IRONCORE LABS

CCPA: WHAT YOU NEED TO KNOW

A white paper on California's new data privacy law

CONTENTS

DISCLAIMER: This is not legal advice and does not substitute for it. We are not lawyers.

EXECUTIVE SUMMARY

The California Consumer Privacy Act (aka CCPA or AB 375) of 2018 shot through the California legislature in seven days. It was going to be on the November ballot and legislators feared it would become law without any opportunity for stakeholders (lobbyists and such) to weigh in and help shape it. The sponsors of the initiative agreed to take it off the ballot if the legislature would pass the bill within a deadline, which they did. In the process, they watered parts down, such as eliminating monetary rewards for whistle-blowers.

Does it even matter?

This law doesn't apply to all businesses. It's primarily targeted at large tech companies and data brokers. Where it does apply, it's possible and maybe even likely that the law will be preempted or watered down before it goes into effect.

CCPA is under attack on a number of fronts. First, the state legislature is actively amending it. Large tech companies like Facebook, who spent $200,000 to try to stop the law despite publicly declaring to be in favor of it, are influencing these amendments. They are also trying to get the California Attorney General, who has rule making and interpretation powers, to issue rules that undercut core principles and penalties. For example, one fight is over the interpretation of the term "violation," which is the unit size of most of the penalties. The original bill writers intended this to count per-person per-event, but there is lobbying underway to instead make this just be per event.

> *Anyone that bets this law will be radically watered down or preempted is likely underestimating the current privacy backlash or overestimating bipartisan cooperation.*

Large tech companies and data brokers are also undercutting the bill at the national level. Lobbyists are pushing the U.S. Congress to enact a privacy law that preempts the California one. Even in a divided Washington, there's broad support for federal tech regulation and privacy protections. There's a chance they enact a law before January 1st, 2020, which is when the California law is scheduled to take effect, and that the Federal law expressly preempts the California one, as most of the lobbyists want.

A Federal law could be much more business friendly and much less protective of consumer privacy. The CCPA provisions around fines, amount of disclosure, and around portability are all under attack in Washington.

Despite the uncertainties, work towards CCPA compliance should start now. Specifically, all sales of data must be tracked for 12 months before the law takes effect, which means disclosures will go back to January 1st, 2019.

So does it matter? It does. This is a landmark law that at the least will influence future legislation. Anyone that bets this law will be radically watered down or preempted is likely underestimating the current privacy backlash or overestimating bipartisan cooperation. It could happen, but that's far from certain.

What does it do?

Although CCPA has been described as GDPR-light, it is in no way light on requirements or penalties. CCPA is focused on these core principles:

1. **Transparency:** consumers get to know what data is collected and for what purpose(s). If the data is sold or shared, they will know the details of what and to whom. Consumers even get to know if a company has sold data to anyone in the last 12 months even if the practice has since stopped.

2. **Control:** consumers get the right to opt-out (or opt-in for minors) of the sale of their data. Consumers also have the right to see their data and the right to have it erased.

3. **Data security:** companies are liable for both fines and civil suits (individual or in classes) for any personal information that they fail to protect from hackers or other misuse (i.e., internal employees looking at data without a business purpose for doing so).

It's worth noting that the data security provisions of CCPA were added as a result of the Equifax breach. Equifax reserved about $2 per affected person to pay for the fallout and, in all likelihood, would make money off the breach by offering their own credit monitoring service to affected customers. CCPA would significantly increase those penalties.

What are the penalties?

If a company does not adhere to the consumer rights in the bill, they can be fined **$2,500 per violation**, which the writers of the law intended to mean to be per person per incident. There are provisions for this to be adjusted down in some cases and at the discretion of the Attorney General.

If the violations are found to be willful, like if executives intentionally decided not to disclose a sale of data, then the penalty **can be up to $7,500 per violation**. A company that intentionally sells the data of 50,000 consumers and willfully fails to disclose that fact, would face up to a $375 million fine.

