Privacy Law Watch™

July 09, 2018

Bloomberg BNA

Consumer Data

INSIGHT: Be Wary of Liability for Statutory Damages under California Consumer Privacy Act

by Lothar Determann, Baker & McKenzie LLP

As of January 1, 2020, companies around the world will have to comply with additional regulations related to processing of personal data of California residents. Pursuant to the California Consumer Privacy Act of 2018, companies have to observe restrictions on data monetization business models, accommodate rights to access, deletion, and porting of personal data, as well as issue or update privacy notices to provide detailed disclosures about data handling practices. For a general overview of the statute and its unusual history, see Lothar Determann, The California Consumer Privacy Act of 2018 - Broad Data and Business Regulation, Applicable Worldwide, IAPP Privacy Tracker (Jul. 2, 2018).

Additionally, companies that become victims of cyber attacks or data theft will become exposed to statutory damages claims of up to $750 per consumer and incident under a new Section 1798.150, which the California Consumer Privacy Act of 2018 adds to the California Civil Code.

1. Who is entitled to claims?

Any California resident whose nonencrypted or nonredacted personal information is subject to an unauthorized access may institute a civil action under the California Consumer Privacy Act, which defines “consumers” as any “natural person who is a California resident” (*Cal. Civ. Code §1798.140(g)*) and includes employees, contractors, patients, students, and any other individuals.

2. What data is protected?

Cal. Civ. Code §1798.150(a) refers to the definition of “personal information” in the existing Cal. Civ. Code §1798.81.5(d)(1)(A), which covers “[a]n individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted”:

> social security number;
>
> driver's license number or California identification card number;
>
> account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
>
> medical information;
>
> health insurance information.

This is much narrower than the broad new definition that applies to the remainder of the California Consumer Privacy Act,

contained in *Cal. Civ. Code §1798.140(o)(1)*, which defines the term "personal information" broadly as "any information that … relates to … a particular consumer or household," and differs from the definition of "personal data" in the existing California data security breach notification laws, which list similar information plus "information collected through an automated license plate recognition system," see, Cal. Civ. Code §1798.82(h); Cal. Civ. Code §1798.29(g).

"Encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security according to Cal. Civ. Code §1798.82(i)(4) a nd Cal. Civ. Code §1798.29(h)(4). Courts may also refer to this definition to determine the meaning of "unencrypted and unredacted" in the new law. But the new law does not extend to two situations covered under the existing breach notification laws, where individuals are protected with respect to encrypted information if the security of the encryption has been compromised (Cal. Civ. Code § 1798.82(a)), and where a user name or email address, if used in combination with a password or security question and answer, would permit access to an online account (Cal. Civ. Code § 1798.82(h)(2)). Moreover, the new law does not refer to the existing definition of a data security breach, but creates a new concept by referring to "unauthorized access and exfiltration, theft, or disclosure" (*Cal. Civ. Code §1798.150(a)(1)*).

3. Who can be subject to claims?

Companies around the world can be covered by the California Consumer Privacy Act if they receive personal information from California residents and if they—or their parent company or a subsidiary—exceed one of three thresholds: (a) annual gross revenues of $25 million; (b) personal information of 50,000 or more California residents, households, or devices annually; or (c) 50% or more annual revenue from selling California residents' personal information. Parent companies and subsidiaries using the same branding are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds.

(a) Whether the $25 million threshold needs to include only California revenue or global sales is not clear. While Cal. Civ. Code § 1714.43(a)(1) defines the scope of the California Transparency in Supply Chains Act expressly in reference to "annual worldwide gross receipts," the new *Cal. Civ. Code §1798.140(c)(1)(A)* merely refers to "annual gross revenues" without an expanding reference to "worldwide." Yet, a limiting reference to California is also missing, as for example contained in Cal. Rev. & Tax. Code § 17942(a)(2), which refers to "total income from all sources derived from or attributable to this state."

(b) Companies are also covered if they receive or sell personal information of at least 50,000 California residents annually. Companies may pass this threshold more quickly than anticipated because the scope of personal information for purposes of this threshold includes any data pertaining to an individual person or household. Most companies operate websites and thus inevitably capture IP addresses. The definitions apply whether the website targets businesses or individual customers in California, given that "consumer" is defined to mean any "resident." Even individual bloggers and relatively small businesses outside California may find it difficult to ensure that they do not receive personal information of more than 50,000 California resident visitors to their website annually, given that their websites are accessible to California internet users. Within California, most retailers, fitness studios, music venues and other businesses will certainly meet this threshold.

