WHITE PAPER

BE READY FOR THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

CYBERSCOUT®

2

THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 GIVES CONSUMERS MORE CONTROL OVER THEIR PERSONAL INFORMATION—AND IT IMPACTS HOW BUSINESSES WILL LEVERAGE THIS DATA.

INTRODUCTION

Many businesses today collect some form of personal data from consumers. That process has been facilitated by ongoing advances in technology, but privacy concerns are following closely behind. As those treasure chests of information have grown, they have brought with them increased risks of a data breach, through both unintentional exposures and deliberate acts. The growing scourge of data breaches has prompted consumers to demand greater transparency from the companies that gather, store, process and share their information.

Striking a balance between protecting consumers' privacy rights and enabling businesses to leverage this data as part of their normal operations is becoming a major challenge for governments across the globe. The EU recently implemented the General Data Protection Regulation (GDPR), a law designed to provide a uniform set of data privacy standards and protections across Europe. Similar efforts are underway in the United States such as the California Consumer Privacy Act of 2018. With the passage of this new law, the California legislature has given the state's consumers more control over their personal information with an aim to further their right to privacy.

In this white paper, you will learn how the new Privacy Act:

- Defines personal information
- Strengthens consumer rights
- Empowers data deletion
- Impacts your organization
- Allows for penalties.

PERSONAL INFORMATION REDEFINED

Under the new law, personal information is any 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.

EXPANDING PROTECTION OF PERSONAL INFORMATION

Set to take effect in January 2020, California's new rule provides increased protections around personal information. To understand where and how the law may impact them, businesses should first be aware of the types of personal information covered by the Act.

In general, any personal information that identifies or could be linked to a consumer or a household—names, postal addresses, even IP addresses and geolocation data—is included in California's new regulation. Some of these datasets have long been considered sensitive, such as Social Security numbers and driver's license numbers. Other pieces of information are also on the protected list: Purchase histories for products and services, for example, are covered. Browsing and search history, along with consumers' preferences, predispositions, and attitudes, are also included in the Act.

7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256
PHONE (480) 355 8500 · FAX (480) 355 8501 · WWW.CYBERSCOUT.COM

3

THE ACT GRANTS CONSUMERS THE RIGHT TO ASK ORGANIZATIONS FOR SPECIFIC PIECES OF INFORMATION. ORGANIZATIONS MUST BE ABLE TO RESPOND WITHIN 45 DAYS, AND THEY CANNOT CHARGE CONSUMERS FOR THE INFORMATION OR REQUIRE THEM TO CREATE ACCOUNTS TO REQUEST OR RECEIVE THE DATA.

For employers, it is important to note that professional and employment information is also shielded by California's upcoming legislation. This includes characteristics of protected classifications under either California or federal law and education information that is not publicly available but is personally identifiable.

STRENGTHENING CONSUMER RIGHTS

Once the Act goes into effect, consumers will have the right to request specific pieces of information from any business that collects their personal information. Companies must be ready to disclose the following:

1. The categories of personal information it has collected about that consumer.
2. The categories of sources from which the personal information is collected.
3. The business or commercial purpose for collecting or selling personal information.
4. The categories of third parties with whom the business shares personal information.
5. The specific pieces of personal information it has collected about that consumer.

If a company sells or shares consumers' data, even if it is for business purposes, they must be able to provide everything above and in addition make available upon request the categories of personal information that were sold or disclosed and the type of companies that purchased that data.

An organization will need to provide the information within 45 days of receiving a request. If additional time is reasonably necessary to satisfy the request, the business can get a 45-day extension, but the law includes parameters about notifying the consumer of the delay. The company cannot charge the consumer for the information and they also cannot require them to create an account with the business as part of requesting or receiving the data. Although a business is obligated to respond in a timely manner to these consumer requests, they will not be required to provide it to the same consumer more than twice in a 12-month period.

California's new Act follows many of the GDPR's rules about responding to consumer requests, with a particular emphasis on transparency and portability. Companies may deliver requested information by mail or electronically, but digital responses need to be in a machine-readable format that allows the consumer to transmit it to another entity without hindrance.

7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256
PHONE (480) 355 8500 · FAX (480) 355 8501 · WWW.CYBERSCOUT.COM

4

BUSINESSES THAT ARE ACTIVE IN CALIFORNIA MUST GIVE CONSUMERS AN OPPORTUNITY TO OPT OUT OF THE SALE OF THEIR PERSONAL INFORMATION, AS WELL AS ITS DELETION, AND HONOR THEIR REQUEST.

DATA DELETION AND CONSUMERS' RIGHT TO OPT OUT

Consumers will now have the right to opt out of the sale of their personal information. Any business that sells this data to third parties must provide notice to consumers that their information may be sold, and if the company receives direction from a consumer not to sell their data, that request must be honored. Additional rules exist to protect the personal information of consumers who are minors. Any business that does not receive consent to sell the minor consumer's personal information is prohibited to do so unless there is an express authorization to sell.

Businesses that are active in California will also need to inform consumers that they can request the deletion of their data. The company then needs to honor those requests, deleting the consumer's personal information from its records and directing any service providers to also remove the individual's data.

Exceptions are available under the Act that allow a business to refuse to comply with a consumer's request to delete their personal information. If maintaining the data is necessary to complete a transaction or to provide the good and/or service requested by the consumer, for example, the business may not be required to wipe the information from its records. Similarly, a company likely will not be compelled to delete consumer data if is needed to perform or satisfy a contract between the business and the consumer, or if the information is reasonably anticipated within the context of an ongoing business relationship between the individual and the firm.

