10 Reasons Why the California Consumer Privacy Act (CCPA) Is Going to Be a Dumpster Fire
July 1, 2019
Alec Stapp

Last year, real estate developer Alastair Mactaggart spent nearly $3.5 million to put a privacy law on the ballot in California’s November election. He then negotiated a deal with state lawmakers to withdraw the ballot initiative if they passed their own privacy bill. That law — the California Consumer Privacy Act (CCPA) — was enacted after only seven days of drafting and amending. CCPA will go into effect six months from today.

According to Mactaggart, it all began when he spoke with a Google engineer and was shocked to learn how much personal data the company collected. This revelation motivated him to find out exactly how much of his data Google had. Perplexingly, instead of using Google’s freely available transparency tools, Mactaggart decided to spend millions to pressure the state legislature into passing new privacy regulation.

The law has six consumer rights, including the right to know; the right of data portability; the right to deletion; the right to opt-out of data sales; the right to not be discriminated against as a user; and a private right of action for data breaches.

So, what are the law’s prospects when it goes into effect next year? Here are ten reasons why CCPA is going to be a dumpster fire.

1. CCPA compliance costs will be astronomical

“TrustArc commissioned a survey of the readiness of 250 firms serving California from a range of industries and company size in February 2019. It reports that 71 percent of the respondents expect to spend at least six figures in CCPA-related privacy compliance expenses in 2019 — and 19 percent expect to spend over $1 million. Notably, if CCPA were in effect today, 86 percent of firms would not be ready. An estimated half a million firms are liable under the CCPA, most of which are small- to medium-sized businesses. If all eligible firms paid only $100,000, the upfront cost would already be $50 billion. This is in addition to lost advertising revenue, which could total as much as $60 billion annually.” (AEI / Roslyn Layton)
2. CCPA will be good for Facebook and Google (and bad for small ad networks)

“It’s as if the privacy activists labored to manufacture a fearsome cannon with which to subdue giants like Facebook and Google, loaded it with a scattershot set of legal restrictions, aimed it at the entire ads ecosystem, and fired it with much commotion. When the smoke cleared, the astonished activists found they’d hit only their small opponents, leaving the giants unharmed. Meanwhile, a grinning Facebook stared back at the activists and their mighty cannon, the weapon that they had slyly helped to design.” (Wired / Antonio García Martínez)

“Facebook and Google ultimately are not constrained as much by regulation as by users. The first-party relationship with users that allows these companies relative freedom under privacy laws comes with the burden of keeping those users engaged and returning to the app, despite privacy concerns.” (Wired / Antonio García Martínez)

3. CCPA will enable free-riding by users who opt out of data sharing

“[B]y restricting companies from limiting services or increasing prices for consumers who opt-out of sharing personal data, CCPA enables free riders—individuals that opt out but still expect the same services and price—and undercuts access to free content and services. Someone must pay for free services, and if individuals opt out of their end of the bargain—by allowing companies to use their data—they make others pay more, either directly or indirectly with lower quality services. CCPA tries to compensate for the drastic reduction in the effectiveness of online advertising, an important source of income for digital media companies, by forcing businesses to offer services even though they cannot effectively generate revenue from users.” (ITIF / Daniel Castro and Alan McQuinn)

4. CCPA is potentially unconstitutional as-written

“[T]he law potentially applies to any business throughout the globe that has/gets personal information about California residents the moment the business takes the first dollar from a California resident. Furthermore, the law applies to some corporate affiliates (parent, subsidiary, or commonly owned companies) of California businesses, even if those affiliates have no other ties to California. The law’s purported application to businesses not physically located in California raises potentially significant dormant Commerce Clause and other Constitutional problems.” (Eric Goldman)

5. GDPR compliance programs cannot be recycled for
CCPA

“[C]ompanies cannot just expand the coverage of their EU GDPR compliance measures to residents of California. For example, the California Consumer Privacy Act:

- Prescribes disclosures, communication channels (including toll-free phone numbers) and other concrete measures that are not required to comply with the EU GDPR.
- Contains a broader definition of “personal data” and also covers information pertaining to households and devices.
- Establishes broad rights for California residents to direct deletion of data, with differing exceptions than those available under GDPR.
- Establishes broad rights to access personal data without certain exceptions available under GDPR (e.g., disclosures that would implicate the privacy interests of third parties).
- Imposes more rigid restrictions on data sharing for commercial purposes.”

