SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 2392 (Irwin)
Version: March 28, 2022
Hearing Date: June 21, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

Information privacy: connected devices: labeling

DIGEST

This bill provides that manufacturers of connected devices satisfy existing security requirements regarding connected devices by meeting certain baseline labeling standards established by the National Institute of Standards and Technology.

EXECUTIVE SUMMARY

Juniper Research, a technology market research and analytics consulting firm, estimates that the number of Internet of Things (IoT) connections in 2024 will reach 83 billion, a 130 percent increase from 2020. [1] As with all technological advances, the virtually endless opportunities come with serious privacy and security issues. The billions of connected devices have varied functionality and implemented various levels of security.

Existing law requires such devices to be equipped with reasonable security features that are appropriate for the device, as provided. This bill creates a safe harbor within that statute that encourages manufacturers to meet baseline standards established by the National Institute of Standards and Technology (NIST) in response to an executive order issued by President Biden. A manufacturer is deemed in compliance with the statute if the connected device meets or exceeds the NIST baseline criteria.

This bill is author sponsored. There is no known support. Consumer Reports has written in opposition arguing the existing statute is already weak and this bill simply adds an additional safe harbor.

---

[1] Press Release, *IoT Connections to Reach 83 Billion by 2024, Driven by Maturing Industrial Use Cases* (March 31, 2020) Juniper Research, https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024. All internet citations are current as of June 9, 2022.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, Sec. 1.)

2) Requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are all of the following:
    a) appropriate to the nature and function of the device;
    b) appropriate to the information it may collect, contain, or transmit; and
    c) designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code § 1798.91.04(a).)

3) Provides that subject to all of the above requirements, if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if the preprogrammed password is unique to each device manufactured or the device contains 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. (Civ. Code § 1798.91.04(b).)

4) Defines "connected device" as any device or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address. (Civ. Code § 1798.91.05.)

5) Provides a series of clarifying exemptions and limitations to the above provisions. (Civ. Code § 1798.91.06.)

6) Requires 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 and requires such businesses to contractually require nonaffiliated third parties to which it discloses such personal information to similarly protect that information. (Civ. Code § 1798.81.5(b), (c).)

This bill:

1) Provides that a manufacturer of a connected device satisfies the above requirements if the connected device does all of the following:
    a) meets or exceeds the baseline product criteria of a NIST conforming labeling scheme;

b) satisfies a conformity assessment as described by a NIST conforming labeling scheme that includes a third-party test, inspection, or certification; and
c) bears the binary label as described by a NIST conforming labeling scheme.

2) Defines "NIST conforming labeling scheme" to mean a labeling scheme conforming to the Cybersecurity White Paper titled "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products" published by the National Institute of Standards and Technology (NIST) on February 4, 2022.

COMMENTS

1. The rise of connected devices

Kevin Ashton is widely credited with coining the phrase "Internet of Things" (IoT). The phrase refers to technology that allows an ever-growing list of devices to communicate wirelessly with other devices. Two decades later, the concept is well known and has gained increasing traction in recent years. Currently, everything from toasters and baby dolls to televisions and thermostats are connected to the Internet, gathering and using a wide range of information. This technology has limitless possibilities. It has revolutionized the capabilities of medical devices and made shopping easier. "The potential economic value that the IoT could unlock is large and growing. By 2030, [McKinsey Digital estimates] that it could enable $5.5 trillion to $12.6 trillion in value globally, including the value captured by consumers and customers of IoT products and services."[2]

However, along with the promise IoT brings comes serious privacy and security concerns. Corporations are rapidly networking the physical world and gathering data from everything. Many of these devices collect a vast amount of personal and intimate information. If not properly secured, this immense amount of private information can be vulnerable to breaches. In addition, many of these devices can be directly hacked into, allowing strangers to conduct surreptitious surveillance on homes or to communicate through devices directly. Perhaps most disturbing, consumers may not even be aware of the full capabilities of these products or the information that is being collected.

[2] Michael Chui, et al., *IoT value set to accelerate through 2030: Where and how to capture it* (November 9, 2021) https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it.

2. The legislative response

To address these innovations and their attendant risks, SB 327 (Jackson, Ch. 886, Stats. 2018)[3] was introduced to establish baseline security requirements for "connected devices," defined as any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address. SB 327 created Civil Code section 1798.91.04. Subdivision (a) of that statute requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are 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 any information contained therein from unauthorized access, destruction, use, modification, or disclosure. The law also has a series of clarifying exemptions and limitations to the above provisions.

Section 1798.91.04(b) addresses one specific functionality of connected devices, a means for authentication outside a local area network. The bill provides that it shall be deemed a reasonable security feature if the preprogrammed password is unique to each device manufactured or the device contains 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. The statute thereby provides one example of what is deemed a "reasonable security feature" with regard to the ability to remotely connect into a device. However, this provision does not act as a safe harbor even for a device with this security feature as there may be other elements of the device requiring other features. The provision makes it clear that it is still "[s]ubject to all of the requirements of subdivision (a)."

