Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Next Steps For Cos. In Light Of New Calif. Privacy Laws

By **Mark Krotoski and Kevin Benedicto** (October 23, 2019, 3:49 PM EDT)


Mark Krotoski


Kevin Benedicto

On Oct. 11, California enacted A.B. 1130, which amends the state's Data Breach Notification Law.[1]

A.B. 1130 expands the definition of "personal information" under the existing Data Breach Notification Law by requiring businesses to notify residents when their "tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual" or biometric information are compromised in a data breach.[2]

The new law takes effect on Jan. 1.

The legislation is part of an ongoing trend in California and other states to expand the definition of "personal information." The expanding scope of the definition broadens the circumstances that may require data breach notification to affected individuals.

Under the current version of the notification law, residents must be notified about a data breach if there is "unauthorized acquisition" of "personal information" as defined. A.B. 1130 expands the scope of personal information to include the noted specific forms of government identification numbers.

A.B. 1130 also adds biometric data as personal information under California law for the first time and defines it as:

> Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

About 11 states already include passport numbers,[3] five states include military identification numbers,[4] and eight states include taxpayer identification numbers[5] as part of their definitions of personal information. Eight states and Puerto Rico also have a catch-all to cover other unique identification numbers issued by a government agency.[6] Similarly, about 20 states have amended their data breach notification statutes to include biometric information.[7]

Legislative Response to Prior Incident

California Attorney General Xavier Becerra proposed, and Assemblyman Mark Levine sponsored A.B. 1130 based largely on a 2018 data breach.[8] Under the current version of the California Data Breach Notification Law, the company that suffered the data breach was not required to notify consumers when only passport numbers were accessed, as passport numbers were not part of the law's definition of personal information.

According to the sponsors, A.B. 1130 was proposed in part as a response to this perceived gap in the Data Breach Notification Law. The new statute also includes new data elements.

The Landmark California Data Breach Notification Law

In 2002, California enacted the first data security breach notification law, which became effective in July 2003.[9] The law required companies to disclose breaches of personal information to California residents whose personal information was, or was reasonably believed to have been, acquired by an unauthorized person. The California statute defined personal information and included other requirements and obligations. The original statute provided a private right of action "to recover damages".[10]

Over time, the statute has been amended to impose additional requirements. For example, in 2011, the statute was amended to require notification to the California attorney general if the personal information of more than 500 California residents was affected by a data breach and new requirements specified the minimum content and form of any notification to residents.[11]

Since California passed the first Data Breach Notification Law, now 54 jurisdictions (50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands) have enacted their own data breach notification laws, many modeled on the California statute. However, each statute is different, and the definition of personal information, the reporting requirements to individuals or state agencies, and the penalties vary in each jurisdiction, which create inconsistencies and complexities for entities attempting to comply with this patchwork of notification requirements.

Trend of Broadening Personal Information Data Elements

While the data breach notification statutes have common elements with significant differences, other trends continue. One recent trend in California and other states has been to expand the definition of personal information over time.[12]

Core Data Elements

The original core definition of personal information in California included "an individual's first name or first initial and last name" with one or more of three unencrypted data elements:

1. Social Security number;

2. Driver's license number or California identification card number; or

3. 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.[13]

Expanded Data Elements

A.B. 1130 continues the trend in California of expanding the definition of personal information under data breach notification laws. For example, the definition of "personal information" was expanded in 2008 to include medical information and health insurance information,[14] and in 2016 to include "[i]nformation or data collected through the use or operation of an automated license plate recognition system."[15]

In January 2014, California was the first state to expand the definition of personal information to include: "User name or email address, in combination with a password or security question and answer that would permit access to an online account."[16] Florida followed in July 2014, and Wyoming in July 2015.[17] Other states and jurisdictions have joined this trend with different approaches.[18]

Under the patchwork of state data breach notification laws, the definitions of personal information vary widely. While these laws include the "core" data elements (noted above) as part of the definition of "personal information," other data elements are added, as summarized in the table, to highlight some of the disparate data elements covered by these laws.