(c) Companies can also be subject to the law based on whether they sell California residents' personal information and derive more than 50% of their annual revenue from selling that information. "Selling" is defined broadly to mean disclosing or making available "for monetary or other valuable consideration" (*Cal. Civ. Code §1798.140(t)(1)*), subject to a number of exceptions set forth in subsection (t)(2), including consumer-directed disclosures to third parties that do not sell the personal information, limited sharing with service providers, and business transfers in bankruptcy, M&A, and similar transactions.

(d) A company without a physical presence or affiliate in California may be able to defend against the applicability of the statute, however, if it can ensure that its "commercial conduct takes place wholly outside of California" for purposes of *Cal. Civ. Code §1798.145(a)(6)*) and that it is not doing "business in the State of California" for purposes of *Cal. Civ. Code §1798.140(c)(1)*. Most U.S. companies will find it difficult to determine that they are not doing business in the State of California, because the term "doing business" is generally understood very broadly. According to Cal. Rev. & Tax. Code § 23101(a), an out-of-state company is "doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California." Furthermore, according to Cal. Corp. Code §§ 191(a), 15901.02(ai) and 17708.03(a), companies outside of California and qualified to do business in California may be subject to the law if they enter "into repeated and successive transactions" in California, which could occur remotely and online.

4. What elements do plaintiffs have to prove?

Plaintiffs would have to show:

1. personal information

2. of a California resident

3. that was nonencrypted or nonredacted

4. subject to an unauthorized (a) access and exfiltration, (b) theft, or (c) disclosure

5. that was caused by

6. a violation of a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

Significantly, plaintiffs would not have to show any actual harm or injury.

5. What remedies are available?

Plaintiffs may institute a civil action for any of the following:

- damages in an amount not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater,
- injunctive or declaratory relief, and
- any other relief the court deems proper.

In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth. Also, *Cal. Civ. Code §1798.194* instructs courts that the new law "shall be liberally construed to effectuate its purposes."

6. What procedural hurdles apply?

Plaintiffs must satisfy a number of requirements before they may bring an action:

(1) *Cal. Civ. Code §1798.150(b)(1)* provides: "Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement."

(2) *Cal. Civ. Code §1798.150(b)(2)* further requires notification to the Attorney General within 30 days of filing an action. Upon receiving that notice, *Cal. Civ. Code §1798.150(b)(3)* requires the Attorney General to take one of the following actions within 30 days:

- declare that Attorney General will prosecute the violation (provided, however, that if the Attorney General does not prosecute within six months, the private plaintiffs may proceed with their action);
- declare that the plaintiff shall not proceed with the action; or
- remain inactive and allow the plaintiff to proceed.

7. What is the impact for companies?

Companies around the world are already required to notify California residents of data security breaches under California's existing breach notification law, which California enacted in 2002 and updated several times since then. See Lothar Determann, New California Data Security and Breach Notification Requirements, Bloomberg BNA Privacy & Security Law Report, 15 PVLR 219, 2/1/16. California was the first jurisdiction in the world to enact such a law. All U.S. states and many other countries have followed suit. And, since May 25, 2018, the European Union now has a breach notification law with the implementation of the General Data Protection Regulation.

But the potential liability resulting from breaches was somewhat contained by the fact that the original 2002 version of the California breach notification law only prescribed notification obligations; there were no penalties or other remedies for the actual breach—only for failures to notify. Plaintiffs were able to refer to various general causes of action, including torts, consumer protection and unfair competition laws, but often found it difficult to show "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical," as required for standing under federal law according to Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016). Particularly in the context of class action lawsuits, plaintiffs' lawyers prefer to assert general harms potentially associated with security breaches as opposed to concrete, individual injuries, which could prevent class action certification. See Lothar Determann, California Privacy Law - Practical Guide and Commentary, 2-15:1 and 6-2:2 (3d Ed. 2018).