(IAPP / Lothar Determann)

6. CCPA will be a burden on small- and medium-sized businesses

“The law applies to businesses operating in California if they generate an annual gross revenue of $25 million or more, if they annually receive or share personal information of 50,000 California residents or more, or if they derive at least 50 percent of their annual revenue by “selling the personal information” of California residents. In effect, this means that businesses with websites that receive traffic from an average of 137 unique Californian IP addresses per day could be subject to the new rules.” (ITIF / Daniel Castro and Alan McQuinn)

CCPA “will apply to more than 500,000 U.S. companies, the vast majority of which are small- to medium-sized enterprises.” (IAPP / Rita Heimes and Sam Pfeifle)

7. CCPA’s definition of “personal information” is extremely over-inclusive

“CCPA likely includes gender information in the “personal information” definition because it is “capable of being associated with” a particular consumer when combined with other datasets. We can extend this logic to pretty much every type or class of data, all of which become re-identifiable when combined with enough other datasets. Thus, all data related to individuals (consumers or employees) in a business’ possession probably qualifies as “personal information.” (Eric Goldman)

“The definition of “personal information” includes “household” information, which is
particularly problematic. A “household” includes the consumer and other co-habitants, which means that a person’s “personal information” oxymoronically includes information about other people. These people’s interests may diverge, such as with separating spouses, multiple generations under the same roof, and roommates. Thus, giving a consumer rights to access, delete, or port “household” information affects other people’s information, which may violate their expectations and create major security and privacy risks.” (Eric Goldman)

8. CCPA penalties might become a source for revenue generation

“According to the new Cal. Civ. Code §1798.150, companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay statutory damages between $100 to $750 per California resident and incident, or actual damages, whichever is greater, and any other relief a court deems proper, subject to an option of the California Attorney General’s Office to prosecute the company instead of allowing civil suits to be brought against it.” (IAPP / Lothar Determann)

“According to the new Cal. Civ. Code §1798.155, companies can be ordered in a civil action brought by the California Attorney General’s Office to pay penalties of up to $7,500 per intentional violation of any provision of the California Consumer Privacy Act, or, for unintentional violations, if the company fails to cure the unintentional violation within 30 days of notice, $2,500 per violation under Section 17206 of the California Business and Professions Code. Twenty percent of such penalties collected by the State of California shall be allocated to a new “Consumer Privacy Fund” to fund enforcement.” (IAPP / Lothar Determann)

“[T]he Attorney General, through its support of SB 561, is seeking to remove this provision, known as a “30-day cure,” arguing that it would be able to secure more civil penalties and thus increase enforcement. Specifically, the Attorney General has said it needs to raise $57.5 million in civil penalties to cover the cost of CCPA enforcement.” (ITIF / Daniel Castro and Alan McQuinn)

9. CCPA is inconsistent with existing privacy laws

“California has led the United States and often the world in codifying privacy protections, enacting the first laws requiring notification of data security breaches (2002) and website privacy policies (2004). In the operative section of the new law, however, the California Consumer Privacy Act’s drafters did not address any overlap or inconsistencies between the new law and any of California’s existing privacy laws, perhaps due to the rushed legislative process, perhaps due to limitations on the ability to negotiate with the proponents of the Initiative. Instead, the new Cal. Civ. Code §1798.175 prescribes that in case of any conflicts with California laws, the law that affords the greatest privacy protections shall control.” (IAPP / Lothar Determann)
10. CCPA will need to be amended, creating uncertainty for businesses

As of now, a dozen bills amending CCPA have passed the California Assembly and continue to wind their way through the legislative process. California lawmakers have until September 13th to make any final changes to the law before it goes into effect. In the meantime, businesses have to begin compliance preparations under a cloud of uncertainty about what the says today — or what it might even say in the future.

View Article