Last Minute Tips for Procrastinators: What Your Company Needs to Know about the California Consumer Privacy Act ("CCPA")

If your company is like many, you have known about the upcoming effective date of the California Consumer Privacy Act ("CCPA"), but are still making last minute preparations in advance of it going into effect.

If you are one of many procrastinators out there just starting to think about the law, here is a recap of some highlights for you:

- Your business is subject to the law, regardless of its location, if any one of the following is true:
  - Your company has gross annual revenues in excess of $25 million.
  - Your company buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices.
  - Your company derives 50 percent or more of its revenues from selling consumers' personal information.
- The CCPA creates new rights for California consumers: (a) the right to know; (b) the right to delete; (c) the right to opt out; and (d) the right to non-discrimination.
- You must provide notice to consumers at or before the point of data collection of the personal information to be collected and the purposes it will be used.
- You must provide clear and conspicuous notice to

consumers of the right to opt out of the sale of personal information, which includes providing a “Do Not Sell My Personal Information” link on the website or mobile application.

- You must respond to requests for consumers to know, delete, and opt-out within specified timeframes (generally 45 days). Privacy settings to opt out must be treated as a validly submitted opt out request.
- You must verify the identity of consumers who make requests to know or to delete, regardless of any password-protected account settings with the business.
- You must disclose any financial incentives offered in exchange for the retention or sale of a consumer’s personal information, explain how the value of the personal information is calculated, and explain how the incentive is permitted under the CCPA.
- You must make available to consumers at least two or more designated methods for submitting requests, including at a minimum a toll-free phone number, and if you maintain a website, a website address by which to submit requests. However, a business that operates exclusively online and has a direct relationship with the consumer from who it collects personal information is only required to provide an email address.
- You must make your privacy policy accessible to consumers with disabilities, or to provide consumers with disabilities information on how they can access the policy in an alternative format.
- You must make your privacy policy available in a format where consumers can print it out in a separate document.
- You must ensure that the privacy policy explains how a consumer can designate an authorized agent to make a request on the consumer’s behalf.
- You must retain records of all requests and responses to requests for at least 24 months; provided that businesses that buy or sell personal information of more than 4 million consumers annually have additional

reporting obligations.

Also, if your business qualifies as a “data broker” you are required to register with the Attorney General by January 1, 2020. How do you know if your business is a “data broker”? Your business knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Three categories of businesses are excluded from these obligations: (i) consumer reporting agencies to the extent they are covered by the Fair Reporting Act; (ii) financial institutions to the extent they are covered by the Gramm Leach Bliley Act; and (iii) entities covered by the Insurance Information and Privacy Protection Act.

The CCPA, its amendments, and regulations define more compliance obligations that businesses should be familiar with, but this list is a good starting point in advance of the effective date.

Obviously, even if your business is not subject to these laws, these privacy requirements will now constitute the best practices for doing business in California, so all businesses should seriously consider incorporating these privacy practices into their standard privacy practices and procedures.

California Finalizes California Consumer Privacy

Act ("CCPA")

In anticipation of the **California Consumer Privacy Act** ("CCPA") going into effect on January 1, 2020, California Governor Gavin Newsom has just signed into law seven amendments to the statute, and the California Department of Justice published the text of its new regulations to be adopted in furtherance of the CCPA.

The signed bills are as follows: **AB 25**, **AB 874**, **AB 1146**, **AB 1355**, **AB 1564,** and **AB 1130.** The text of the published regulations are made available **here**. The deadline to submit written comments is 5 p.m. on December 6, 2019. California is accepting comments submitted in accordance with the instructions posted on this Office of the Attorney General website: **https://www.oag.ca.gov/privacy/ccpa.**

So now that there is a little more statutory and regulatory clarity on what exactly will be going into effect on January 1st, 2020, SaaS and tech companies are in a better position to start preparing for the law to take effect.