If a business is breached, a private right of action is given to consumers to sue for the greater of actual damages, or **an amount between $100 and $750 per record**. In the case of the Equifax breach, where 148 million consumers (56% of American adults) were impacted, a theoretical class action suit would result in damage awards between $14.8 billion and $111 billion -- except, in practice, only California residents could bring suit. Even so, with 40 million residents, 31 million adults, and assuming only 56% of those were impacted, Equifax could face $13.1 billion in damages. This is quite a bit more than the $300 million they set aside.

What businesses are impacted?

The law is generally aimed at two classes of businesses:

1. **Data brokers:** companies that either make a majority of their revenue by selling personal information of consumers or that trade (obtain, sell, or barter) more than 50,000 records per year.

2. **Medium and large companies:** companies with greater than $25 million in annual gross revenues.

That means that the vast majority of small businesses, including most tech startups, are unaffected.

Executive Conclusion

CCPA's biggest contribution will be a huge increase in transparency of data collection and behind-the-scenes flows of that data. Consumers don't have to give over their data unless absolutely required for the service, which means things like giving up an email address before getting access to a white paper will no longer be lawful. And buying credit monitoring services will no longer be sufficient to stop damages and individual lawsuits. Most importantly, the law is likely to spread well beyond residents of California and to change many practices in the tech industry. Compliance initiatives should start immediately.

A good privacy platform, such as IronCore's developer-focused data control solution, can help companies meet many of the CCPA obligations and other compliance needs as well.

CCPA DEEP DIVE

As always, the devil is in the details. This is not meant to be a comprehensive list of details, but rather a survey of the most interesting parts of the law as a reference for anyone who is looking to kick off a compliance initiative.

Consumer Rights

The law spells out a number of rights. They don't name them, but we do:

- **Right to deletion:** A consumer can request deletion of their personal information and barring a good reason not to, the business must comply.
- **Right to know details:** A consumer has the right to know exactly what data is collected both in specifics and in terms of the categories of data held.
- **Right to know source:** A consumer may learn the categories of sources from which the data was obtained, which will help consumers find data sources and opt out.
- **Right to know purpose:** A consumer has the right to know the purpose for why data is collected, why it is being sold, and how it will be used.
- **Right to know sharing:** A consumer has the right to know with whom their data is shared.
- **Right to portability:** A consumer may request a copy of their data and it must be provided in a portable and readily usable format. Unlike with GDPR, a company cannot charge for this.

> “*The vast majority of small and mid-size businesses, including most tech startups, are unaffected.*

- **Right to private action:** A consumer has the right to sue a company if their data is breached. A pending amendment would, if passed, also grant consumers the right to privately sue for privacy-related failures.
- **Right to opt out:** A consumer has the right to opt out of the sale of their personal information. For children 16 years old or younger, they or a guardian must first opt-in before their data can be sold.
- **Right of opt-out delegation:** A consumer may enlist a third-party person or organization to request opt outs on their behalf.

Covered Data

Under CCPA, almost any data related to a consumer is considered to be “personal information.” Additionally, the list of information that is considered to be “identifiable,” which matters for deidentification purposes, is long. Personal information includes real name, alias, online identifier, IP address, email address, health information, financial information, social security numbers, location information, biometric data, audio and visual data (photos, recordings), activity information, history data, and any inferences that can be made from any of this information or combinations thereof.

Consumers Covered

All residents of California even when they’re traveling.

Businesses Covered

Applies to businesses in California, those that process information or buy or sell it in California, and those that hold the data of residents of California. If any part of a business or its customer base crosses into California, the law applies.

Additionally, a company must meet ***any one of a set of criteria*** before most of the provisions of the law kick in:

- **Medium to Large company:** gross revenues over $25 million; or
- **Data broker:** annually obtains, sells, or shares personal information of at least 50,000 consumers; or
- **Data vendor:** derives more than half of its revenue from selling personal information.

These qualifiers effectively exempt most small businesses and tech startups from the various provisions unless the startup is selling user data.

Obligations of a Covered Business

For large businesses, it’s likely that they’ve already undergone GDPR compliance efforts. With the exception of some very specific details like required home page links and categorizations of information and partners, these companies should have very little incremental work. That said, there are a number of key obligations that covered businesses must expressly handle to be compliant with CCPA:

1. **Disclosure of rights:** on websites and in privacy policies, companies must disclose the consumer rights in a way that is "reasonably accessible to consumers" (i.e., not buried in legal docs alone). This includes disclosing the rights to delete, to ask for data, to opt-out, etc.

