The Flurry Guide to CCPA

FLURRY

Seven surprising facts about CCPA compliance that mobile developers should know

The California Consumer Privacy Act (CCPA) has changed the face of data privacy practices across many technical domains, including mobile app development. App developers must work to understand the CCPA because it requires that mobile developers make significant changes in both their code and their business practices.

While the long term implications of the CCPA and the regulators' enforcement priorities remain to be seen, one thing is certain:

CCPA has wide-reaching data privacy requirements—and the most regulatory enforcement 'teeth'—of any state-based US regulation to date.

It's clear that CCPA compliance calls upon mobile app developers to rethink many of their data handling methods, their data sharing practices, their capabilities for deleting personal data on command, and their monetization strategies.

To help the mobile app development community meet CCPA compliance, Flurry put together this guide to help clear up the common misperceptions among mobile stakeholders that could prove costly. We believe knowing these facts can help mobile developers stay ahead of the most common pitfalls and avoid finding themselves in the regulators' sites.

What is CCPA?

The California Consumer Privacy Act (CCPA) is a wide reaching data privacy law that went into effect January 1st, 2020. It governs the way that any app developer, website owner, or business handling personal data of a California resident protects this information. App developers seeking more information to help them with CCPA compliance can start **here** to read the text of the legislation.

CCPA impact creeps far beyond California

Whether a mobile developer is based in California, in another state, or even in a country outside the United States, CCPA applies whenever the end user is a California resident.

With a population of 39.5 million and making up over 10% of the US population, Californians represent a significant number of users to the mobile app marketplace, domestically and worldwide.

It would be a rare app that wouldn't count a statistically significant segment of users from California. In fact, we conducted our own analysis and found that for apps that report over 100k weekly active users in the United States, on average, 16% reside in California.[1] For this reason, the law's jurisdictional scope crosses state lines and borders, regardless of where a developer is located.

16% App users that live in California for apps with over 100,000 weekly active users[1]

Device identifiers count as "personal information"

Personally identifiable information (PII) has long been defined in data privacy circles to include details tied specifically to a person such as their name, address, email address, credit card numbers, social security numbers and so-on. All of that traditional PII remains in play for CCPA regulators, but the oversight doesn't stop there.

CCPA extends its jurisdiction to what legislators call 'personal information,' which also includes anonymized device identifiers, IP addresses, and household information.

[1] Flurry internal data, November 2019.

CCPA differs from GDPR in several key ways

With so many similarities in regulatory oversight and intent, CCPA has often been referred to as the US version of the European Union's General Data Protection Regulation (GDPR). This rings true when it comes to general principles of what GDPR calls data subject rights of consumers.

Similar to GDPR, CCPA says that people have the right to:

Disclosure: knowledge that a company is collecting information about them and for what purposes

Access: the option to request a copy of all of the data the company collects about them

Deletion: the ability to request that the company delete the data related to them

However, CCPA is no carbon copy of GDPR.

There are some subtle and key differences between the two. For example, the expanded jurisdiction over device identifiers is unique to CCPA. And while GDPR generally operates with a philosophy of opt-in data use, CCPA takes an opt-out approach.

So, for activities like email marketing and collection of cookies, GDPR has generally been interpreted to require consent in advance before carrying out collection and processing. Whereas CCPA requires no such advanced consent, but does stipulate that organizations must be able to comply with a consumer's request that it does not sell their personal information to third parties.

The last example is an important one, because it also illustrates another difference. GDPR regulations tend to center around the use and processing of data, while CCPA primarily focuses on the sale of data between third parties. However, the definition of what constitutes selling of data is different in CCPA than GDPR. We'll expand on that in a moment, but the point here is that mobile developers cannot afford to simply assume that if they're GDPR compliant then they're also CCPA compliant. Similarly, they can't just copy and paste from a GDPR compliance strategy to handle CCPA compliance.

GDPR compliance does not equal CCPA compliance.

You may be selling data and not even know it

Another big surprise that CCPA has in store for developers is the extensive scope of sale defined by lawmakers. The term 'data sale' applies even when an organization is renting or sharing the information temporarily for a price. And whether renting or handing over the data permanently, the price doesn't have to be monetary.

Sharing data in exchange for any 'valuable consideration' also counts, which means providing access to data in exchange for a free service will be considered a data sale. This puts mobile app developers under the purview of CCPA when they use any number of free data analytics services, Flurry included.

In many instances, app developers do not sell data to a service provider for cash, but they may share data with the provider for the use of the product or service. As a result, that puts both mobile developers and that provider under the microscope of CCPA auditors. The important thing for developers to note is that they'll need transparency and cooperation from these vendors and partners to ensure the CCPA compliant handling of data across its entire lifecycle.

Developers will need to be sure every free service to which they send data supports the ability for consumers to be marked as opt-out.

Sharing data

Sharing data in exchange for any 'valuable consideration' also counts, which means providing access to data in exchange for a free service will be considered a data sale.

Developers will need to be sure every free service to which they send data supports the ability for consumers to be marked as opt-out.

Providing consumers access to their data will prove trickier than you think

As we've explained above, the right to data access is one of the core consumer protection tenants of CCPA. The law stipulates that a user can go to any website or app and ask for all of the personal information that's been collected about them. That request by the user triggers a series of obligations by the app developer: the developer must respond in a timely fashion, track all user requests and be able to report on those requests should the California Attorney General ask for specific metrics.