Examples of Disparate Data Elements in Current Data Breach Statutes	
Data Element	**Jurisdiction**
Birth certificate	South Dakota and Wyoming[19]
Marriage certificate	Wyoming[20]
Challenge questions	South Dakota[21]
Date of birth	North Dakota, Texas, Washington[22]
Digital signature	North Carolina and North Dakota[23]
DNA profile	Delaware and Wisconsin[24]
"Information or data collected through the use or operation of an automated license plate recognition system"	California[25]
Password	Georgia, Maine, North Carolina, South Dakota[26]
Financial account password	Alaska[27]
Maiden name of the individual's mother	North Dakota and Texas[28]
Employer identification card "in combination with any required security code, access code, or password"	North Dakota[29]
State identification number	Alabama, Alaska, California, Connecticut, Georgia, Hawaii, Maine,
	Maryland, Oregon, Utah, Virginia, Washington, Wisconsin, Wyoming, among other states[30]
Student identification number	Colorado and Washington[31]
Tribal identification number	Rhode Island, South Dakota, Wyoming[32]
Voter's identification	Puerto Rico[33]
Security tokens used for data based authentication	Wyoming[34]
Telecommunication access device	Texas[35]
"[U]nique electronic identification number, address, or routing code"	Texas[36]
Work-related evaluations	Puerto Rico[37]

The different definitions create the circumstances in which the same incident may require notification in some but not all jurisdictions.

The patchwork of federal and state statutes adopting different and conflicting standards creates an unnecessarily complex, cumbersome and costly system. Congress and state governments can and should minimize the growing conflicts.[38] Eventually, a uniform federal standard is necessary to promote effective cybersecurity, simplify the process and ensure consistent standards.[39] Until then, companies will continue to operate under the patchwork of inconsistent standards in multiple jurisdictions.

Contrasting the CCPA

Looming on the horizon are more significant changes to the data protection statutory regime in California. On June 28, 2018, California passed the California Consumer Privacy Act,[40] which, like A.B. 1130, takes effect on Jan. 1.

The CCPA is a sweeping new law establishing new statutory privacy rights including the right to know what personal data is being collected; to know whether it is being sold or disclosed; to opt out of such disclosure; to access the data; to data portability; to be forgotten; to opt out of the sale of personal information to third parties; and to request that a business delete personal information that has been collected.

Under the CCPA, "personal information" is defined much more expansively. In contrast with the narrow definition of "personal information" under the California Data Breach Notification statute, the CCPA definition of "personal information" includes any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[41] Nonexhaustive examples include:

- Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number or passport number;
- Categories of personal information described in California's customer records destruction law;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property; products or services purchased, obtained or considered or other purchasing or consuming histories or tendencies;
- Biometric information;
- Geolocation data;
- Internet or other electronic network activity, such as browsing history, search history and information regarding a consumer's interaction with a website, application or advertisement;
- Audio, electronic, visual, thermal, olfactory or similar information;
- Professional or employment-related information;
- Education information that is subject to the Family Educational Rights and Privacy Act; and

- Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.[42]

In addition to the broader scope, the CCPA includes significant penalties, including statutory damages and fines. First, the California attorney general may bring an enforcement action against a business that "fails to cure any alleged violation within 30 days after being notified of alleged noncompliance" seeking an injunction and a "civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation".[43]

Enforcement actions have been delayed under the CCPA "until six months after the publication of" final regulations "or July 1, 2020, whichever is sooner."[44] Final regulations are under review and expected by the end of the year based on the regulations that issued on Oct. 10.[45]

Second, the CCPA includes a limited private right of action for consumers when their "nonencrypted and nonredacted personal information" is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures."[46]

Presently, the private right of action relies on a narrower definition of "personal information" under a California statute requiring a "business that owns, licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[47]

Under the narrower definition, the CCPA private right of action applies to personal information includes "(i) Social security number; (ii) Driver's license number or California identification card number; (iii) 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; (iv) Medical information; or (v) Health insurance information."[48] Note that California law does not define what constitutes "reasonable security procedures."

