EPSTEIN BECKER GREEN | Employment, Labor & Workforce Management

ACT NOW ADVISORY

California's New Consumer Privacy Act: What Employers Need to Know

July 30, 2018

By Brian G. Cesaratto and Deanna L. Ballesteros

California continues to lead the way on privacy and cybersecurity legislation with the enactment on June 28, 2018, of the California Consumer Privacy Act ("Privacy Act" or "Act").[1] The Privacy Act joins other California laws safeguarding California residents' privacy rights under the California Constitution.[2] Also, the Act adds to the steadily expanding number of state laws, including the laws of New York, Illinois, and Massachusetts, providing for the privacy and cybersecurity of personal information.[3] The Act becomes effective on January 1, 2020, to afford California businesses sufficient time to achieve compliance.

It is not surprising that the Privacy Act's enactment comes one month after the effective date of the European Union's General Data Protection Regulation ("GDPR"). Nor is it surprising that the Act follows the recent congressional investigation into Cambridge Analytica's apparent misuse of personal information stored on Facebook.[4] The Act was enacted in response to private efforts by an organization called Californians for Consumer Privacy to place on the November 2018 ballot a statewide initiative titled the "Consumer Right to Privacy Act of 2018."[5] This effort reportedly resulted in more than 600,000 supporting signatures.

---

[1] Cal. Civ. Code § 1798.198(a).

[2] *See id.* at § 1798.82 (providing for data breach notification by California businesses where unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person); Cal. Civ. Code § 1798.81.5 (requiring that businesses implement and maintain reasonable security procedures and practices to protect personal information owned or licensed by them from unauthorized access, destruction, use, modification, or disclosure); Cal. Bus. Code §§ 22575-22579 (mandating that businesses that operate commercial websites maintain an accessible privacy policy disclosing the categories of personal information collected).

[3] *See* NYS Department of Financial Services Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500; Illinois Biometric Information Privacy Act, 740 ILCS 14; Massachusetts Data Protection Law, 201 CMR 17.

[4] *See* the Legislative Counsel's Digest: "In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened."

[5] *See* Cal. Civ. Code § 1798.198(b).

The Privacy Act applies to any for-profit business that (i) collects personal information on California residents, (ii) does business in the state of California, and (iii) satisfies one or more of the following thresholds: (a) has annual gross revenues in excess of $25,000,000; (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (c) derives 50 percent or more of its annual revenues from selling consumers' personal information.[6] Businesses that hit the thresholds will be covered even if they are located outside the state of California.

The Privacy Act establishes the rights of Californians:

- to know what personal information is being collected about them;
- to know whether their personal information is sold or disclosed and to whom;
- to say "no" to the sale of their personal information;
- to access their personal information collected and receive a copy;
- to be free from discrimination for exercising their privacy rights;
- to the deletion of their personal information, subject to certain exceptions; and
- to bring a private right of action if certain personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable cybersecurity procedures and practices.[7]

Does the Privacy Act Cover the Personal Information of Employees?

While the Privacy Act is ostensibly a consumer protection statute, its requirements, on their face, apply in the employment context. The Act defines a "consumer" as "a natural person who is a California resident . . . however identified, including by a unique identifier." Although the Act does not mention employees specifically, no provision excludes them from coverage. The Act, therefore, apparently protects the personal data of any employee who is domiciled in the state of California or who is in the state other than for transitory or temporary purposes.[8]

There are legislative references indicating that the Act may protect an individual's privacy rights in the collection of personal information in the workplace. The Legislative

[6] *See id*. at § 1798.140(c).
[7] The private right of action provision applies only to the more limited definition of "personal information" contained in section 1798.81.5 of the California Civil Code, which applies to information containing the individual's name coupled with certain identifiers, such as a Social Security number. The remaining provisions of the Act are enforced by the California Attorney General.
[8] *See* Section 17014 of Title 18 of the California Code of Regulations.

Counsel's Digest to the Act highlights the sharing of personal information with a potential employer as covered under the Act: "It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information." In addition, the Act includes "professional or employment-related information" as protected personal information. The California Chamber of Commerce has recognized the apparent inclusion of personnel-related information and recently issued an alert stating that "the bill provides 'consumers' with the right to request that a business delete their personal information, but the definition of consumer is so broad that it could apply to employees of a business."[9]

The Act also has a number of similarities to the GDPR (e.g., the right to notice of collection of personal data and the right to be forgotten), which applies in the employment context. Absent clarification by the California Legislature to exclude employers from the Act's coverage in advance of the effective date, or subsequently by the courts, the Act will apparently extend additional privacy rights to California employees in connection with the collection by employers of their personal information. This conclusion is reinforced by the Act's reference to the various statutes already on the books effectuating Californians' constitutional right to privacy, including existing privacy and cybersecurity protections in the workplace, and the mandate that "the provisions of the law that afford the greatest protection for the right of privacy of consumers shall control."[10]

What Personal Information Is Covered?

The Privacy Act defines "personal information" as names and other individual personal identifiers, but also more broadly includes "information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household."[11] The following types of information that an employer may collect or process on job applicants or employees will fall within the definition of "personal information":

- name, address, and telephone number;
- Social Security, passport, or drivers' license number;
- email address;
- unique identifiers, such as Internet Protocol address, user identification number, or persistent cookies that may identify an individual;
- educational, professional, and employment-related information;

[9] *See* CalChamber Alert titled "CalChamber Seeking Cleanup Suggestions on Newly Adopted Privacy Bill."

