Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2392 (Irwin) – As Amended March 28, 2022

SUBJECT: Information privacy: connected devices: labeling

SUMMARY: This bill would specify that a manufacturer of a connected device satisfies existing law requiring the device to be equipped with reasonable security features if the connected device complies with a labeling scheme that conforms to criteria developed by the National Institute on Standards & Technology (NIST), as specified. Specifically, **this bill would**:

1) Specify that a manufacturer of a connected device satisfies the requirements in existing law pertaining to reasonable security features on connected devices if the connected device does all of 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.

2) Define "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 NIST on February 4, 2022.

3) Repeal a title in the Civil Code that is duplicative to the title being amended.

4) Makes findings and declarations, on behalf of the Legislature, relating to the NIST publication detailing recommendations for a cybersecurity labeling scheme for IoT products.

EXISTING LAW:

1) Requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are all of the following: 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. (Civ. Code Sec. 1798.91.04(a).)

2) Specifies that, subject to the requirements in 1), above, if a connective device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under 1), above, if either of the following requirements are met: 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 Sec. 1798.91.04(b).)

3) Defines "connected device", for the purposes of 1) and 2), above, to mean 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 Sec. 1798.91.05(b).)

4) Defines "security feature", for the purposes of 1) and 2), above, to mean a feature of a device designed to provide security for that device. (Civ. Code Sec. 1798.91.05(d).)

5) Defines "manufacturer", for the purposes of 1) and 2), above, to mean the person 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. (Civ. Code Sec. 1798.91.05(a).)

6) Establishes the information security law, which requires a business that owns, licenses, or maintains personal information, as defined, 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. (Civ. Code Sec. 1798.81.5(b).)

7) Requires a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to the provision in 6), above, to require by contract that the third party 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. (Civ. Code Sec. 1798.81.5(c).)

FISCAL EFFECT: Unknown

COMMENTS:

1) Purpose of this bill: This bill seeks to provide additional clarity as to how manufacturers of connected devices can comply with existing law requiring the device to be equipped with a reasonable security feature or features, by specifying that compliance with a NIST conforming labeling scheme is sufficient to satisfy that requirement. This bill is author sponsored.

2) Author's statement: According to the author:

> Over the past decade there has been an explosion of connected devices in the home. From traditional smart phones, laptops, and printers, to light bulbs, thermostats, and vacuums, nearly every part of our lives has developed a "smart" version that can be automated and controlled remotely. While this has enormous benefits for consumers, it also created personal and societal risks. […]
>
> As identified by E.O. 14028, and NIST's recommendation, a robust labeling scheme that educates and informs consumers about the security of the devices they are considering purchasing is the most accessible and effective way to limit personal and societal risk when using IoT devices. Consumers aren't experts and need easily identifiable indicators, like labels, to understand a device has verified security features.
>
> This bill will create additional value for manufacturers by creating an additional pathway to avoid potential litigation, through making participation in a NIST conforming labeling scheme satisfy the requirement to equip a connected device with reasonable security features. This incentive also benefits consumers as the NIST guidelines, and this bill explicitly, require a third party assessment of the IoT device's security, meaning the IoT

marketplace will be more likely to have easily identifiable and verified secure devices available for purchase by Californians, with little to no due diligence needed by the consumer.

3) **Internet of things (IoT) and "reasonable security features"**: The internet of things (IoT) generally refers to the growing constellation of appliances, devices, and other goods with the capacity for interconnectivity either through the internet or through more local means of interface. As a 2014 Forbes article on the topic describes:

> Simply put, [the IoT] is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. [I]f it has an on and off switch then chances are it can be a part of the IoT. […] The IoT is a giant network of connected 'things' (which also includes people). The relationship will be between people-people, people-things, and things-things. […] On a broader scale, the IoT can be applied to things like transportation networks: 'smart cities' which can help us reduce waste and improve efficiency for things such as energy use; this helping us understand and improve how we work and live.[1]