Since January 1, 2016, operators and users of automated license plate recognition (ALPR) systems were subjected to specific data security requirements and notification obligations in case of a data security breach under Cal. Civ. Code §§ 1798.90.5, 1 798.29 and 1798.82; individuals harmed by a violation of the California ALPR law were also entitled to bring a civil action against persons who knowingly caused the harm—including harm by data security breaches—and claim actual damages, liquidated damages in the amount of $2,500, punitive damages (upon proof of willful or reckless disregard of the law), reasonable attorney's fees and other litigation costs, and preliminary and equitable relief, see Lothar Determann, California Privacy Law - Practical Guide and Commentary, 3d Ed. 2018, Ch. 2-5:5, 2-15.1.54 and 2-19:6.9.

Now, based on the new cause of action in *Cal. Civ. Code §1798.150* for statutory damages, plaintiffs generally do not have to show concrete, individual harm associated with certain data security breaches captured by the new statute, at least not in California courts, where no particular standing requirements apply. Therefore, companies have to prepare themselves for significantly increased liability exposure in cases of data security breaches. For example, if a hospital falls victim to a cyberattack or plain old burglary and theft of an appointment calendar with 10,000 patient names for doctor visits (without any sensitive medical history), the hospital could be exposed to damages claims between $1 million and $7.5 million plus cost of litigation, even if not one patient suffers any concrete harm of any kind.

8. What should companies do?

First and foremost, companies should ramp up their data security programs to reduce the risk of becoming subject to data security breaches. This is required by many other domestic and international laws and is also necessary for trade secret protection and general corporate governance, see, Determann's Field Guide to Privacy Law, Checklist (3d Ed. 2017).

Second, companies should document their technical and organizational data security measures (a.k.a. TOMs) to increase their chances that they can defend against claims by showing that they "maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." This is required for EU GDPR compliance and also favored by a number of other California privacy laws. See Lothar Determann, California Privacy Law - Practical Guide and Commentary, Chapters 5 and 7 (3d Ed. 2018).

Third, companies should proactively disclose their vendor- and customer-facing TOMs and incorporate them into contracts with business partners to define what is reasonable, at least for contractual indemnification claims. This is already required to some extent under the EU Standard Contractual Clauses 2010 and generally helpful to define and allocate compliance obligations. See Lothar Determann, EU Standard Contractual Clauses for Transfers Of Personal Data to Processing Service Providers Reassessed, BNA Privacy and Security Law Report (2011), 10 PVLR 498.

Fourth, companies should revisit their broader data collection and retention strategies to decide whether they can delete more data and upgrade their data retention and deletion programs. Of course, data minimization and deletion is particularly challenging where companies need more data than ever before to remain competitive in the fields of various new technologies, such as artificial intelligence, autonomous cars, and big data systems.

Fifth, companies should review and improve their contractual protections vis-à-vis data processing service providers and other

vendors, as well as vis-à-vis customers, to pursue adequate risk allocations in the supply and distribution chain. Unlimited contractual liabilities or indemnification clauses for data security breaches are as questionable as absolute disclaimers or caps on liabilities. Moreover, indemnification promises for penalties or punitive damages may run afoul of public policy under Cal. Civil Code §1668 and similar laws as such arrangements could induce contracting parties to violate laws or rights of third parties. More granular risk allocations with respect to pricing, costs, and primary obligations for security are appropriate.

Sixth, companies should reconsider insurance policies, premiums, and deductibles in the context of their overall risk profile and risk management program.

Seventh, companies should consider regular incident preparedness exercises, dry-runs, training and policy upgrades, given the rapidly evolving landscape of data security breach notification requirements and liability risks. An unintended consequence of the new law could be that companies may shy away from proactive, voluntary breach notifications if they have to fear draconian litigation consequences without regard to consumer harm.

Lothar Determann is a partner at Baker & McKenzie LLP, Palo Alto. He is the author of Determann's Field Guide to Privacy Law (3d Ed. 2017) and California Privacy Law - Practical Guide and Commentary (3d Ed. 2018). He also teaches privacy and computer law at Freie Universität Berlin, at the University of California, Berkeley School of Law, and at UC Hastings College of the Law, San Francisco.

The author is grateful for edits and input from his Baker McKenzie colleagues Andrea Tovar and Brendan Gilmartin.

The views expressed in this article are those of the author and not necessarily those of Baker McKenzie or its clients, or of Bloomberg Law.