A data breach may result in separate claims under each statute once the prerequisites are established. However, the big difference now is the potential for large damages under the CCPA.

In many data breach cases under current law, establishing harm or actual damages has been challenging and has limited damages to harm that can be established. In contrast, under the CCPA, damages will be based on the greater of the actual damages or statutory damages "in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident," along with injunctive relief or "[a]ny other relief the court deems proper."[49]

The potential for large statutory damages under the CCPA, depending on the number of consumers impacted, has not been seen before in any data breach litigation. The increased risk of injunctive relief and damages and the private right of action under the CCPA has the potential to significantly reshape the landscape of data protection and data breach litigation for any company that does business in California.

What Should Companies Do?

Both the amendment under A.B. 1130 and the CCPA take effect on Jan. 1. Companies can take a number of steps to comply with both laws including:

- Assessing whether information that companies collect meets the broader definition of "personal information," including biometric information under the new law and also under the CCPA;

- Ensuring safeguards are in place to protect that information including by encrypting the data, if possible;

- Giving careful consideration, including consultations with counsel, to whether "reasonable security procedures" are in place to protect the personal information under the CCPA and separate reasonable security law. Counsel can advise on the legal issues and potential claims that may arise depending on the circumstances and personal information at issue and appropriate security options to consider;

- Checking and updating breach notification policies and procedures;

- Reviewing and updating incident response plans;

- Having compliance efforts underway to meet the new CCPA standards, which is a separate area of focus; and

- Checking with experienced counsel for legal guidance and any questions.

Mark Krotoski is a partner at Morgan Lewis & Bockius LLP. He previously served as the national coordinator of the computer hacking and intellectual property program in the Criminal Division of the U.S. Department of Justice and as a cybercrime prosecutor.

Kevin Benedicto is an associate at the firm.

[1] Cal. Civ. Code § 1798.29; 1798.80 et seq.

[2] Assembly Bill 1130 (enrolled Sept. 9, 2019; enacted Oct. 11, 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130; see also Press Release, Governor Newsom Issues Legislative Update 10.11.19 (Oct. 11, 2019) (confirming AB 1130 was signed into law), https://www.gov.ca.gov/2019/10/11/governor-newsom-issues-legislative-update-10-11-19/.

[3] See, e.g., Alabama (Ala. Code 1975 § 8-38-2(6)(a)(2)); Arizona (A.R.S. § 18-551(11)(g)); Colorado (Colo. Rev. Stat. Ann. § 6-1-716(1)(g)(I)(A)); Delaware (Del. Code Ann. tit. 6, § 12B-101(7)(a)(4)); Florida

(Fla. Stat. Ann. § 501.171(1)(g)(1)(a)(II)); Louisiana (LA Rev Stat § 51:3073(4)(a)(iv)); Maryland (Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(1)); North Carolina (N.C. Gen. Stat. § 75-66(c)(2)); Oregon (Or. Rev. Stat. Ann. § 646A.602(11)(a)(C)); Virginia (Va. Code Ann. § 18.2-186.6); Washington (Wash. Rev. Code § 19.255.005(2)(a)(i)(F)).

[4] See, e.g., Alabama (Ala. Code 1975 § 8-38-2(6)(a)(2)); Colorado (Colo. Rev. Stat. Ann. § 6-1-716(1)(g)(I)(A)); Florida (Fla. Stat. Ann. § 501.171(1)(g)(1)(a)(II)); Virginia (Va. Code Ann. § 18.2-186.6); Washington (Wash. Rev. Code § 19.255.005(2)(a)(i)(F)).

[5] See, e.g., Arizona (A.R.S. § 18-551(11)(h)); Delaware (Del. Code 6 § 12B-101(7)(a)(9)); Maryland (Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(1)); Montana (Mont. Code § 30-14-1704(4)(B)(i)(E)); North Carolina (N.C. Gen. Stat. § 75-66(c)(1)); Virginia (Va. Code Ann. § 18.2-186.6); Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(xiv), Wyo. Stat. Ann. § 40-12-501(a)(vi)); see also Puerto Rico (10 P.R. Laws Ann. § 4051(a)(6) ("Tax information")).