Juniper Research, a technology market research and analytics consulting firm, estimates that the number of IoT connections in 2024 will reach 83 billion, a 130% increase from 2020[2]. This meteoric rise in IoT does not come without risks. As the same 2014 Forbes article points out:

> The reality is that the IoT allows for virtually endless opportunities and connections to take place, many of which we can't even think of or fully understand the impact of today. It's not hard to see how and why the IoT is such a hot topic today; it certainly opens the door to a lot of opportunities but also to many challenges. Security is a big issue that is oftentimes brought up. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also opens up companies all over the world to more security threats. Then we have the issue of privacy and data sharing.

A 2017 report by the U.S. Department of Justice (DOJ) Criminal Division's Cybersecurity Unit and the Consumer Technology Association advising IoT device owners on practices to institute when using most internet-connected devices, details the risks as follows:

> In recent years, the dramatic growth of Internet-connected devices has transformed how people, households, and businesses interact with each other and the physical world. Connected devices as diverse as security cameras, digital video recorders, printers,

---

[1] Jacob Morgan, Forbes, "A Simple Explanation of 'The Internet Of Things'", *Forbes*, May 13, 2014, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ [as of Apr. 16, 2022].)

[2] Juniper Research, "IoT Connections to Reach 83 Billion by 2024, Driven by Maturing Industrial Use Cases," *Press Release*, Mar. 31, 2020, https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024 [as of Apr. 16, 2022].

wearable devices, "smart" lightbulbs, and Internet connected-appliances have come to be collectively known as the "Internet of Things" ("IoT"). IoT devices represent a growing constellation of gadgets and tools designed to collect, exchange, and process information over the Internet to furnish their users with convenient access to an array of services and information.

Unfortunately, IoT devices have also become an increasingly attractive target for criminals. To attack IoT devices, cyber criminals often probe the devices for security vulnerabilities and then install malicious software ("malware") to surreptitiously control the device, damage the device, gain unauthorized access to the data on the device, and/or otherwise affect the device's operation without permission. Installed malware may not only compromise the operation and information security of the infected IoT device, but can also provide hackers a conduit for penetrating other electronic devices on the same network. Unless appropriate precautions are taken, malware can quickly spread across networks of IoT devices without a user opening a file, clicking on a link, or doing anything other than turning on an Internet-connected device.

Although malware has existed for many years, the burgeoning popularity of IoT devices has significantly increased the number of Internet-accessible targets that may be exploited; the advent of a new generation of malware dedicated to exploiting IoT devices is largely to blame.[3]

In 2018, California took a significant step toward addressing the risks associated with security vulnerabilities in IoT devices by passing AB 1906 (Irwin, Ch. 860, Stats. 2018) and SB 327 (Jackson, Ch. 886, Stats. 2018), identical bills with contingent enactment language, which required manufacturers of connected devices to equip those devices with reasonable security features to protect the device and information therein from unauthorized access, destruction, use, modification, or disclosure. Specifically, these bills established a requirement that manufacturers of connected devices sold in California equip those devices with "a reasonable security feature or features" that fit all of the following criteria: 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.

Those bills specified that "subject to all of the requirements" above, a connected device equipped with a preprogrammed password that is unique to each device, or a security feature that requires a user to generate a new means of authentication before accesses is granted to the device for the first time, shall be deemed to be equipped with a reasonable security feature under the specifications above (*see* Comment 5). However, the bills did not further specify what those reasonable security features might look like, nor how they should be implemented.

Though this supply-side approach to IoT cybersecurity requires consideration of cybersecurity in the design of IoT devices, many vulnerabilities are not identified until after these devices enter the market. Depending on how the devices are being used at the time a vulnerability is exploited, the costs of overlooking such security weaknesses can be dire. This bill seeks to provide additional clarity on possible avenues for compliance with existing

---

[3] "Securing Your 'Internet of Things' Devices," *U.S. DOJ Cybersecurity Unit*, Jul. 2017.

requirements to equip connected devices with "reasonable security features." The bill's inclusion of a required third-party conformity assessment if a manufacturer elects to satisfy the requirement through the avenue provided by the bill seems prudent to ensure that the efficacy of a device's security features is inspected prior to sale.