2. **Disclosure of data use:** at or before the point of collection, companies must inform consumers as to the categories of personal data to be collected and the purposes for which each category of personal data will be used. The disclosure has to be specific about which information will be shared or disclosed, including the categories of partners that it will be shared with and the business purpose for the sharing.

3. **Disclosure of data sales:** even if information is no longer being sold and policies around sharing of information have changed, a company must update their privacy policy every 12 months to disclose any personal information that was sold in the preceding 12 months or to expressly state that no data was sold if that's the case. This disclosure reaches back to January 1st, 2019.

4. **Respond to information requests:** businesses must provide at least two different methods including, at a minimum, a toll free telephone number and, if applicable, a web address through which consumers can make their CCPA requests. A response to a request for copies of personal information being held must be prompt and free of charge unless the requests are unfounded or excessive. Material must be provided in a portable and readily usable format. Company has 45 days to provide the data and may, with written notice, gain a single 45 day extension. A request for data must not require account creation.

5. **Respond to erasure requests:** and cascade those requests through to any service providers so they, too, delete the consumer's records. In other words, if you share the data or store it with a 3rd party, you have to ask them to also delete it.

6. **No resale:** any personal information that was obtained through a third-party may not be resold or shared unless the consumer has received explicit notice and is first given the opportunity to opt out.

7. **Provide opt-out:** consumers can elect to not have their data ***sold or shared***. Businesses cannot discriminate against consumers who opt out by denying them goods or services or by providing a different level of quality or by charging different prices unless the data is expressly needed to provide the product or service. This does not eliminate the ability of a service to be ad supported or to have an ad-supported pricing tier, however.

A clear and conspicuous link on the business's home page must exist and be titled, "Do Not Sell My Personal Information." That link must allow a consumer to opt out without creating an account.
Note 1: this calls into question the practice of making someone give their name and email before they can download a white paper.
Note 2: a business may keep information that is needed in order to honor an opt-out request.

> *This calls into question the practice of making someone give their name and email before they can download a white paper.*

8. **No nagging:** opt out requests must be honored for 12 months before asking the consumer to reconsider.

9. **Contracts with 3rd-parties:** CCPA has a bit of a viral aspect in that it requires companies that are covered to have contracts with any partners with whom personal information is shared that expressly forbid the selling of information that is held on behalf of the company. The contracts must also forbid any use of the data outside of the specific business purpose of the relationship. The 3rd-party must sign a separate statement expressly certifying that they understand the CCPA regulations and that they are forbidden from using the personal information.

10. **Explanations:** If any consumer requests are denied, the consumer must be told why. For example, if they didn't prove their identity sufficiently or if there's another reason why the data must not be deleted, that has to reflect back to the consumer.

11. **Data protection:** procedures and practices must be implemented and maintained to protect personal information from unauthorized access. This one is vague and talks about a "duty to implement and maintain ***reasonable*** security procedures." That one word is the fulcrum point upon which any data breach litigation will hinge.

Enforcement / Penalties

Civil Penalties

Civil penalties will be pursued by the California Attorney General (AG), who has a high degree of latitude in terms of levels of penalty sought, rule writing, and interpretations. For example, in the case of data security, the law is intentionally vague to allow the definition of "reasonable practices" to evolve over time as attacks and counter-measures evolve.

Any company failing to meet the obligations of CCPA will first get a warning letter from the

AG giving them 30 days to remedy the issue.

If, after the 30 day period, the non-compliance issues remain, the AG may seek up to $2,500 per violation. The writers of the law intended that to mean per consumer per event, but the final definition will be made by the AG before the law kicks in. If the AG believes the non-compliance to be intentional, then the maximum fines may increase to $7,500 per violation.

Any collected fines go into a dedicated Consumer Privacy Fund that will pay for the AG's efforts in this area.

In the case of a data breach, the AG may seek penalties in addition to the private right of action explained below.