[6] See, e.g., Alabama (Ala. Code 1975 § 8-38-2(6)(a)(2)) ("other unique identification number issued on a government document used to verify the identity of a specific individual"); Fla. Stat. Ann. § 501.171(1)(g)(1)(a)(II) ("other similar number issued on a government document used to verify identity"); Iowa (Iowa Code § 715C.1-2(11)(a)(2) ("other unique identification number created or collected by a government body")); Maryland (Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(1) ("other identification number issued by the federal government")); Missouri (Mo. Rev. Stat. §407.1500(9)(b) ("other unique identification number created or collected by a government body")); New Hampshire (N.H. Rev. Stat. § 359-C:19(IV)(a)(2) ("other government identification number")); Oregon (Or. Rev. Stat. Ann. § 646A.602(11)(a)(C)(iii) ("other identification number issued by the United States")); Puerto Rico (10 P.R. Laws Ann. § 4051(a)(2) ("other official identification")); Texas (Tex. Bus. & Com. Code Ann. § 521.002(1)(A) ("government-issued identification number")).

[7] See Arkansas (Arkansas Code § 4-110-103(7)(E)(i)); Arizona (A.R.S. § 18-551(11)(i)); Colorado (Colo. Rev. Code § 716(1)(g)(I)(A)); Delaware (Del. Code 6 § 12B-101(7)(a)(8)); Iowa (Iowa Code § 715C(11)(5)); Illinois (815 Ill. Comp. Stat. 530/5(1)(F)); Iowa (Iowa Code § 715C.1-2(11)(a)(5)); Louisiana (LA Rev Stat § 51:3073(4)(a)(iv)); Maryland (Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(6)); Nebraska (Neb. Rev. Stat. §§ 87-802(5)(v)); New Mexico (NM Stat § 57-12C-2); New York (N.Y. Gen. Bus. Law § 899-aa(b)(i)(5)); North Carolina (N.C. Gen. Stat. § 75-66(c)(10)); Oregon (Or. Rev. Stat. Ann. § 646A.602(11)(a)(E)); South Dakota (SDCL 22-40-9(10)); Texas (Tex. Bus. & Com. Code Ann. § 521.002(1)(C)); Washington (Wash. Rev. Code § 19.255.005(2)(a)(i)(I)); Wisconsin (Wis. Stat. § 134.98(1)(b)(5)); Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(xiii), Wyo. Stat. Ann. § 40-12-501(a)(vi)).

[8] See Press Release, Attorney General Becerra and Assemblymember Levine Unveil Legislation to Strengthen Data Breach Notification Law (Feb, 21, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-and-assemblymember-levine-unveil-legislation-strengthen; Press Release, Levine Measure to Protect Californians' Personal Data Approved by State Assembly (May 29, 2019), https://a10.asmdc.org/press-releases/20190529-levine-measure-protect-californians-personal-data-approved-state-assembly; Press Release, Levine Measure to Protect Californians' Personal Data Approved by State Legislature (Sept. 5, 2019), https://a10.asmdc.org/press-releases/20190905-levine-measure-protect-californians-personal-data%C2%A0approved-state-legislature.

[9] Senate Bill 1386 (Cal. 2002) (amending Cal. Civ. Code §§ 1798.29, 1798.82), http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.

[10] Cal. Civil Code § 1798.84(b).

[11] Senate Bill No. 24 (enacted Aug. 31, 2011; effective Jan. 1, 2012).

[12] For example, for a summary of recent changes in New York taking effect on Oct. 23, 2019, see M. Krotoski & M. Hirschprung, Preparing for the New Data Breach and Security Requirements Under the New York SHIELD Act, New York Law Journal (Oct. 1, 2019) (expanding the definition of "private information" to include: (1) biometric information; (2) an account, credit or debit card number, if the number could be used to access an individual's financial account without any additional identifying information, such as a security code or password; and (3) "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account").