Nevertheless, with so much of modern app business development dependent upon user-level analytics and sharing of that information with analytics and advertising partners, this could turn into a chain of custody nightmare for developers.

The good news is that when consumer identifiers are anonymized as a part of regular business processes, there's no need to re-identify that data in order to meet requirements. However, with device identifiers and IP addresses under the purview of the law, simple anonymization of usernames or other PII won't satisfy the regulators.

Let's be real about the situation: most analytics are collected and tagged with some kind of identifiers tied to the device.

SDKs pull in advertising identifiers and other methods similarly collect information to help place the user or device into a demographic for the developer so they can do segmentation and analysis. This kind of analysis is the basis for mature app development. User-level information helps developers make targeted app enhancements and sound business decisions.

Simple anonymization of usernames or other PII won't satisfy the regulators

You're going to need the power to granularly track and opt-out data

What all of this means is that mobile developers will need to ensure that they have a way to granularly track personal information at the individual user level as it moves within their systems and their partners'. So, if a consumer requests an app to delete their consumer data, the company itself needs to be able to find it and delete it internally, but also needs a way to ensure copies of that data held by service providers will also be deleted.

Developers need to build functionality into their apps to make it possible for users to request access or deletion, and to request data isn't sold to third-parties.

But not only that, they need code-based mechanisms on the back-end to automatically carry out those tasks across the app's ecosystem.

Doing all of this on an individual user level could add a tremendous amount of complexity to the mobile business. Some developers may be tempted to avoid that high cost of compliance by taking the nuclear option and simply opting out all of their users voluntarily—in other words, ceasing collection of any identifiable information about users. That might be an option, but app makers should be mindful that this choice will bring unintended consequences. It will likely cripple their ability to carry on with valuable analytics programs and it could make it difficult to use certain free developer services. It may also interrupt certain monetization methods that require sharing data with advertisers and other partners.

This is why preparing with a granular tracking and opt-out method will prove to be extremely important as developers move forward in this new CCPA era.

Some developers may be tempted to avoid that high cost of compliance by taking the nuclear option and simply opting out all of their users voluntarily—but this choice will bring unintended consequences.

There could be more data privacy legislation and platform changes coming soon

CCPA and GDPR are just the start of a new era in data privacy regulations. Other states and countries are also working to update or implement their own strongly fashioned data handling legislation.

When GDPR first went live in 2018, many developers outside of the EU made the business decision to avoid the regulatory complexity and simply block European residents from accessing their apps. It was a quick fix, but it's not a sustainable one in this new global regulatory environment. CCPA is another data privacy domino to fall, and its existence will likely topple over others in its wake. Each subsequent piece of rulemaking will likely come with its own slightly different requirements and tweaks.

As such, developers can no longer afford to take an avoidance strategy.

They need to be ready to respond with a code-based framework and business plan that can help them comply with the kind of data transparency and controls that will satisfy regulators long term.

How mobile developers can prepare for CCPA and beyond

Do a data inventory

Start surveying all of the data that your app is collecting about people and all of the third parties that you're integrating SDKs with. Make a determination about which ones are high-risk and low-risk from a CCPA compliance standpoint. From there, start planning now how you'll provide users access and deletion to the data.

Make your platform as flexible as possible

Start surveying all of the data that your app is collecting about people and all of the third parties that you're integrating SDKs with. Make a determination about which ones are high-risk and low-risk from a CCPA compliance standpoint. From there, start planning now how you'll provide users access and deletion to the data.

Vet your third-parties SDKs for CCPA compliance

Developers must ensure at a code level that their data sharing arrangements don't put them at risk of running afoul of CCPA. This means vetting all third-party SDKs to ensure that they're compliant and that they provide the integrations that the developer needs to opt-out users and delete their data when necessary. As a point of example, the Flurry SDK has an opt-out API that indicates whether the user has opted out of data sharing or not, along with APIs to receive data deletion requests from customers. For more information on CCPA compliance using the Flurry SDK, please review **this documentation**.

Simplify data deletion for customers

Customer experience should always be tantamount for developers, even when it comes to CCPA compliance. In order to maintain the best experience for users, developers should think about ways to simplify requests for data access, deletion, and opting out of data sale. This means offering an easy menu of options within the app, and the assurance that this request will be done across all third-party relationships. On the back end, the developer should also be doing work to clearly maintain the state of opt-in/opt-out status for all of their users.

Brace for monetization impacts

The cost of compliance could be high for some developers and not everyone has the wherewithal to build do-not-sell controls into their apps. For developers that depend upon advertising and data sharing to generate revenue and who don't believe they can weather the storm, it may be time to come up with creative monetization alternatives. Some may choose to lean more heavily toward a subscription model—though that brings with it its own data privacy concerns. Nevertheless, CCPA will likely reshape how mobile developers plan for monetization.

How Flurry can help

As a key partner in the app analytics market, Flurry closely tracks the progress of CCPA and the interpretation coming from legal experts. Our team has prepared our platforms and business process to ensure that data handling is compliant with the CCPA. We're prepared to offer the kind of data access rights CCPA requires across all of the consumers that use the hundreds of thousands of different apps we work with. In addition, we've worked to create options in our SDK that provide easy opt-out options for developers to bake CCPA compliance into their apps. You can find more information **here**.

FLURRY