Should Pharma Care About California's New Data Privacy Law?

INTOUCH SOLUTIONS®

Executive Summary

Concerns about data privacy abound as we head into the final quarter of 2018. Large-scale data breaches at hospitals, banks, retailers, and other organizations — and on social media platforms like Facebook — have most Americans, including lawmakers, thinking about how best to protect their personal information.

In response, several states have been creating or fine-tuning their privacy laws, among them, California, which passed the California Consumer Privacy Act (CCPA) in June 2018. Although it is less all-encompassing than the European Union's recently enacted General Data Protection Regulation (GDPR), California's law is considered to be the most comprehensive law of its kind so far in the United States.

In this POV, we discuss the CCPA, what it entails, how pharma marketers might be affected, and what they can do to prepare for the law's 2020 implementation.

Overview

On June 28, 2018, California's governor signed into law the California Consumer Privacy Act (CCPA), which gives California residents greater control over the data-collection and use practices of companies collecting their personal information. This law may affect any company doing business in the state of California, regardless of whether the company is physically located in the state.

The CCPA goes into effect in January 2020 and will make it easier for consumers to sue companies after a data breach. And it gives California's attorney general more authority to hold accountable companies that don't comply. If violations aren't addressed within 30 days, "violators might face **penalties of not more than $2,500 for each violation, or $7,500 for each intentional violation.**"

California was the first state to pass a data-breach notification law; now all 50 states have one. It's been said that California leads the way for the rest of the United States in many regards — e.g., environmental protections, social and political movements, tech innovation — and it likely will lead with data privacy protections as more states follow suit and either shore up or create their own data privacy laws.

What Rights Does the CCPA Grant to California Residents?

Under the CCPA, California residents have the right to:

- Know what personal information is being collected about them
- Access their personal information
- Know whether their personal information is disclosed, and if so, to whom
- Know whether their personal information is sold, and if so, the right to opt out of the sale of their personal information
- Equal service and price regardless of whether they exercise their privacy rights

What Is Considered "Personal Information" Under CCPA?

With respect to the CCPA, personal information includes information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." This is an expansive definition of personal information which may include the following examples **(even when no names are attached)**, such as:

- Names
- Addresses
- Social security numbers
- Email and physical mailing addresses
- Geolocation
- IP addresses of all devices a consumer uses (i.e., smart phones, tablets, computers)
- Shopping or browsing history
- Psychological profiles
- Behaviors and attitudes
- Consumption behaviors and consumer preferences

Information exempt from the CCPA includes "protected health information that is collected by a covered entity or business associate governed by the privacy, security and breach notification rules issued by" the U.S. Department of Health and Human Services and governed by HIPAA. According to the International Association of Privacy Professionals, "The lawmakers extended the HIPAA/CMIA [Confidentiality of Medical Information Act] exemption to providers of health care governed under CMIA or covered entities governed by the specified federal privacy, security, and breach notification rules established pursuant to HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information." Ultimately, this means that exemptions in the CCPA are intended to prevent double regulation where an entity is already complying with a more rigorous privacy regime.

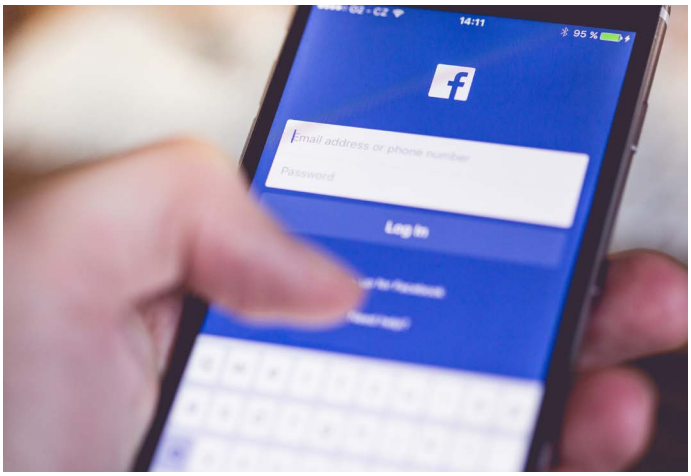
What Kinds of Companies Are Affected?

As stated previously, CCPA affects any company doing business in the state of California, regardless of whether the company is physically located in the state.

Tech companies like Facebook, Google, IBM and Microsoft are diving right into the discussion with lawmakers, lobbying the Trump administration in order to have a voice in any federal laws that may eventually be passed. Some are concerned that without a unified federal law, individual state laws will result in a regulatory nightmare that could hobble their ability to do business across state lines.

As it currently stands, the CCPA affects companies that meet at least one of the following criteria:

- Over $25MM in gross annual revenue
- You buy, hold, sell or share personal information of 50K consumers, and/or households or devices
- You derive at least 50% of your revenue from selling consumers' personal information



Does the Consumer Even Care?

