries are layering in data portability, data security, and data localization in cloud environments

(see Nov 22 2019 brief on global cloud race) into their privacy laws as further complicating factors.

There is also a host of **downstream sometimes-unintended consequences** that will inevitably ensue. For instance, the CCPA includes **"inferences" among the personal data that consumers have a right to view**. This could mean customer segmentations like "Status Seeking Singles" or "Blue Collar Comfort," or prioritizations like "National Accounts" and "Inconsequentials" – leading to awkward situations. Since the CCPA does not significantly distinguish between consumers and employees, **companies who are employers will find themselves having to explain to their employees how their personal data is used and shared**. Ad agencies and consulting firms, who habitually receive data from their clients and partners, may have to take a **new look at their service-provider agreements** to make sure all the business purposes for the data are in scope.

The extent of the impact of regulations like CCPA will **depend on how far consumers take their rights**. The CCPA, for instance, allows consumers to make a maximum of two requests in a 12-month period. Will many consumers "capitalize" on and exercise their rights? Or will the majority not care and instead allow the status quo to perpetuate? The early outcomes of CCPA will be informative and help shape the policy view on privacy. The number of requests and opt-outs received by companies will serve as a mechanism to see how much US consumers actually care about privacy, particularly if they come with tradeoffs – e.g. some of the services they know and love might stop working effectively. The CCPA's impact will also depend on the California attorney general's ability to enforce its strictures.

One recurring criticism of privacy laws is that they **help reinforce the position of the established monoliths with deep pockets and hurt smaller companies who lack the resources to comply**. Larger firms have the legal and technical resources to adapt, in some cases already having taken steps to comply with GDPR and build out relevant infrastructure. In contrast, smaller companies may hope to fly under the radar, responding to requests on a case-by-case basis and avoiding the regulatory regimes in other markets. The dynamic may deter startups from entering spaces involving large personal-data sets, leaving the terrain to the big tech firms. We may see a **mindset shift among smaller firms from "data is gold" to "data is risk."**

In the longer run, however, **the potential for privacy regulation to upend the advertising business model could shake up even the largest tech firms** – turning the industry on its head and opening up new opportunities for entrants. The CCPA's requirement to stop selling an individual's information upon request **will impact business models of data brokers, credit agencies, digital-advertising platforms, financial services companies, retail and consumer goods, telecom companies,** and more. In advertising, for example, CBS Interactive's EVP of global programmatic revenue told Business Insider that their cost per thousand impressions is 20% lower than before GDPR. We may eventually see advertisers move away from the current state of targeted and retargeted advertising in favor of **alternative "post-cookie world" approaches like contextual advertising and**

anonymous personalization. Across industries, those that own and depend more on first-party data (e.g. direct-to-consumer brands) than third-party data (e.g. automakers) will be impacted less.

We'll see continued emphasis on **ownership of the customer relationship and especially user trust**. Distrusted companies will likely see more "delete" and "opt-out" requests, while users gravitate towards the ecosystems of companies they view as "trusted advisors." These trusted companies will gain access to **increasingly valuable first-party data**, rather than relying on more highly regulated third-party data. They will work to own and act on more of the data they collect, rather than pass or sell to outside parties. To provide a better customer experience, these companies may move towards verticalization (e.g. Apple), in addition to serving as a trusted gatekeeper of a managed ecosystem. Some will vie to become platforms (e.g. Microsoft's Project Bali) where **consumers can take greater control of their data and even monetize it directly,** with explicit incentives for them to share their data.

In addition to challenges for businesses, **privacy regulation like CCPA will also open up an array of new business opportunities** for those able to take advantage of this new reality. Consulting and law firms will be called on to help clients with updates to legacy systems, the evolution of their business models to survive and thrive, and their technology and operating model roadmaps. New compliance frameworks and tools will emerge, as well as managed services to help companies operate new compliance functions. Customer verification and the biometrics industry also stand to gain from new opportunities. Companies will also need data services – from data architecture and pipeline to to data-lineage management to cleansing and anonymization. While cloud players like AWS and Microsoft will be pursuing these opportunities, privacy is also a growth area for regtech startups and compliance tech vendors. Ogury, for instance, just raised $50M for R&D around its user consent tools. Vendors are already offering services to help publishers and marketers adjust their practices and business models.

Disclosure: Contributors have investment interests in Microsoft. Amazon and Google are vendors of 6Pages.

Have a comment about this brief or a topic you'd like to see us cover? Send us a note at tips@6pages.com.