Private Right of Action

Individuals or groups of individuals in a class may directly sue companies who are responsible for unauthorized access to their personal information. In other words, if a company is hacked and personal information is stolen, then the ultimate victims of the theft, the individuals whose information was stolen, can seek compensation.

There are three cases where companies may not be liable:

- **Encrypted:** The accessed data was encrypted and attackers couldn't decrypt.
- **Deidentified:** The accessed data was redacted or otherwise deidentified.
- **Well protected:** The company had "reasonable" practices and procedures in place to protect the data.

Damages in such a suit will be **no less than $100** per record per incident and **no more than $750 per record per incident** or actual damages if they should be greater.

Exemptions / Exceptions

- **Consumer verification:** A business may deny a request for data or erasure if they are unable to verify that a consumer (or agent of a consumer) making the request is who they say they are.
- **Conflicting law:** A business may retain data that is required to meet Federal laws such as HIPAA and GLBA.
- **Public records:** Any records that are public, such as if they are lawfully made avail-

able by Fed/state/local Government (i.e., property records) may be retained.

- **Excessive requests:** Need not provide information if a consumer requests info more than twice in 12 months.
- **Contractual need:** Need not delete data that is required to complete a transaction or a contract in an ongoing relationship with the consumer.
- **Intrusion or fraud detection:** Need not delete data if it is required for detection of security incidents or fraud.
- **1st amendment:** Need not delete data if it would infringe on another consumer's right to free speech.
- **Research:** Need not delete data that is needed for public interest research.
- **Law enforcement:** Must not delete data that is needed to comply with a legal obligation such as a law enforcement request.
- **Deidentified:** Need not delete data that is deidentified or aggregated provided it can't be re-identified and that the company takes the following measures to ensure that: 1) technical safeguards; and 2) business processes that prohibit reidentification; and 3) business processes that prevent the release of such data.
- **Outside California:** If data is collected and processed outside of CA and doesn't pertain to a CA resident. Note: can't hold data on a device until a resident leaves the state and then transmit it.

DATA SECURITY EXAMPLE

This law very much had Equifax in mind when the data security component was added, per two of the writers of the original law. Since then, much more has come out about the Equifax breach, including the "*Equifax Data Breach Report*" by the Congressional House Oversight Committee.

Equifax is an interesting case study because, by all accounts, they invested quite a bit in security. They had numerous teams including a "Global Threat and Vulnerability Management" team. They had intrusion detection in place, scanners searching for out of date software, and more.

> “ *Sometimes it's hard to see how broken a system is until it fails spectacularly.*

In the CCPA, the security requirement is to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." They certainly implemented a number of security practices. But they fell down in the maintenance side.

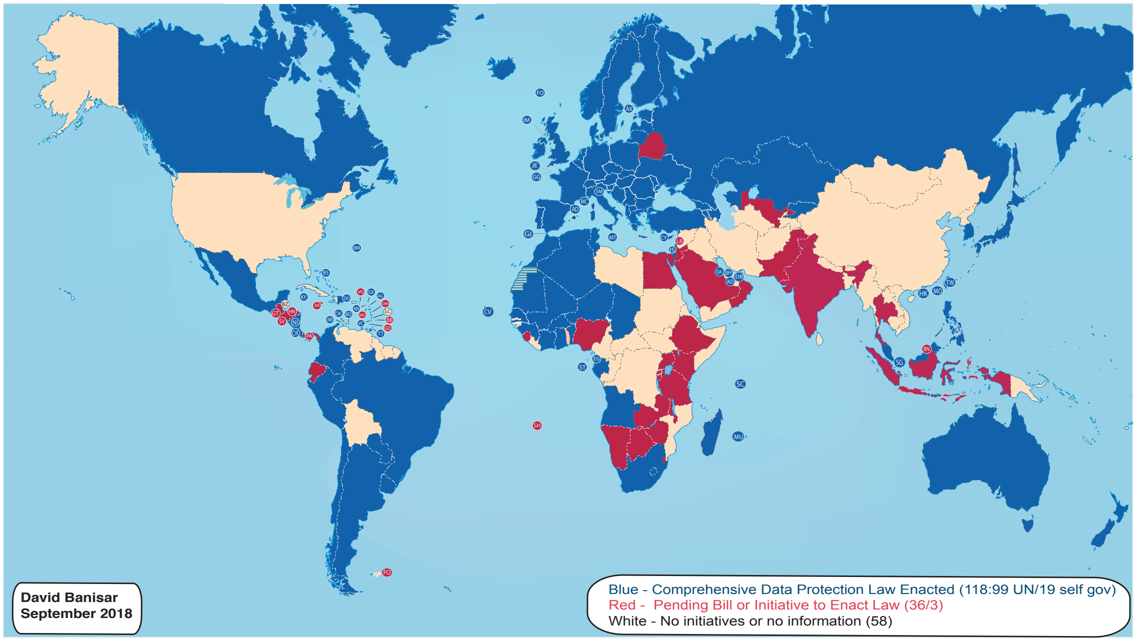
For example, they were slow to respond to new vulnerabilities, their intrusion detection software had not been working for 19 months, their scans for vulnerable software weren't configured correctly and were falsely reporting a lack of issues. They also didn't encrypt the sensitive personal information they held on consumers.

