CommonSenseMedia_FAV_SB443
Uploaded by: Jerome, Joseph
Position: FAV

common sense kids action™

February 19, 2020

The Honorable Delores G. Kelley, Chair
Senate Finance Committee Members
3 East
Miller Senate Office Building
Annapolis, MD 21401

RE: SB443, Security Features for Connected Devices—SUPPORT

Dear Chair Kelley and Members of the Committee:

Thank you for considering SB443, which would mandate security features for connected devices.

Common Sense is a national organization representing kids, parents, and educators that is dedicated to helping kids and families thrive online and on social media. We are particularly concerned with the spread of insecure and unsafe connected devices and toys sold to kids and families across the country.

While Maryland has existing data security protections as part of its data breach notification rules, these rules apply only to certain categories of personal information whose unauthorized disclosure would trigger a breach notification. Specifically, existing law applies to an individual's first name or first initial and last name in combination with one of six data elements like Social Security numbers or driver's license number. In other words, the vast majority of data exhaust created by devices and so-called "Internet of Things" devices is not protected under the law.

The threat is acute. In 2017, the FBI warned that smart toys threaten children's privacy and put them at risk for child identity theft and inappropriate contacts. Last Christmas, hackers used Ring surveillance cameras to look into and listen inside homes and even talk with children.

Many of the most popular connected products target families. For instance, 800,000 Spiral Toys & Cloud Pets were compromised, alongside 2 million voice recordings of families. A so-called smart toaster was hacked within minutes of being installed. Thousands of ordinary devices in American homes made into a botnet to attack parts of the internet. The German government declared the "My Friend Cayla" doll unsafe due to security lapses.

SB443 begins to address this by requiring manufacturers to equip their devices with reasonable security features appropriate to the nature of the device. This simple standard will protect families in Maryland from manufacturers who continue to cut corners on basic security features for smart connected products. Requiring "reasonable security standards" is a flexible standard that allows

companies to tailor their security features and protections in a fashion that will best help consumers and families of connected products.

works to protect Maryland families from security and privacy harms caused by connected devices that are unregulated and unsafe by requiring manufacturers to equip their devices with reasonable security features appropriate to the nature of the device. This simple standard will protect families in Maryland from manufacturers who continue to cut corners on basic security features for smart connected products.

Self-regulation and best practices have been insufficient to improve the security of connected devices. Legislation is needed, and SB443 is a positive first step. Common Sense is eager to work with members of this committee to advance this bill, and please do not hesitate to reach out with any questions to 563.940.3296 or via email at jerome@commonsense.org

Sincerely,
Joseph Jerome
Multistate Policy Director

Aviel Rubin_FAV_SB443
Uploaded by: Rubin, Aviel
Position: FAV

SUPPORT

Aviel D. Rubin
Professor, Computer Science
Technical Director of the Information Security Institute
Johns Hopkins University

Testimony in Support of

SB 443 Consumer Protection - Security Features for Connected Devices
Primary Sponsor: Senator Susan Lee

Senate Finance Committee, 19 February 2020

Chairwoman Kelly, Vice Chairman Feldman, and members of the Committee, thank you for the opportunity to speak before you today on behalf of SB 443 pertaining to security features of connected devices.

My name is Avi Rubin, and I am a full professor of Computer Science at Johns Hopkins University and Technical Director of our Information Security Institute. I am also the Founder and Chief Scientist of Harbor Labs, a Maryland CyberSecurity company that has developed an IoT Security Analysis product. I have been an active researcher in the area of Computer and Network Security since 1992. The primary focus of my research is Security for the Internet of Things (IoT Security). These are the types of connected devices that are addressed in SB 443.

We have entered the era of Smart Things where everyday objects are imbued with computational capabilities and the ability to communicate with each other and with services across the Internet. In fact, the Internet of Things involves the deployment of Smart Things in everyday living environments -- homes, offices, cars, shops, schools, clinics, and more -- resulting in Smart Environments.

According to Gartner, there will be 20.4 Billion IoT Devices online by 2020, and companies will invest $15 Trillion in IoT between 2017 and 2025 (See https://www.vxchnge.com/blog/iot-statistics).

These connected devices offer many potential benefits to the owners of the Smart Environments (more efficient use of energy, for example) or to the occupants of the Smart Environments (personalized services, ready access to information, improved fitness, health and wellness).

However, if these connected devices are not designed, deployed, configured, or managed properly, they can create unsafe conditions and increase risk of harm to persons and property.

In preparation for this testimony, I visited the popular web site Tech Republic for some examples that illustrate a few recent examples of attacks against IoT connected devices. Here are 5 highlights of IoT security failures from Tech Republic in 2018 that give an idea of the magnitude of the risks: (I should point out that even a quick Google search would yield dozens more of these):

1. SirenJack, https://www.sirenjack.com/

   Attacks against public warning systems causing false alarms and distrust of public warning sirens, as well as disruption of daily life. E.g. 150 false tornado warnings in Dallas in 2017.

2. LoJack, https://www.techrepublic.com/article/beware-of-russian-attackers-impersonating-lojack-security-software-to-hack-computers/

Allowed the Russian state sponsored hackers known as “Fancy Bear” to take control of remote machines, ironically exploiting an anti-theft software feature.