CCPA Compliance Requirements

So, what does your SaaS or tech company need to know about complying with the California law as of January 1, 2020, as the California privacy laws collectively stand today?

First of all, your business will be subject to the law if at least one of the following are true:

- Your company has gross annual revenues in excess of $25 million;
- Your company buys, receives, or sells the personal information of 50,000 or more consumers, households or devices;
- Your company derives 50 percent or more of its revenues from selling consumers' personal information.

"Consumer" is currently defined as a natural person who is a California resident. "Personal information" is currently defined as any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirect, with a particular consumer or household" and includes not only name, address, and social security number, but also purchasing history or tendencies, biometric information, internet activity, geolocation data, employment information, and education information. However, publicly available information and de-identified or aggregate consumer information is now specifically excluded from the definition. "Business" is currently defined to include for-profit businesses as well as other legal entities.

CCPA Consumer Rights

Second all, California consumers are going to have certain new rights that your business will be responsible for ensuring:

- A **Right to Know** (a) the specific pieces of personal information the business has collected about the consumer; (b) the categories of personal information it has collected or sold about that consumer; (c) the purpose for which it collected or sold the categories of personal information; and (d) the categories of third parties to whom it sold the personal information.
- A **Right to Delete** personal information held by your business or by a service provider of your business; provided that, however, there will be some exceptions, where it is necessary for your business or service provider to do any of the following: (a) complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with consumer, or

otherwise perform a contract between the business and the consumer; (b) detect security incidents; protect against malicious, deceptive fraudulent, or illegal activity; or prosecute those responsible for that activity; (c) debug to identify and repair errors that impair existing functionality; (d) exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law; (e) comply with the California Electronic Communications Privacy Act; (e) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent; (f) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; (g) to comply with a legal obligation; or (h) to otherwise use consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. If you or your service provider does not delete consumer's information upon request, you must inform the consumer as to why and notify the consumer of any rights he or she has to appeal the decision, and you must do it within the timeframe you would have had to delete the information.

- A **Right to Opt Out of the Sale** of personal information. "Sale" is defined to include selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other consideration. The proposed regulations provide more clarification on

the practices businesses should follow to ensure this right to opt out of the sale. In the case of children under the age of 16, your business cannot sell their personal information unless they have opted-in to the sale. In the case of children under 13, a parent or guardian must opt-in on behalf of the child. The proposed regulations further define the rules related to the protection of children.

- A **Right of Non-Discrimination**. Your business will be prohibited from discriminating against a consumer for exercising his or her rights under the CCPA. Discrimination will be defined to include denying goods or services to the consumer, charging different prices or rates for goods or services, providing a different level or quality of goods or services to the consumer, or suggesting that the consumer will receive a different price or quality of goods or services; provide that you will be able to charge a different price or rate, provide a different level or quality of goods or services, or offer financial incentives if the difference is reasonably related to the value provided to the business by the consumer's personal data, so long as the business practice is not unjust unreasonable, coercive, or usurious in nature. The proposed regulations further define how the right of non-discrimination will be implemented.

CCPA Business Obligations

Third, businesses will now have other new business obligations to consumers, including the following:

- Provide notice to consumers at or before the point of collection of the categories of personal information to be collected from them and the purposes they will be used.
- Provide clear and conspicuous notice to consumers of the right to opt-out of the sale of personal information in

the form of a “Do Not Sell My Personal Information” link on their website or mobile application.

