GIBSON DUNN

October 5, 2018

NEW CALIFORNIA SECURITY OF CONNECTED DEVICES LAW AND CCPA AMENDMENTS

To Our Clients and Friends:

California continues to lead the United States in focusing attention on privacy and security of user data and devices. Last week, Governor Jerry Brown signed into law two identical bills requiring manufacturers to include "reasonable security feature[s]" on all devices which are "capable of connecting to the Internet" (commonly known as the Internet of Things).[1] The law is described as the first of its kind in the United States, and comes just three months after passage of the California Consumer Privacy Act of 2018 ("CCPA");[2] both laws are set to take effect January 1, 2020.[3] Collectively, these laws represent a dramatic expansion of data privacy law that will impact the products and processes of many companies.

Also last week, Governor Brown signed into law Senate Bill 1121, which implemented amendments to the CCPA relating primarily to enforcement of the provisions, and clarification of exemptions relating to medical information.

Security of Connected Devices

The new law is aimed at protecting "connected devices" from unauthorized access, and requires "reasonable security feature[s]" proportional to the device's "nature and function" and the "information it may collect, contain, or transmit."[4] There are various notable exclusions, particularly where the devices are covered by certain other laws, or when a company merely purchases devices for resale (or for branding and resale) in California.[5] Nonetheless, the law is unique in that it may require security for Internet-connected products regardless of the type of information or data at issue—a contrast to the CCPA and other data privacy and security laws.

Who Must Comply with the Law?

Anyone "who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California" is subject to the statute.[6] However, the law includes an explicit carve-out that "contract[ing] with another person to manufacture on the person's behalf" does *not* include a "contract only to purchase a connected device, or only to purchase and brand a connected device."[7] Thus, if a company is merely purchasing whole units, and reselling, or even branding and reselling—effectively without the ability to indicate specifications for the device—it will likely not be subject to the new law.

What's Required?

The law applies to manufacturers of "connected devices." A "connected device" is defined as "capable of connecting to the Internet . . . and . . . assigned an Internet Protocol address or Bluetooth address."[8] The number of products falling into this category is increasing at a remarkable rate, and the products span a multitude of applications, from consumer products (such as smart home features, including automatic lights or thermostats controlled remotely), to commercial use cases (such as electronic toll systems and "smart agriculture").

The law requires that such manufacturers "equip the device with a reasonable security feature or features" that is:

- Appropriate to the nature and function of the device;
- Appropriate to the information it may collect, contain, or transmit; and
- Designed to protect the device and its information from unauthorized access, destruction, use, modification, or disclosure.[9]

The law does not specify what is "reasonable," and relies upon the manufacturer to determine what is appropriate to the device. As a result, "reasonable" will likely be further refined through enforcement actions (described below) .

However, the law does provide that a device will satisfy the provisions if it is "equipped with a means for authentication outside a local area network," and (1) each device is preprogrammed with a unique password, or (2) the user must create a "new means of authentication" (such as a password) before the device may be used.[10] [11]

What's Not Covered?

Notably, the law excludes certain devices or manufacturers, particularly where they are covered by other existing laws, and makes clear statements of what this law does *not* do. For example, the law does not apply to[12]:

- Any unaffiliated third-party software or applications the user adds to the device;
- Any provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications;
- Devices subject to security requirements under federal law (e.g., FDA); and
- "Manufacturers" subject to HIPAA or the Confidentiality of Medical Information Act—at least "with respect to any activity regulated by those acts."[13]

How Will It Be Enforced?

The law expressly does not provide for a private right of action, and it may only be enforced by the "Attorney General, a city attorney, a county counsel, or a district attorney."[14] It further does not set forth any criminal penalty, include a maximum civil fine, or specify any other authorized relief. Nonetheless, the authorization of the enumerated entities to enforce it presumably includes the authority for those entities to seek civil fines, as they can under other consumer protection statutes (for example, Section 17206 of the California Business & Professions Code).[15]

What Can You Do?

If your company sells, or intends to sell, a product in California that connects to the Internet, consider:

- Whether the company is a "manufacturer";
- The security features of the device, if any;
- What security features might be reasonable given the nature and function of the device and the nature of the data collected or used;
- Possibilities for alternative, or additional security measures for the specific device; and
- Engineering resources and timeline required to implement additional features.