[13] Senate Bill 1386, § 2(e) (Cal. 2002) (amending Cal. Civ. Code §§ 1798.29, 1798.82), http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.

[14] Assembly Bill 1298 (enacted Oct. 14, 2007; effective Jan. 1, 2008).

[15] Senate Bill 34 (enacted Oct. 6, 2013; effective Jan. 1, 2016).

[16] Senate Bill 46 (enacted Sept. 27, 2013; effective Jan. 1, 2014) (codified at Cal. Civ. Code § 1798.82(h)(2)), http://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201320140SB46&version=20130SB4695CHP; see also M. Krotoski & S. Tester, LawFlash, Three States Join Others To Expand Personal Information Definition to Include Usernames Or Email Addresses (Jan. 3, 2017) (Illinois, Nebraska, and Nevada join trend).

[17] See Florida Senate Bill 1524 (approved June 20, 2014; effective July 1, 2014) (codified at Fla. Stat. Ann. § 501.171(1)(g)(1)(b)); Wyoming SF 36 (approved March 2, 2015; effective July 1 2015) (codified at Wyo. Stat. Ann. § 6-3-901(b)(ix)).

[18] Alabama (Ala. Code 1975 § 8-38-2(6)(a)(6)); Arizona (A.R.S. § 18-551(7)(a)(ii)); Colorado (Colo. Rev. Stat. Ann. § 6-1-716(1)(g)(I)(B)); Delaware (Del. Code Ann. tit. 6, § 12B-101(7)(a)(5)); Illinois (815 Ill. Comp. Stat. 530/5(2)); Maryland (Md. Code Ann., Com. Law § 14-3501(e)(1)(ii)); Nebraska (Neb. Rev. Stat. Ann. § 87-802(5)(b)); Nevada (Nev. Rev. Stat. Ann. § 603A.040(1)(e)); New Jersey (N.J. Stat. Ann. § 56:8-161); New York (N.Y. Gen. Bus. Law § 899-aa(b)(ii)); Rhode Island (R. I. Gen. Laws § 11-49.3-3(8)(v)); South Dakota (SDCL 22-40-9(9)); Washington (Wash. Rev. Code § 19.255.005(2)(a)(ii)); Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(xiv), Wyo. Stat. Ann. § 40-12-501(a)(vi)); see also Puerto Rico (10 P.R. Laws Ann. § 4051(a)(4) ("Names of users and passwords or access codes to public or private information systems.")).

[19] See, e.g., South Dakota (SDCL 22-40-9(1)); Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(x), Wyo. Stat. Ann. § 40-12-501(a)(vi)).

[20] See, e.g., Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(x), Wyo. Stat. Ann. § 40-12-501(a)(vi)).

[21] See, e.g., South Dakota (SDCL 22-40-9(8)).

[22] See, e.g., North Dakota (N.D. Cent. Code Ann. § 51-30-01(4)(a)(5)); Texas (Tex. Bus. & Com. Code Ann. § 521.002(1)(A); Washington (Wash. Rev. Code § 19.255.005(2)(a)(i)(D)).

[23] See, e.g., North Carolina (N.C. Gen. Stat. § 75-66(c)(8); North Dakota (N.D. Cent. Code Ann. § 51-30-01(4)(a)(10)).

[24] See, e.g., Delaware (Del. Code tit. 6, § 12B-101(7)(a)(6)); Wisconsin (Wis. Stat. § 134.98(1)(b)(4)).

[25] See Cal. Civ. Code § 1798.82(h)(1)(F).

[26] See, e.g., Georgia (Ga. Code Ann. § 10-1-911(6)(D)); Maine (10 Me. Rev. Stat. Ann. § 1347(6)(D)); North Carolina (N.C. Gen. Stat. § 75-66(c)(12); South Dakota (SDCL 22-40-9(8)).

[27] See, e.g., Alaska (AK Stat § 45.48.910(7)(B)(v)).

[28] See, e.g., North Dakota (N.D. Cent. Code Ann. § 51-30-01(4)(a)(6)); Texas (Tex. Bus. & Com. Code Ann. § 521.002(1)(B)).