These things led to the damning conclusion of the Congressional report: "*Equifax, however, failed to implement an adequate security program to protect this sensitive data. As a result, Equifax allowed one of the largest data breaches in U.S. history.* ***Such a breach was entirely preventable***."

Sometimes, it's hard to see how broken a system is until it fails spectacularly. This was an organization who spent a lot on security, but ultimately failed to manage the complexities of their environment. It's easy to imagine CCPA leading to massive class action awards with penalties in the billions for this kind of mismanagement. What Equifax was doing for security, on the surface, sounded "reasonable," but after a breach, it became clear that what they were doing was far from sufficient and that they did not maintain reasonable security.

GLOBAL CONTEXT

National Comprehensive Data Protection/Privacy Laws and Bills 2018


David Banisar
September 2018
Blue - Comprehensive Data Protection Law Enacted (118:99 UN/19 self gov)
Red - Pending Bill or Initiative to Enact Law (36/3)
White - No initiatives or no information (58)

California's newest privacy law is just one of many. Over 100 countries have enacted data privacy laws and dozens more have legislation pending.

Contrary to the map above, the U.S. does have pending data privacy legislation, and that's in addition to a patchwork of laws with privacy requirements for the handling of health care data (HIPAA), financial data of public companies (SOX), data on students (FERPA), children (COPPA), and numerous state laws.

For companies who have customers that operate around the world, the complexity of complying with these laws is daunting and getting worse almost daily.

At a macro level, the overriding theme of these laws is putting the control of a consumer's data into the hands of the consumer so that they know how their data is used and can object to it. We believe in most cases this also gives businesses better control of their data held by third parties.

In this macro sense, CCPA is unexceptional.

Another common theme of these laws is the requirement to protect data from being exposed to unauthorized people. In nearly every case, there is a specific clause that calls out the idea that a company has not failed their responsibility if the thieves can only see personal data in encrypted or deidentified form.

Moving forward, companies will need to significantly increase the amount of their infrastructure that is non-transparently encrypted.

FURTHER READING

Alastair Mactaggart and Ashkan Soltani, two of the folks most responsible for making CCPA happen, maintain a website that's all about CCPA and the ongoing battles:

https://www.caprivacy.org/

If you'd like to read the actual bill, you'll need to first read the bill that passed in Summer 2018, and then read each of the amendments. These two links will get you started:

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB1121

IRONCORE LABS

ABOUT IRONCORE

We are a data privacy platform for application layer encryption and customer managed keys (CMK). We enable software developers and businesses to rapidly build enterprise applications with strong data control. Data owners decide who can access their data, monitor how it's used, when, where, and by whom, and can revoke that access at any time. We are the fastest and easiest way to control data in multi-cloud and SaaS environments.

IronCore Labs
1750 30th Street #500
Boulder, CO 80301, USA

Inquiries
Email: info@ironcorelabs.com
Phone: +1.415.968.9607

CONNECT WITH US

blog.ironcorelabs.com
linkedin.com/company/ironcore-labs
twitter.com/ironcorelabs
ironcorelabs.com