Keeping Pace With California's Data Privacy And Security Laws

In 2003, California became the first state to enact a data breach notification law.[1] Under this law, all persons, businesses, state and local agencies that own or license a database of personally identifiable information must notify a California resident when his or her unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[2] Since 2003, the law has been amended seven times, with the three most recent legislative enactments, effective in January of 2016, clarifying important statutory requirements.

First, Assembly Bill (A.B.) 964 added a new definition for the term "encrypted," which is referenced throughout the statute.[3] 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."[4] Because the law requires notification only after a breach of unencrypted data, the new definition clarifies that notification is required unless personal information is entirely unreadable and, thus, would not necessarily threaten an individual's security. While California law does not yet affirmatively require data encryption, the data breach notification law incentivizes a more widespread practice of encryption by only focusing on notifications requirements for unencrypted data.

In light of the growing need to protect personal data security, the California Attorney General provided practical advice in the February 2016, *California Data Breach Report: 2012-2015*, which should not be ignored. The Attorney General recommends that organizations should "consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers."[5] Specifically, the Attorney General notes that it "is a particular imperative for health care, which appears to be lagging behind other sectors in this regard."[6] Creating a standard for what types of data should be encrypted and how to impose such requirement is a pressing issue for the Attorney General.

Second, Senate Bill (S.B.) 570, outlined specific requirements for how notice should be provided once it is determined a breach has occurred.[7] The notification of the breach must be titled "Notice of Data Breach," and include the headings "What Happened," "What Information was Involved," "What We Are Doing," "What You Can

Do," "Other Important Information," and "For More Information." Additionally, the statute now provides a model security breach notification form, which if utilized, can deem an organization presumptively in compliance with the notification requirement. [8] Since 2011, organizations have been required to also notify the Attorney General when, as a result of a single breach, more than 500 California residents were notified of a breach of their personal information.[9] From 2012-2015, the Attorney General received 657 data breach reports, the majority of which resulted from security failures.[10]

Third, S.B. 34 expanded the definition of what constitutes "personal information" with regard to data breach notification, and in particular, to include information collected through automated license plate recognition systems.[11] In 2013, this definition of personal information was last amended to include a user name and password or security question and answer.[12] Ultimately, a clear trend is visible by which the legislature seeks to broaden the statutory scheme as additional breaches are reported to encompass new types of "personal information."

California's data privacy and security laws continue to evolve. Most recently, Assembly member Chau introduced A.B. 2828 to expand the disclosure notification requirement to also include encrypted information if the encryption keys have been compromised.[13] In addition, the Attorney General's *California Data Breach Report* clarified, for the first time, what constitutes "reasonable security practices and procedures"[14] under the law, stating that the failure to implement all 20 Center for Internet Security's Critical Security Controls constitutes a lack of reasonable security.[15]

Careful scrutiny of California's data privacy and security laws is necessary in order to maintain compliance with the collection, maintenance, protection, and notification provisions concerning personal data.

[1] See 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700), operative July 1, 2003.

[2] See Cal. Civ. Code, §§ 1798.29, subd. (a) [applying to agencies], 1798.82, subd. (a) [applying to businesses and persons].

[3] See 2015 Cal. Legis. Serv. Ch. 522 (A.B. 964), effective January 1, 2016.

[4] See Cal. Civ. Code, §§ 1798.29, subd. (h)(4), 1798.82, subd. (i)(4).

[5] Kamala D. Harris, Attorney General, California Department of Justice, *California Data Breach Report: 2012*-2015, (February 2016), Executive Summary.

[6] Kamala D. Harris, Attorney General, California Department of Justice, *California Data Breach Report: 2012*-2015, (February 2016), Executive Summary.

[7] See 2015 Cal. Legis. Serv. Ch. 543 (S.B. 570) effective January 1, 2016.

[8] See Cal. Civ. Code, §§ 1798.29, subd. (d)(1)(D); 1798.82, subd. (d)(1)(D).

[9] See Cal. Civ. Code, §§ 1798.29, subd. (e); 1798.82, subd. (f).

[10] Kamala D. Harris, Attorney General, California Department of Justice, *California Data Breach Report: 2012-2015*, (February 2016), Executive Summary.

[11] 2015 Cal. Legis. Serv. Ch. 532 (S.B. 34), effective January 1, 2016.

[12] 2013 Cal. Legis. Serv. Ch. 396 (S.B. 46).

[13] See 2015 California Assembly Bill No. 2828, California 2015-2016 Regular Session, 2015 California Assembly Bill No. 2828, California 2015-2016 Regular Session.

[14] Cal. Civ. Code, § 1798.81.5.

[15] Kamala D. Harris, Attorney General, California Department of Justice, *California Data Breach Report: 2012-2015*, (February 2016), Executive Summary.

For more information, please contact:

Robert A. McFarlane, Partner
415-995-5072
rmcfarlane@hansonbridgett.com