Published on *The National Law Review* https://natlawreview.com

California Considers Connected Product Security and Data Collection Notice Requirements

Article By:

Tracy P. Marshall

Sheila A. Millar

California, the state that so often seems to strive to dictate policy for the whole country, is now considering a bill that would use reasonable-sounding goals to impose a heavy burden on connected product makers and sellers around the country. A state senator has proposed a bill to require the manufacturers of connected products to implement security measures and provide specific notices to consumers about information collection practices, among other objectives. The sponsor introduced the bill, ***S.B. 327***, on February 13, 2017, styling it the "***Teddy Bear and Toaster Act***."

The bill itself is fairly simple, with only three sections. However, the requirements apply broadly to all connected products, meaning "any device, sensor, or other physical object that is capable of connecting to the Internet, directly or indirectly, or to another connected device." This language is so broad that it would apply to any device that is capable of connecting to the internet or to another device, including computers, toys, appliances, cell phones, and professional equipment. Even products such as Ethernet and USB cables potentially would be included, since they are, strictly speaking, "physical objects" that can connect to the internet or other connected devices and transmit information.

Manufacturers would be obligated to implement "reasonable security features" appropriate to the nature of the device and the information that it may collect, contain, or transmit. Devices would have to have an indication that they are collecting information, and would have to be designed to obtain consumer consent before "collect[ing] or transmit[ting] information beyond what is necessary ... to fulfill a consumer transaction or for the stated functionality of the connected device."

Sellers of connected products would be required to provide notice of information collection functions *at the point of sale*, including, for example, the capability of collecting audio, video, location, biometric, or other personal or sensitive data. Note that "sellers" may or may not be the manufacturer, so retailers may have obligations that would be almost impossible for them to fulfill. Notice of a privacy policy would be required, along with a description of how a device or device owner would be notified of security patches and updates. Further, even though "sellers" may lack any visibility into the security patch/update process, they appear to be obliged to provide consumers with direct notification of security patches and updates for the products they sell.

There are numerous standards and guidelines that businesses can and should consider in developing connected products, but reasonable security is a necessarily flexible concept that only makes sense in the context of the particular product, type of information, and potential risk it poses. The Federal Trade Commission (FTC) has pursued numerous enforcement actions against companies that failed to provide "reasonable" security. It, too, recognizes that the appropriate level of security will depend on specifics.

Requiring a visible indicator of data collection could force reengineering of devices where the nature of the device itself evidently involves personal information collection. For example, should a computer or cell phone blink when a user sends or receives an email? Although the bill lacks details on enforcement, in theory the bill could be enforceable by the state attorney general and local district attorneys through a *parens patriae* action. Individual consumer and class action lawsuits could even be permitted.

While concerns about connected products have been in the news, a strong legal framework governing privacy and security of information collected online from children is already in place at the federal level. The ***Children's Online Privacy Protection Act (COPPA)*** covers the online collection of data from children. The FTC has confirmed that it has jurisdiction over products or services that involve the collection of online information from children.

COPPA includes the type of safeguards the sponsors seek. For example, COPPA requires operators of websites or online services directed to children to:

- provide notice of information collection;
- obtain verifiable parental consent prior to collection use or disclosure of a child's personal information (absent an exception);
- provide parents with reasonable means to review the personal information from a child and to require deletion;
- not collect more information than is necessary to participate in a particular online activity; and
- "establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children."

See 16 C.F.R. §312.3. These requirements are further detailed in other sections of the COPPA Rule, including §312.4 (notice); §312.5 (parental consent); §312.6 (right of parent to review personal information provided by a child); §312.7 (prohibition against conditioning a child's participation on collection of personal information); §312.8 (confidentiality, security and integrity of personal information collected from children); and §312.10 (data retention and deletion requirements).

Makers of connected products do need to consider privacy and security issues. However, this bill could discourage innovation, conflict with the federal children's privacy law, and increase litigation. Anyone making or selling connected products should pay close attention to the progress of this bill.

National Law Review, Volume VII, Number 87

Source URL:https://natlawreview.com/article/california-considers-connected-product-security-and-data-collection-notice