4) **Federal E.O. 14028 and NIST criteria for cybersecurity labeling of IoT products**: In May 2021, President Biden issued an Executive Order on "Improving the Nation's Cybersecurity" (E.O. 14028) directing the National Institute of Standards and Technology (NIST) to develop cybersecurity criteria and labeling approaches for consumer software and IoT products, and to initiate pilot programs based on those criteria. The intention behind this order was to provide a mechanism by which businesses are incentivized to develop security by design in their connected products, and to allow consumers to quickly evaluate cybersecurity fitness (without the need for in-depth technological expertise) in their purchasing decisions. NIST satisfied these requirements in a white paper published on February 4, 2022 entitled "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products." The paper laid out several detailed criteria to which a labeling scheme should conform, and particular cybersecurity considerations that a labeling scheme should assess in order to determine approval. According to the paper's introduction:

> NIST proposes an approach and key considerations to be taken into account in a consumer IoT product cybersecurity labeling program, including proposed baseline product criteria as well as labeling and conformity assessment considerations. **NIST will identify key elements of labeling program** [*sic.*] **in terms of minimum requirements and desirable attributes – rather than establishing its own program; it will specify desired outcomes, allowing providers and customers to choose best solutions for their devices and environments.** One size will not fit all, and multiple solutions might be offered by label providers. [] Nevertheless, NIST has concluded that multiple variations of labeling approaches likely would cause confusion among consumers and limit the effectiveness of such efforts. It is critical that labeling criteria and the labels themselves be consistent across products and labeling program offerings.

The criteria identified by NIST consist of all of the following, with additional detail provided in sub-criteria and justifications of the "cybersecurity utility" served by each criterion:

- Asset identification: the IoT product is uniquely identifiable and inventories all of the IoT product's components.

- Product configuration: the configuration of the IoT product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other IoT product components.

- Data protection: the IoT product and its components protect data stored (across all IoT product components) and transmitted (both between IoT product components and outside the IoT product) from unauthorized access, disclosure, and modification.

- Interface access control: the IoT product and its components restrict logical access to local and network interfaces – and to protocols and services used by those interfaces – to only authorized individuals, services, and IoT product components.

- Software update: the software of all IoT product components can be updated by authorized individuals, services, and other IoT product components only by using a secure and configurable mechanism, as appropriate for each IoT product component.

- Cybersecurity state awareness: the IoT product supports detection of cybersecurity incidents affecting or affected by IoT product components and the data they store and transmit.

- Documentation: the IoT product developer creates, gathers, and stores information relevant to cybersecurity of the IoT product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.

- Information and query reception: the ability of the IoT product developer to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.

- Information dissemination: the IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the IoT product ecosystem) information relevant to cybersecurity.

- Product education and awareness: the IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

As NIST points out, these criteria are general outcome objectives rather than prescriptive of particular mechanisms for achieving those ends. With respect to this approach, NIST explains:

> Considering the heterogeneity of consumer IoT products, components, use cases, risks, and mitigations, the criteria outlined [] are not prescriptive with respect to how they would be achieved. Rather, they are stated in such a way that resources such as standards or conformity assessment approaches can be used to build a program that demonstrates support for the recommended outcomes. This approach offers multiple benefits:
>
> - Flexibility in meeting the criteria to support different IoT products (e.g. component combinations) cybersecurity (e.g. ways to satisfy the criteria) approaches, which allows for a robust cybersecurity marketplace and ecosystem that can meet disparate needs and contexts.
>
> - Easy adaptability as technologies and risks change over time. Outcome oriented criteria enable those changes rather than specifying current solutions. This allows cybersecurity solutions and mitigations to be upgraded and changed over time without significant changes in the product criteria for labeling.
>
> - Outcomes speak directly to the risks they are intended to mitigate, which can help guide a developer or conformity assessor in determining the applicability of criteria to a specific IoT product or its components.