[29] See, e.g., North Dakota (N.D. Cent. Code Ann. § 51-30-01(4)(a)(9)).

[30] See, e.g., Alabama (Ala. Code 1975 § 8-38-2(6)(a)(2)); Alaska (AK Stat § 45.48.910(7)(B)(ii)); California (Cal. Civ. Code § 1798.82(h)(1)(B)); Connecticut (Conn. Gen. Stat. §§ 36a-701b(a)(2)(B)); Georgia (Ga. Code Ann. § 10-1-911(6)(B)); Hawaii (Haw. Rev. Stat. § 487N-1); Maine (10 Me. Rev. Stat. Ann. § 1347(6)(B)); Maryland (Md. Code Ann., Com. Law § 14-3501(e)(1)(i)(2)); Oregon (Or. Rev. Stat. Ann. § 646A.602(11)(a)(B)); Utah (Utah Code Ann. § 13-44-102(4)(a)(iii)); Virginia (Va. Code Ann. § 18.2-186.6); Washington (Wash. Rev. Code § 19.255.005(2)(a)(i)(B)); Wisconsin (Wis. Stat. § 134.98(1)(b)(2)); Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(ii), Wyo. Stat. Ann. § 40-12-501(a)(vii)).

[31] See, e.g., Colorado (Colo. Rev. Stat. § 716(1)(g)(I)(A)); Washington (Wash. Rev. Code § 19.255.005(2)(a)(i)(F)).

[32] See, e.g., Rhode Island (R. I. Gen. Laws § 11-49.3-3(8)(ii)); South Dakota (SDCL 22-40-9(1)); Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(x), Wyo. Stat. Ann. § 40-12-501(a)(vi)).

[33] See, e.g., Puerto Rico (10 P.R. Laws Ann. § 4051(a)(2)).

[34] See, e.g., Wyoming (Wyo. Stat. Ann. § 6-3-901(b)(viii), Wyo. Stat. Ann. § 40-12-501(a)(vi)).

[35] See, e.g., Texas (Tex. Bus. & Com. Code Ann. § 521.002(1)(E)).

[36] See, e.g., Texas (Tex. Bus. & Com. Code Ann. § 521.002(1)(D)).

[37] See, e.g., Puerto Rico (10 P.R. Laws Ann. § 4051(a)(7)).

[38] See, e.g., Mark Krotoski & Martin Hirschsprung, The Government's Role in Promoting and Leading Effective Cybersecurity, BNA's Privacy & Security Law Report, 16 PVLR 1555 (Dec. 4, 2017), https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2017/bloomberglaw_govtrolecybersecurity_4dec17.ashx?la=en&hash=2A39124A43EB65C2233EA86859CA34EC1671ABD3.

[39] See, e.g., Mark Krotoski, Lucy Wang, & Jennifer Rosen, The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze, BNA's Privacy & Security Law Report, 15 PVLR 271

(Feb.8,2016), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.ashx?la=.

[40] Assembly Bill 375 (enacted June 28, 2018; effective January 1, 2020) (codified at Cal. Civil Code §§ 1798.100 to 1798.198), amended, Senate Bill 1121 (Sept. 13, 2018). The CCPA is available at: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[41] Cal. Civ. Code § 1798.140(o)(1).

[42] Id. §§ 1798.140(o) and 1798.145(c)-(f).

[43] Id. § 1798.155(b).

[44] Id. § 1798.185(c).

[45] See California Department of Justice, Notice Of Proposed Rulemaking Action (Notice to be Published on October 10, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf; see also Press Release, Attorney General Becerra Publicly Releases Proposed Regulations under the California Consumer Privacy Act (Oct. 10, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-publicly-releases-proposed-regulations-under-california.

[46] Cal. Civ. Code § 1798.150(a) (as amended by Assembly Bill 1355 (effective Oct. 11, 2019)).

[47] Id. § 1798.81.5(b).

[48] Id. § 1798.81.5(d)(1)(A).

[49] Id.