[10] The Act provides, "This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers personal information." *See* Cal. Civ. Code § 1798.175.

[11] *See id.* at § 1798.140(o).

- financial or bank account information;

- medical or health insurance information of employees that is *not* protected health information ("PHI") regulated by California's Confidentiality of Medical Information Act or by the Health Insurance Portability and Accountability Act's ("HIPAA's") privacy, security, and notification rules;

- characteristics of protected classifications under California or federal law (e.g., requests for accommodation that disclose a disability);

- biometric information; and

- any "inferential information" that may be drawn from any of the information collected to create a profile reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Information that is "publicly available information" (i.e., information already made available from federal, state, or local records) does not constitute personal information.[12] The Privacy Act also does not apply to the collection or sale of personal information if "every aspect of the commercial conduct takes place wholly outside of California."[13]

Although PHI is exempted, health care companies that otherwise collect personal information are subject to the Act's requirements.

What Notices and Responses to Individual Requests Are Required?

The individual's privacy rights are implemented under the Act through required notices and disclosures. A business that collects personal information must, at or before the point of collection, inform the individual in writing of the categories of personal information to be collected and the business purposes for which the categories of personal information will be used.[14] The individual must also have the right to receive, upon request, a written disclosure of the categories and specific pieces of personal information that the business has actually collected, the categories of sources from which the personal information is collected, the business purpose for collecting (or selling) the personal information, and the categories of third parties with whom the business shares personal information.[15] If the personal information was shared with third parties, the individual has the right to know the categories of third parties with whom the business shares personal information and the business purpose for disclosing the information.[16] The business must, at a minimum, provide a toll-free

[12] *See id.* at § 1798.140(o)(2).
[13] *See id.* at § 1798.145(a)(6)).
[14] *See id.* at § 1798.100(b).
[15] *See id.* at §§ 1798.100(a), 1798.110(a)(b).
[16] *See id.* at §§ 1798.110(c), 1798.115.

number for an employee to make the request, and, if it maintains a website, a website address.[17]

Is There an Obligation to Publish an Online Written Privacy Policy?

There is an obligation to publish in the business's online privacy policy, or otherwise on its website, notice of the rights to request disclosure of the categories and personal information actually collected, the business purpose for collection and disclosure, the categories of third parties with whom the business shares personal information, the business purpose for sharing the information, and the right to be free from discrimination because the individual exercised any rights under the Act.[18]

Does the Privacy Act Provide for a Right of Deletion of Personal Information?

A consumer must have the right to request that a business delete any personal information about the consumer that the business has collected from the consumer.[19] A business may refuse the request, however, in certain circumstances, including to comply with regulatory or other legal obligations requiring the information's retention. The business may also refuse the request if it maintains the information for internal purposes in a lawful manner that is compatible with the context in which the information was originally provided. In the employment context, the exceptions to an employee's right to request deletion may frequently permit the employer to continue to retain the records despite the request.

What California Employers Should Do Now

California employers should:

- plan for compliance while watching for any legislative or regulatory clarification in the coming months that may exclude the collection of employee personal information;

- identify the categories of employment-related personal information that fall within the Act and how the information is collected and processed;

- pinpoint the computers and information systems (e.g., laptops, servers, databases, cloud-based repositories, and communications systems) that process personal information and employment roles that have access to the personal information;

- identify any third-party vendors or business partners that maintain personal information of employees or applicants;

[17] *See id.* at § 1798.130(a)(1).
[18] *See id.* at § 1798.130(a)(5)(A).
[19] *See id.* at § 1798.105.

- determine the associated business reasons for the collection and processing of the "in scope" information falling within the Act's definition of "personal information";

- assess the value of the personal information collected and determine whether certain information may be excluded from collection on a going-forward basis because of the lack of a compelling business purpose;

- identify the policies, procedures, and technology that must be implemented to achieve compliance as to the "in scope" personal information and systems (e.g., updated privacy policies, revised employee handbooks, notices regarding inquiries about current and prior employees' employment history, benefits forms, just-in-time website notices, or other disclosures that will be needed at the time the information is provided), and consider privacy by design and policies, procedures, and technologies to evaluate and implement individual requests for the deletion of personal information across systems, when required;

- set up a hotline and process to quickly address and resolve complaints;

- identify any cybersecurity protections that may need to be applied to protect personal information within the data breach and private right of action provisions of the Act, including the 20 controls in the Center for Internet Security's Critical Security Controls;[20]

- speak to insurance brokers and insurance companies regarding purchasing cybersecurity insurance given the Act's private right of action; and

- develop a plan to curtail the collection of personal information or to ensure compliance as of the January 1, 2020, effective date.

* * * *

For more information about this Advisory, please contact:

Brian G. Cesaratto
New York
212-351-4921
bcesaratto@ebglaw.com

Deanna L. Ballesteros
Los Angeles
310-557-9547
dballesteros@ebglaw.com

[20] The California Attorney General has stated that the 20 controls in the Center for Internet Security's Critical Security Controls "define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in locations throughout the United States and supporting domestic and multinational clients, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.