CLIENT ALERTS & INSIGHTS

A New Wave Of Data Security Regulations Foreshadows What Is To Come

DECEMBER 4, 2018

Authors: Michael D. Stovsky, Kristopher J. Chandler

California "Connected Devices" Law

On September 28, 2018, California passed a new law that raised the baseline for the security of Internet of Things ("IoT") devices, or "connected devices." Under this new law, manufacturers of connected devices are required to include reasonable security measures, at least some measure of protection against unauthorized access, with all "connected devices." With enforcement beginning on January 1, 2020, California Senate Bill No. 327 will most likely increase the cost of manufacturing IoT devices, as manufacturers will now be required to equipment the devices with a "reasonable security features."

The new manufacturing requirement applies to all "connected devices." Under the language of the law, a "connected device" is any device, or other physical object that is capable of connecting to the Internet and that is assigned an IP address or Bluetooth address. Such a broad definition casts a wide net of enforcement across the industry and seeks to increase the data security protections on any device that has the potential to transmit collected data.

The law provides that if a connected device is equipped with a means of authentication outside a local area network, the obligation to implement a reasonable security feature is satisfied if the manufacturers equips the device with one of the following: (1) a preprogrammed password unique to each device manufactured; or (2) a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time. Outside of those specifically enumerated security features, manufacturers will satisfy the obligations of the law by equipping the device with a security feature that is (1) appropriate to the nature and function of the device; (2) appropriate to the information it may collect, contain, or transmit; and (3) designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. The law requires that each manufacture equipment each connected device with such security feature or features that satisfies those three enumerate requirements.

Those persons or entities that manufacturer, or contract with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California will all be required to satisfy the increased data security mandate. Based on this applicability language, an entity will not be able to avoid its obligations by contracting with a third party for manufacturing. However, based on a narrow reading of the law, it may be possible to avoid triggering its applicability if you purchase "connected devices" for resale. It will be interesting to see how a court interprets this possible exception.

Ohio Incentivizing Cybersecurity Programs

In related news, this past August, Ohio became the first state to pass legislation incentivizing corporate entities to develop and implement strong and effective data privacy and cybersecurity policies and procedures. Beginning on November 1, 2018, the Ohio Data Protection Act ("DPA") established a safe harbor from data breach litigation. Under the DPA, an organization can claim an affirmative defense to a lawsuit that alleges a data breach was caused by the organization's failure to implement a cybersecurity framework. To qualify for the affirmative defense, the organization must implement and maintain a cybersecurity program that reasonably complies with one of the following industry-recognized cybersecurity frameworks enumerated in the DPA:

1. National Institute of Standards and Technology ("NIST") Cybersecurity Framework;

2. The Federal Risk and Authorization Management Program Security Assessment Framework;

3. The Center for Internet Security Critical Security Controls for Effective Cyber Defense'

4. The International organization for Standardization/International Electrotechnical Commission 27000 Family - Information Security Management Systems;

5. HIPAA Security Rule;

6. Gramm-Leach-Bliley Safeguards Rule;

7. The Federal Information Security Modernization Act; or

8. The Heath Information Technology for Economic and Clinical Health Act

Under the DPA, adhering to the cybersecurity framework will be voluntary, though there is a significant incentive to establishing and maintaining these cybersecurity controls, the affirmative defense. The DPA specifically states that it does not allow a person to sue an organization for failing to follow the DPA's cybersecurity requirement, unless another law would allow the person to do so. As currently implemented, the DPA requires that organizations implement a cybersecurity program that "reasonably conforms" with one of the above enumerate frameworks, though it is unclear how "reasonably conforms" will be interpreted by a future fact finder. It is important to note that the DPA does not bestow judicial immunity on an organization that satisfies the language of the DPA. Instead, the DPA merely provides a qualifying entity a new defense in a judicial proceeding. Entities can still be found liable under data security actions even if they satisfy the obligations of the DPA.

Colorado Rolls Out New Consumer Data Protection Law

Along the same lines as the recent California Consumer Protection Act slated to go into effect in 2020, Colorado adopted and began enforcement of a new consumer protection act that is designed as one of the most demanding standards for consumer data protection in the United States. The Protections for Consumer Data Privacy Act ("PCDPA"), signed into law May 29, 2018 and going into effect September 1, 2018, requires businesses and government agencies to maintain a written corporate policy describing how they will dispose of personally identifiable information ("PII"), notify consumers of a data breach within 30 days of the breach, and take "reasonable" steps to protect the PII it maintains.

Broad in nature, the PCDPA applies to all "covered entities," those entities or persons that maintain, own, or license PII in the course of the person's or entity's business, vocation, or occupation. Under

the language of the act, PII includes social security numbers, passwords, pass codes, driver's license numbers, passport numbers, biometric data, and financial account numbers. Though the PCDPA does not define what satisfies "reasonable," the security procedures and practices maintained by the new legislation must be "appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." Designed to be flexible depending on the size of the business operations, it will be interesting to follow any judicial interpretations of this law as courts attempt to establish some essence of certainty for what satisfies the required data security practices and procedures.

These new California, Ohio, and Colorado initiatives show that more and more states are becoming concerned with data security and privacy and are seeking legislative ways to protect their resident's data. As more and more devices become connected to the Internet, and more business seek to collect and utilize consumer data for entrepreneurial ventures, interested parties will need to keep a close eye on both state and federal enforcement measures in order to keep up-to-date on increasingly more stringent compliance burdens.

For more information on these topics, contact a member of Benesch's Intellectual Property/3iP Practice Group.

Michael D. Stovsky at mstovsky@beneschlaw.com or 216.363.4626.

Kristopher J. Chandler at kchandler@beneschlaw.com or 614.223.9377.