Many connected devices on the market today already have authentication and security features, but even those that do may benefit from an evaluation of their sufficiency in preparation for this new law. Because the law may require actual product changes, rather than merely policy changes, addressing these issues early is important. Consultation with legal and information security professionals may be helpful.

Amendments to CCPA Signed by Governor Brown on September 23, 2018

As anticipated, the California Legislature has begun to pass amendments to the CCPA, though the current changes are relatively modest. Governor Brown signed the latest amendments to the CCPA on September 23, 2018, which included[16]:

- Extending the deadline for the California Attorney General ("AG") to develop and publish rules implementing the CCPA until July 1, 2020;
- Prohibiting the AG from enforcing the Act until either July 1, 2020, or six months after the publication of the regulations, whichever comes first;
- Limiting the civil penalties that the AG can impose to $2,500 for each violation of the CCPA or up to $7,500 per each intentional violation;

- Removing the requirement for a consumer to notify the AG within 30 days of filing a civil action in the event of a data breach and to then wait six months to see if the AG elects to pursue the case;

- Clarifying that consumers only have a right of action related to a business' alleged failure to "implement and maintain reasonable security procedures and practices" that results in a breach and not for any other violations of the Act;

- Updating the definition of "personal information" to stress that certain identifiers (e.g., IP address, geolocation information and web browsing history) only constitute personal information if the data can be "reasonably linked, directly or indirectly, with a particular consumer or household"; and

- Explicitly exempting entities covered by HIPAA, GLBA and DPPA, as well as California's Confidentiality of Medical Information Act and its Financial Information Privacy Act.

The foregoing amendments may not have been of major significance—they were passed on the last day of the most recent legislative session. The California Legislature is expected to consider more substantive changes to the law when it reconvenes for the 2019 – 2020 session in January 2019, including addressing additional concerns regarding enforcement mechanisms, the law's broad scope, and the sweeping disclosure obligations.

Companies that may be impacted by the CCPA should continue to monitor legislative and regulatory developments relating to the CCPA, and should begin planning for the implementation of this broad statute.

---

[1] Assembly Bill 1906 and Senate Bill 327 contain identical language.

[2] The California Consumer Privacy Act was the subject of a detailed analysis in a client alert issued by Gibson Dunn on July 12, 2018. That publication is available here.

[3] The law will be enacted as California Civil Code Sections 1798.91.04 to 1798.91.06.

[4] Cal. Civil Code § 1798.91.04(a)(1) and (a)(2).

[5] Cal. Civil Code § 1798.91.05(c) and § 1798.91.06.

[6] Cal. Civil Code § 1798.91.05(c).

[7] Cal. Civil Code § 1798.91.05(c).

[8] Cal. Civil Code § 1798.91.05(b).

[9] Cal. Civil Code § 1798.91.04(a)(1), (a)(2), and (a)(3).

[10] Cal. Civil Code § 1798.91.04(b) (emphasis added).

[11] Authentication is simply defined as a "method of verifying the authority" of a user accessing the information or device. Cal. Civil Code § 1798.91.05(a).

[12] Cal. Civil Code § 1798.91.06.

[13] That said, those laws generally require stricter provisions for security measures.

[14] Cal. Civil Code § 1798.91.06(e).

[15] *See* Cal. Bus. & Prof. Code § 17204.

[16] S.B. 1121. S. Reg. Sess. 2017-2018. (CA 2018)

The following Gibson Dunn lawyers assisted in the preparation of this client alert: Joshua A. Jessen, Benjamin B. Wagner, and Cassandra L. Gaedt-Sheckter.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

United States

Alexander H. Southwell - Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Christopher Chorba - Los Angeles (+1 213-229-7396, cchorba@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Shaalu Mehra - Palo Alto (+1 650-849-5282, smehra@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)

GIBSON DUNN

Europe

Ahmed Baladi - Co-Chair, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)207071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 (0)1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Nicolas Autet - Paris (+33 (0)1 56 43 13 00, nautet@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)

Asia

Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)