AB 2392 would provide that a connected device manufacturer may satisfy the "reasonable security feature" requirement if the connected device does all of the following: 1) meets or exceeds the baseline product criteria of a NIST conforming labeling scheme; 2) satisfies a conformity assessment as described by a NIST conforming labeling scheme that includes a third-party test, inspection, or certification; and 3) bears the binary label as described by a NIST conforming labeling scheme. The bill 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."

The Association of Home Appliance Manufacturers (AHAM), who have taken a "support if amended" position on the bill, express support for this approach:

> We were supporters of this approach when it was discussed and rejected as part of AB 1906/SB 327 in 2018. The reason for our support then and now is because the standards process is where cybersecurity is best addressed so that it can be more adaptive and nimble as cybersecurity protocols continually evolve. As stated during the deliberation of AB 1906/SB 327 in 2018, AHAM favors national standards in this area to ensure input from diverse stakeholders and to avoid the ambiguity and inefficiency that would result from a patchwork of differing state laws or the ambiguity of "reasonable security features" that can be enforced by the state or each locality in California in a number of different ways. We are glad to see it now moving forward.

NIST is a well-respected body for promulgating technological standards, and the conformity requirements laid out in the white paper seem consistent with best practices in cybersecurity as it pertains to product development. While no NIST conforming labeling schemes currently exist, the author contends that the bill is permissive, suggesting that satisfying the requirements of the scheme is just one way among others to conform to the "reasonable security feature" requirements in existing law. Generally speaking, this bill could provide an incentive for either an agency or a private organization in California to establish a NIST conforming labeling scheme, and provides some clarity in what is envisioned by the existing requirement for "reasonable security features."

5) **Bill could benefit from clarification in several ways**: This bill is likely to provide additional clarity for manufacturers of connected devices as they seek to determine how to comply with the "reasonable security feature" requirement under existing law. That said, the particular language of several provisions of the bill introduces ambiguity, clarification of which could significantly benefit the bill's capacity to achieve the author's intent.

   Required vs. permissive: The author has indicated that the intent of the bill is make compliance with a NIST conforming labeling scheme permissive as an approach to equipping reasonable security features. However, the language could seemingly be interpreted to indicate that this is one among many ways in which a manufacturer can satisfy the requirement, as the author alleged to intend, or that this is the sole way to do so. The bill in print reads "A manufacturer of a connected device *satisfies* the requirements of subdivision (a) if […]". This is clear in indicating that a manufacturer of a device that meets all of the criteria is deemed to be in compliance with the "reasonable security feature" law, but is not

clear with respect to whether the inverse is true, i.e. that a manufacturer does *not* satisfy the requirements of subdivision (a) if its product does *not* meet all of the specified criteria.

At the time of writing, no NIST conforming labeling schemes have yet been established in the United States, let alone California. As such, should the provisions of the bill be interpreted as necessary rather than sufficient for complying with existing law, compliance with that law would be impossible. To avoid this problematic outcome, as the bill moves through the legislative process, the author may wish to consider clarifying that "a manufacturer of a connected device *may* satisfy the requirements of subdivision (a) *by ensuring* the connected device […]".

In their "support if amended" letter, AHAM point out this ambiguity:

> AB 2392 is unclear and could be interpreted that a NIST label is required. Our interpretation, and on what our possible support for this bill is contingent, is that manufacturers would not be required to institute labeling, but would just need to conform to the NIST guidelines in the Whitepaper. We ask that the bill be amended to make clear that labeling would not be required following the finalization of the labeling scheme. If manufacturers would be required to use a new label, we would oppose this requirement because manufacturers should have flexibility in how they certify standards and what certification programs they use, including self-certification.