Additional operational concerns are also covered under the new law. Consumer data can be retained even if the person has requested its removal if that information is necessary to detect or protect against security incidents and illegal activity, or if it will be used during the prosecution phase for those types of activities. Debugging efforts may also require that consumer data be kept intact despite a request for removal.

Maintaining compliance with other legal obligations and rights—the exercise of free speech and compliance with the California Electronic Communications Privacy Act among them—are additional scenarios where businesses may be justified in refusing to delete consumer information.

IS YOUR BUSINESS AFFECTED BY THE ACT?

A broad range of for-profit companies doing business in the state of California—whether they are small sole proprietorships or mega-corporations—will fall under the jurisdiction of the new law. In general, annual gross revenues in excess of $25,000,000 create an obligation to comply with the Act, as does the handling of data for 50,000 or more consumers, households, or devices. That means

7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256
PHONE (480) 355 8500 · FAX (480) 355 8501 · WWW.CYBERSCOUT.COM

5

COMPANIES MUST BE READY TO COMPLY WITH CALIFORNIA'S UPDATED LEGISLATION BEFORE IT GOES INTO EFFECT IN 2020.

information gathered from or about individuals, as well as data gleaned from smartphones, Internet-of-Things devices (e.g., web-enabled household appliances, televisions), and even fitness trackers and similar wearables. Data does not just need to be harvested from these sources and stored. Any information that is shared also contributes to the company's total count when considering whether the Act applies to them. Businesses that derive 50 percent or more of annual revenues from selling consumers' personal information will also be covered by the Act.

There are numerous examples of companies that gather personal information but where data disclosures don't count as a sale. If a consumer uses the business to intentionally disclose personal information or to interact with a third party, for example, the new regulations may not cover the data shared as part of that relationship. Personal information transferred as an asset associated with a transaction—a merger, acquisition, bankruptcy, or similar situation—is also likely not part of the Act. However, if the party receiving those assets uses or shares the data in a way that's inconsistent with the promises made when the consumer provided the information, they need to notify customers so they can opt out if they choose to do so.

YOUR ORGANIZATION'S OBLIGATIONS

Companies must be ready to comply with California's updated legislation before the expected 2020 effective date. That includes informing consumers at or before the point of collection which categories of personal data will be gathered from them and how it will be used. The company can't expand those categories or uses without providing a notice to the consumer. To maintain adequate transparency about its privacy policies and obligations, businesses are expected to outline a description of consumers' rights and the designated methods for submitting requests. A list of the categories of personal data collected about consumers in the preceding 12 months must also be provided, with information broken down by categories of data sold and categories disclosed for business purposes. These lists must be updated at least once every 12 months.

Each covered business's online home page will need to include a clear and conspicuous link—titled "Do Not Sell My Personal Information"—where consumers can opt out of the sale of their personal data. A description of consumers' right should also be available on the website, with additional links to or details about its online privacy policy, if one exists.

Employees involved in handling consumer inquiries about the business's privacy practices or complying with the new legislation should be trained on the impending rules, as they will need to know how to respond to requests in the time allotted and how to direct consumers to exercise their rights under the law. This training can also be used to ensure that internal practices prevent the sale of personal data if

7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256
PHONE (480) 355 8500 · FAX (480) 355 8501 · WWW.CYBERSCOUT.COM

6

BUSINESSES THAT FAIL TO IMPLEMENT SECURITY PROCEDURES AND PRACTICES TO PROTECT CONSUMERS' PERSONAL INFORMATION MAY INCUR DAMAGES IF THEY EXPERIENCE A BREACH.

a consumer has opted out, and that information collected from the consumer as part of their opt-out submission is not used for anything except complying with the opt-out request.

KNOW THE PENALTIES

Firms should be aware that the Act prohibits discrimination against any consumer who exercises their rights to data privacy and protection. Businesses are not allowed to deny that consumer goods or services, or to provide them a different level or quality of goods or services. It will also be a violation of the new law to charge a consumer a different price as a punitive measure. Even suggesting a consumer could receive either a different price or a different quality of goods and services is verboten. A business may offer financial incentives to consumers as compensation for the collection or sale of their personal information, but it is important to first ensure you are familiar with the strict guidelines around those activities.

A business that fails to implement and maintain security procedures and practices that are appropriate for protecting consumers' personal information—and that includes providing proper encryption and/or redacting data as necessary—could incur damages if there is a data breach, whether through negligence or as a result of a targeted hack or similar event. The Act enables individuals to recover damages up to $750 per incident or actual damages, whichever is greater, and a court may also award additional relief if it deems it proper. This private right of action applies only to data breaches.

The attorney general can seek $2,500 per violation in an action against the business and $7,500 per violation, if the violation was intentional.

CONCLUSION

The passage of the California Consumer Privacy Act of 2018 heralds a new era in data privacy regulations in the U.S. Consumers in California have pushed for a stronger law, and individuals' desire to protect their personal information in the face of a litany of devastating data breaches and ever-increasing technological challenges should come as no surprise.

The Act also signals a change for firms that do business in the state of California. By ensuring they have the tools and protocols available to exercise more rigorous oversight of the consumer data they harvest and hold, companies can better protect their customers while also reducing their own vulnerabilities in data management and data security. ■

7580 N DOBSON RD, SUITE 201 · SCOTTSDALE, AZ 85256
PHONE (480) 355 8500 · FAX (480) 355 8501 · WWW.CYBERSCOUT.COM