A few years ago, we noted that a 2014 Pew Research study found that 55% of U.S. adults were willing to share some personal information in order to gain access to online services. We also noted that, at the time, experts predicted that by 2025, "the public will have lost the concept of privacy as we know it today." Fast forward to 2018, and consumers are a little spooked, with two-thirds saying that current laws aren't providing adequate privacy protection.

It's only been a few months since the European Union's GDPR went into effect in, but according to one recent article, "the U.K.'s data privacy watchdog says that the number of complaints it has received under GDPR has nearly doubled, and [as more people become aware of their rights] the trend is expected to continue." If EU consumer response to the GDPR is any indication, U.S. attitudes about privacy may shift and demands for greater protections may gain momentum.

In the United States, assistant secretary of the U.S. Department of Commerce David J. Redl noted in his remarks at the 2018 Internet Governance Forum that a 2017 National Telecommunications and Information Administration study showed that, "**nearly three quarters of Internet-using households** had significant concerns about privacy and security risks, such as identity theft or loss of control over personal information. What's more, over a third of online households said that privacy or security concerns had led them **not to engage** in an online activity, such as buying goods or making a financial transaction, at some point in the last year."

Is California the Only State Enacting Privacy Laws?

Several states around the country have also recently put into place or amended their own privacy laws, including Alabama, Colorado, Oregon, Louisiana, Vermont, and Virginia. Of note, Alabama's new breach-notification law includes a relatively broad definition of personally identifiable information, including health information, health insurance identifiers, and online log-in credentials.

More to Come in California: What About Bill AB-2546, the "Email Marketing Bill"?

Another bill being proposed in California would expand the state's existing anti-spam law, which applies to "any person or entity initiating or advertising in a commercial email advertisement either sent from California or to a California email address." The bill expands the definition of "commercial email advertisements."

The **new definition of commercial email advertisement**, with the changes underlined is as follows:

> "an electronic mail message initiated for the purpose of advertising or promoting the lease, sale, rental, gift offer, promotion, or other disposition of any property, goods, services, credit, stocks, bonds, sweepstakes, insurance, employment opportunities, or any other solicitation, excluding charitable or political solicitations."

The amendment would also expand the class of persons who can bring a lawsuit under California's anti-spam law to include not only the recipients of emails, but also, "Because federal law (the CAN-SPAM Act) covers or preempts many of the provisions in California's anti-spam law, the practical impact of the California anti-spam legislation (including this amendment) is limited to regulation of false or misleading spam emails, such as falsified "from" addresses; misrepresented unsubscribe links; etc.," says attorney and privacy expert Steve Hengeli, "Nonetheless, this California amendment should be monitored because it creates additional avenues for lawsuits — whether or not ultimately meritorious — for unsolicited marketing emails." It is unclear whether the definition of commercial email advertisement will remain as broad in the final text or whether this law will pass at all.

Implications for Pharma

The CCPA is more targeted than the EU's GDPR in that it focuses on consumer rights surrounding data at the point of collection. Unlike Amazon, with its acquisition of PillPack and the unprecedented access to personal health information it brings, **most pharmaceutical companies may find that the CCPA affects them less than other businesses**.

Of note for pharma marketers, California lawmakers have already amended the CCPA, particularly with regard to two areas:

01. Clarification of the definition of personal information, to make it less broad
02. **An exemption for clinical trials**

According to the IAPP, "The bill also addresses clinical trials, exempting certain information. The new clinical trial exemption apples [sic] to data from trials that (i) are subject to the so-called "Common Rule" (Federal Policy for the Protection of Human Subjects), and (ii) follow certain leading clinical practice

guidelines. This provision is a new substantive exemption since the original law did not address clinical trials."

In other words, if the amendment is approved, the CCPA will not apply to data already regulated by federal policy, as long as the clinical trial is conducted under clinical practice guidelines.

Recommendations

The CCPA doesn't go into effect until January 1, 2020, and more changes to it may be made when the California legislature begins its new session in January 2019, but why wait to make sure you're compliant? Initial steps, even if you don't expect to be heavily impacted at first, include:

- Conducting a data audit to determine how your company collects, uses, discloses and/or sells personal data
- Implementing the technology changes necessary to comply with the CCPA
- Developing a process — whether automated or human-controlled — to accommodate verifiable requests for access to and deletion of personal information
- Understanding how your digital marketing teams collect, store and share data
- Updating privacy policies and notices
- Amending third-party/vendor agreements if necessary to ensure compliance
- Creating an internal training plan, if appropriate

Conclusion

The CCPA gives consumers a whole new level of control over their personal information. As concerns over data security and privacy grow, it's likely that other states will follow California's example and create or expand their own privacy protections. While the pharma industry may be less affected by the CCPA than other types of businesses, preparing for compliance is still recommended. Reach out to your account team today to make sure your brand is covered.

Author: Chris Nelson, Vice President, Marketing Automation & Data Management

Want to learn more about CCPA?
Contact Chris Nelson at 913.956.4322
chris.nelson@intouchsol.com
agencyofmore.com