AHAM's comment raises the additional question of whether the bill implies that meeting or exceeding the baseline product criteria of a NIST conforming labeling scheme alone is not sufficient to satisfy the "reasonable security feature" law. Because the bill requires that the connected device satisfy *all* of the criteria (i.e. meeting or exceeding the NIST criteria, satisfying a conformity assessment, *and* bearing a binary label), it seems to suggest that even if a device possesses all of the features necessary to meet or exceed the baseline product criteria of a NIST conforming labeling scheme, it has not yet satisfied the requirements of the "reasonable security feature" law unless it also undergoes a conformity assessment, is approved by the labeling scheme, and displays the label indicating as such. Notably, existing law requires no independent verification of security features by a third party, and as such, many devices may meet or exceed NIST conforming labeling scheme criteria already, without that verification. In these cases, it is not clear whether the devices could be deemed in compliance with the existing law. While requiring third party verification could arguably be beneficial, it does not seem consistent with the author's intent. To clarify that satisfying a conformity assessment and bearing the binary label are ways of *verifying* compliance, rather than of *establishing* compliance, as the bill moves through the legislative process, the author may wish to consider amending the bill to provide that meeting or exceeding the baseline product criteria of a NIST conforming labeling scheme alone is sufficient to satisfy existing law, and that satisfaction of a conformity assessment and bearing the label serve as a defense against liability under the "reasonable security feature" law.

<u>*Limitations in scope of bill and existing law*</u>: Consumer Reports, which opposes the bill unless amended, raises several shortcomings in the existing "reasonable security feature" law, and one issue in the bill in print, that they hope to see resolved, arguing:

> 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 [NIST] labeling framework – compounding the problems with 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. […]

The author of this bill (and of AB 1906) contends that the language in existing law was intentionally drafted so as to *not* constitute a safe harbor and rather to serve as an augmentation or clarification of the existing provisions, but the language is arguably unclear. Because the inclusion of password protection is preceded by "Subject to all of the requirements of subdivision (a)," it could reasonably be read to only constitutes satisfaction of the requirements in subdivision (a), i.e. the existing "reasonable security feature" law, if it already meets those criteria. This somewhat recursive interpretation, that a manufacturer satisfies subdivision (a) if it both satisfies subdivision (a) and an additional requirement, results in significant uncertainty with respect to the function of that provision. That said, those provisions arguably fall outside the scope of this bill as it is in print.

Germane to the text of this bill, however, is the argument raised by Consumer Reports that the bill does not allow for updates to the NIST document. The bill defines "NIST conforming labeling scheme" to mean a labeling scheme conforming to the Cybersecurity White Paper titled 'Recommended Criteria for Cybersecurity Labeling for Consumer [IoT] Products" published by [NIST] *on February 4, 2022*." By specifying this exact document, the bill arguably creates ambiguity as to whether compliance with a labeling scheme based on a revision of the document or successor publication would be sufficient to satisfy "reasonable security feature" requirements. While the NIST criteria are intended to be technology neutral, and accordingly maintain some resilience against obsolescence, the possibility that changes in technology or experts' understanding of best cybersecurity practices requires an update to this document may render this rigidity problematic. To protect against this possibility, as the bill moves through the legislative process, the author may wish to consider amending the bill to include in the definition of "NIST conforming labeling scheme" the document published on February 4, 2022, *or revisions or successor publications* to that document.

Finally, Consumer Reports raises concerns that both existing law, and by extension, this bill, define "connected device" too narrowly. For the purposes of the "reasonable security feature" law, "connected device" is defined to mean any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, that is assigned an Internet Protocol address or Bluetooth Address. Consumer Reports argues:

> All connected devices should be covered by a data security requirement. Existing law is currently limited to devices with IP addresses and Bluetooth, but there are a wide variety of protocols that should be covered, especially as smart home devices often run on these other protocols. IoT Times lists several, including ZigBee; other lists are even more extensive. Researchers were able to hack into devices running on ZigBee protocol; white-hat hackers were able to break into Z-Wave devices. Moreover, carving out these various protocols will incentivize manufacturers to use these unregulated protocols, making devices even less secure.