- Respond to requests from consumers to know, delete, and opt-out within the specified timeframe (generally 45 days). The proposed regulations require businesses to treat privacy settings to opt out selected by a consumer as a validly submitted opt out request.
- Make available to consumers at least two or more designated methods for submitting requests for information, including at a minimum, a toll-free phone number, and also specify other business practices for handling requests by consumers.
- Verify the identity of any consumer making a request to know or delete. Password protected account settings are not considered sufficient verification. The proposed regulations require a business unable to verify a request to comply to the greatest extent it can even if it denies a request.
- Disclose financial incentives offered in exchange for the retention or sale of consumer’s personal information (as specified by the proposed regulations), including a short summary of the incentive, a description of the summary and the categories of personal information impacted, an explanation of how a consumer can opt-in to the incentive, a notice to consumer that he or she has the right to withdraw at any time and how he or she can exercise this right, and an explanation of why the incentive is permitted under California privacy law.
- Retain records of all requests and responses to those requests for at least 24 months; provided that businesses (alone or in combination) collecting, buying or selling the personal information of more than 4 million consumers annually are subject to extra recordkeeping obligations.
- Disclose a privacy policy which describes consumer’s rights under California privacy law, how to submit requests to exercise rights under California privacy

law, and information regarding their data collection and sharing practices. The proposed regulations define additional requirements for the privacy policy, including that it must be accessible to consumers with disabilities or provide consumers with disabilities information on how they can access the policy in an alternative format; that it must be in a format where consumers can print it out as a separate document; it must explain the right of a consumer not to receive discriminatory treatment; and it must explain how a consumer can designate an authorized agent to make a request on the consumer's behalf under California privacy law.
- Train employees or contractors handling consumer requests on compliance with California privacy law and directing consumers to exercise their rights under California privacy law; provided that businesses collecting, buying or selling the personal information of more than 4 million consumers are subject to higher training obligations.

CCPA Conflicts with GDPR

Fourth, businesses are now going to have to reconcile the requirements of the European Union's General Data Protection Regulation ("GDPR") with California's privacy laws. In particular, California's Department of Justice has advised businesses to be wary of the following:

- Data inventory and mapping of data flows to demonstrate compliance with the GDPR may have to be re-worked to reflect the different requirements of California.
- Processes and/or systems set up to respond to individual requests for access to or erasure of personal information will need to be reviewed in order to apply different definitions of what constitutes personal information and different rules on verification of consumer requests.

- Contracts with service providers or data processors adopted to comply with the GDPR may need to be rewritten to reflect the requirements under California law.

Regardless of whether your SaaS or tech company is going to meet the threshold to be subject to the new California law when it goes into effect, it would be prudent to start incorporating these new requirements into your company's privacy practices and procedures, since they will at the very least become the new best practices for businesses serving California consumers effective January 1, 2020. It goes without saying that companies who will be subject to the law when it goes into effective need to take steps to become compliant immediately, as the law is set to go into effect in less than 75 days.

If you have questions regarding the CCPA and your company's compliance obligations, schedule a consultation with today at this link.

Facebook Agrees to Record $5 Billion Settlement with FTC on Privacy Practices

Multiple media outlets are reporting today that the Federal Trade Commission has agreed to settle its case against Facebook on its privacy practices for $5 Billion.

The Wall Street Journal reports that the vote by FTC commissioners was 3-2 in favor of accepting the agreement and split along party lines with the Republican majority favoring the settlement. According to **The Wall Street Journal**, the

matter next goes the the Justice Department's civil division for final review.

According to the **Mercury News**, assuming reports are correct, this will be the largest fine imposed to date by the U.S. government on a tech company. **The Washington Post** reports that the fine is more than 200 times higher than any previous fine.

Interestingly enough, **The Wall Street Journal** is reporting that the fine obtained by the FTC exceeds what the European Union could have obtained under its privacy laws.

The Washington Post predicts that the settlement will impose serious consequences on Facebook that go far beyond just a $5 billion fine. However, **The Washington Post** acknowledges that the dissenting commissioners opposed the settlement because they wanted some assessment of personal liability against CEO Mark Zuckenberg; commissioners reportedly decided to accept a settlement without any such assessment in order to ensure that the matter did not end up in litigation.

While controversial, the FTC's enforcement action in this matter still sets a significant precedent for the software industry with respect to the consequences of not protecting data uploaded to or generated by software. Software companies are on notice: the FTC is closely following your privacy practices and may assess fines in the billions of dollars against you if you fail to take sufficient steps to protect user data.