3. Further responding to the surge in IOT devices

Concerns continue to exist that IOT devices are not adequately protected. The author points to a study conducted by NIST in 2019 that evaluated the security of select consumer connected devices:

> The results of the review showed that all reviewed IoT devices implemented at least some cybersecurity features. Common features that devices supported included secure communications among components of the consumer home IoT ecosystem using TLS 1.2, password protection for applications and devices, and secure access to the IoT devices from various user interfaces.
>
> These features were not always implemented, though, or did not all have the same level of maturity across devices in a category. Many devices provided update features, but most categories had some issue with the

[3] Another bill, AB 1906 (Irwin, Ch. 860, Stats. 2018) was later introduced and the bills were eventually merged into identical vehicles with contingent enactment.

> security of the update process, such as lack of automatic download options; unprotected update communications; or insufficient control provided to the user to schedule or stop automatic updates, including the inability to roll back an update if needed.[4]

President Biden emphasized the gravity of the cybersecurity issues facing the nation in an executive order issued last May:

> The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.[5]

As part of the order, the Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, was required to initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of IoT devices and software development practices and consider ways to incentivize manufacturers and developers to participate in these programs. In addition, he ordered the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, to identify IoT cybersecurity criteria for a consumer labeling program, and to consider whether such a program may be operated in conjunction with or modeled after existing government programs. The order stated:

> The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to

---

[4] Michael Fagan, et al., *Security Review of Consumer Home Internet of Things (IoT) Products* (October 2019) NIST, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf.

[5] *Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021) The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

> inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

In response to this mandate, NIST published "Recommended Criteria for Cybersecurity Labeling of Consumer IoT Products."[6] The white paper lays out "recommended criteria for a cybersecurity labeling effort for consumer internet of things (IoT) products." However, it specifically states that rather than "establishing its own scheme or program" or "designing or proposing a design of a consumer IoT product label," the document identifies key elements of a potential labeling scheme with criteria recommended by NIST stated in terms of minimum requirements and desirable attributes.

This bill seeks to create a safe harbor within the connected device statute that incentivizes manufacturers to implement security features that meet this criteria. It provides that a manufacturer of a device is deemed to have complied with Section 1798.91.04(a) if the device does the following:

- meets or exceeds the baseline product criteria of a NIST conforming labeling scheme;
- satisfies a conformity assessment as described by a NIST conforming labeling scheme that includes a third-party test, inspection, or certification; and
- bears the binary label as described by a NIST conforming labeling scheme.

The bill ties this to the white paper discussed above by defining "NIST conforming labeling scheme" as a "labeling scheme conforming to the Cybersecurity White Paper titled 'Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products' published by the National Institute of Standards and Technology (NIST) on February 4, 2022."

According to the author:

> AB 2392 will help Californians more easily identify secure Internet of Things (IoT) devices by encouraging the development and voluntary [adoption] of consumer-friendly cybersecurity labels. While California already has the strongest security requirements in law for IoT devices, President Biden and NIST's recent efforts on consumer cybersecurity

[6] NIST Cybersecurity White Paper, *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* (February 4, 2022) NIST, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

> labels provide us a key opportunity to provide even greater security and confidence to California consumers.

4. Stakeholder positions

Consumer Reports writes in opposition to the bill:

> Internet-connected devices like smart speakers and cameras are growing in popularity, leaving more and more consumers vulnerable to security breaches. In 2018, California adopted a first-of-its-kind law requiring manufacturers to adopt reasonable security procedures to keep IoT devices protected from hackers. Unfortunately, because the 2018 measure already included a safe harbor for enabling a device with a password — even though passwords are just one element of reasonable security — existing law does not adequately protect the security of these devices.
>
> This bill, AB 2392, proposes to add a new safe harbor to the IoT security requirement — for compliance with the recent National Institute of Standards and Technology (NIST) labeling framework — compounding the problems with the existing law. Neither safe harbor is suited to constitute reasonable security. At the very least, we recommend replacing the existing safe harbor for unique passwords in Cal. Civ. Code § 1798.91.04(b) with a stronger safe harbor, similar to the one proposed in this bill, but adjusted to account for updates to the NIST document.

In response to the specific request that the bill and the standard therein should account for any updates to the NIST document, the author has agreed to an amendment that requires manufacturers to maintain standards that meet the minimum criteria in the existing white paper and any revisions or successor publications. This ensures that devices will keep up with advances in technology and the standards that evolve with it.

In addition, the Association of Home Appliance Manufacturers writes in a support if amended position. It argues that the bill could be read to require a NIST label and urges clarification that compliance with NIST labelling standards is one route to comply with the law. In response, the author has agreed to amendments that make that clarification.

SUPPORT

None known

OPPOSITION

Consumer Reports

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

SB 327 (Jackson, Ch. 886, Stats. 2018) *See* Comment 2.

AB 1906 (Irwin, Ch. 860, Stats. 2018) *See* Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 62, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)

****