Beyond the limitation in covered protocols, there also exists an asymmetry between this definition of "connected device," and the way in which the NIST criteria consider IoT products. Connected device as defined refers only to the physical device itself, whereas the NIST criteria are intended to apply to the physical device and all other components of the device's operation. As the NIST document explains:

> In the context of these labeling recommendations, an IoT product is defined as an IoT device and any additional product components that are necessary to use the IoT device beyond its basic operational features. For example, an unconnected smart lightbulb may still illuminate in one color, but its smart features, such as color changes, cannot be used without other product components. […]
>
> Product criteria are recommended to apply to the IoT product overall, as well as to each individual IoT product component (e.g., IoT device, backend, companion app), as appropriate.

Because the definition of IoT product does not correspond to the limited definition of connected device applicable to this bill, it is not entirely clear whether all components of the IoT product must conform to the criteria to satisfy the "reasonable security feature" law, or whether only the physical device itself must, as the narrow definition of connected device would imply. Should the bill pass out of this Committee, the author may consider addressing this asymmetry.

Despite these ambiguities, this bill seems to be a significant step forward in better defining scope of the existing law requiring connected devices to be equipped with reasonable security features. Whether or not a manufacturer elects to comply through adoption of a NIST labeling scheme, the ability to compare the security features included in a manufacturer's device against the NIST labeling scheme criteria should provide crucial clarity to manufacturers as to how they can best comply with the law.

6) Related legislation: AB 2135 (Irwin, 2022) would require state agencies that do not fall under the direct authority of the Governor to adopt and implement certain information security and privacy policies, standards, and procedures meeting specified federally-established criteria, and would require those agencies to perform a comprehensive independent security assessment (ISA) every two years for which they may contract with the Military Department or a qualified responsible vendor.

AB 2190 (Irwin, 2022) would enact a recommendation from the State Auditor's 2022 report to require that the Department of Technology (CDT) confidentially submit an annual statewide information security status report, including specified information, to the Chair of the Assembly Committee on Privacy & Consumer Protection no later than January 2023.

AB 581 (Irwin, 2021) would require all state agencies to review and implement guidelines published by NIST, or derived therefrom, for reporting, coordinating, publishing, and receiving information about security vulnerabilities of state IT systems and resolving those vulnerabilities.

AB 1262 (Cunningham, 2021) would establish limitations on the use, retention, sharing, and sale of recordings or transcriptions containing personal information collected by the voice recognition feature of a smart speaker device, and would prohibit a person or entity from

providing the operation of a voice recognition feature without prominently informing the user during the initial setup of a smart speaker device.

7) Prior legislation: AB 2564 (Chau, 2020) stated the intent of the Legislature to enact legislation to improve the security of information technology systems and connected devices by requiring public agencies and businesses to develop security vulnerability disclosure policies. This bill was never referred to a committee, and died at the Desk.

AB 1987 (Gonzalez, 2020) would have allowed a party to request that a court, as part of a domestic violence protective order, prohibit another party from remotely controlling any connected devices in the home of the protected party. This bill did not receive a hearing in the Assembly Committee on Privacy & Consumer Protection due to constraints on the legislative process imposed by the COVID-19 pandemic.

AB 455 (Kiley, 2019) was substantially similar to AB 1987. This bill died in the Assembly Committee on the Judiciary.

AB 1906 (Irwin, Ch. 860, Stats. 2018) *See* Comment 3.

SB 327 (Jackson, Ch. 886, Stats. 2018) *See* Comment 3.

AB 1116 (Committee on Privacy and Consumer Protection, Ch. 524, Stats. 2015) prohibits a person or entity from providing the operation of a voice recognition feature without first prominently informing either the user or the person designated by the user to perform the initial setup or installation of a connected television.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

Consumer Reports (unless amended)

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200