3. State Actors hiding malware in routers (VPNFilter): https://www.techrepublic.com/article/vpnfilter-malware-infected-500k-devices-smb-and-home-office-routers-are-at-risk/

   Cisco reported finding 500,000 compromised devices across 54 countries. Compromised devices manufactured by ASUS, D-Link, Linksys, Netgear, and all of the other major manufacturers. The malware included data exfiltration, command execution, file collection, and command and control botnet code.

4. Data Firm LocationSmart leaked cell phone data. https://www.techrepublic.com/article/phone-tracking-service-locationsmart-exposed-api-allowing-free-tracking/

   Vulnerability in a product demo allowed attacker to locate any mobile phone based on its phone number without requiring a password.

5. Amazon Echo recorded and sent conversation. https://www.techrepublic.com/article/no-alexa-isnt-spying-on-you-but-be-careful-with-sensitive-conversations/

   An Amazon Echo accidentally randomly recorded conversations and sent the recordings to someone in the owner’s contact list.

In another well-known example, the Mirai botnet used insecure default passwords on IoT devices, in particular, CCTV cameras, to bring down much of the Internet on the East Coast in 2016 by attacking a DNS service on the Internet with a denial of service attack.

These are just examples of some of the many vulnerabilities that exist today due to the widespread and rapid adoption of IoT. It is imperative to take steps wherever possible to curtail the risks, and this bill, while it may not go far enough, is a great first step in the right direction.

Based on my experience working in the security of connected devices, I strongly support SB 443 because it addresses the concerns that I have raised earlier in this testimony and is consistent with my belief that devices are most vulnerable when they are first connected to a network. By requiring authentication, we can eliminate some of the most persistent threats.

To the members of this committee, thank you once again for the opportunity to give testimony here today.

I encourage a favorable report of SB 443. Thank you for your consideration.

CPD_FAV_SB443
Uploaded by: Sakamoto-Wengel, Steve
Position: FAV

BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

(410) 576-6566 (F)

WRITER'S DIRECT DIAL NO.

(410) 576-6307

February 19, 2020

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Steven M. Sakamoto-Wengel
Consumer Protection Counsel for Regulation, Legislation and Policy

RE: Senate Bill 443 – Consumer Protection -- Security Features for Connected Devices (SUPPORT)

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 433, sponsored by Senators Lee, Patterson and Rosapepe, which would take a meaningful first step in protecting us from unsecured internet-connected devices that are collecting sensitive information about us. The Consumer Protection Division has a long-standing commitment to promoting data security.

Marylanders are welcoming large numbers of connected devices into our lives. We have internet-connected smart speakers, thermostats, refrigerators, televisions, cars, children's toys, and even home security systems with cameras recording inside our homes. Some of that is good – technology should make our lives easier.

However, the security of these devices has lagged behind the innovation. Currently, there are no clear rules governing the security features that manufacturers of these products must include[1] before they place these devices into commerce and into our homes. A large number of these devices have fatally-flawed password protection. Some connected device manufacturers set the same default password for all of their devices, and do not force consumers to change it. For example, imagine 100,000 internet-connected children's dolls being sold, each with a preset password of "12345" or "password." Once that is discovered, either by being easily guessed, or by someone who buys the doll, all 100,000 are accessible. Worse yet, in many other connected devices, these default credentials are hardcoded into the device's firmware. In that situation, a consumer is able to use the device without ever being asked to create or enter a username or password, and the vulnerability can only be fixed by recalling the product.

[1] California and Oregon have passed laws, which are similar to this bill. *See* California Senate Bill 327 Information Privacy: Connected Devices (2017-2018), and Oregon House Bill 2395 (effective January 1, 2020).

The consequences of a connected device getting hacked and controlled can be significant. A vulnerable device can serve as an access point to the rest of a consumer's home network, putting their broader security and physical safety at risk. Certain devices, like medical devices and cars, present the risk of ransomware attacks (e.g., pay us $250 if you want to start your car). Other devices can be targeted for the personal information that they hold, such as children's toys that hold recordings of the children or home alarm systems that track your patterns of activity.

This bill provides useful guidance. It requires manufacturers to equip their devices with a reasonable security feature, and allows them to accomplish that by simply either: (1) giving each device a unique password, or (2) requiring the user to set up their own password before they are able to use the device. Any responsible manufacturer is already complying with this requirement (for example, manufacturers of computers or smart phones will not have to change their practices). Yet because many manufacturers are not, this bill is necessary.

Existing law is inadequate to cover this, as our privacy laws focus on protecting specific categories of information once it has been collected. This bill adds protection to the data-collecting devices prior to their gathering our sensitive personal information. With the wave of these devices being thrust into commerce, this step should be taken now, before more of our data is exposed by unsecured devices.

The Division respectfully requests that the Senate Finance Committee give Senate Bill 433 a favorable report.

Lee_FAV_SB443
Uploaded by: Senator Lee, Senator Lee
Position: FAV

SUSAN C. LEE
Legislative District 16
Montgomery County

MAJORITY WHIP

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair Emeritus
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

February 19, 2020

Senate Finance Committee

Senate Bill 443 – Consumer Protection – Security Features for Connected Devices

Senate Bill 443 codifies existing federal guidelines under the unfair trade practices section of the commercial law article, as a recommendation of the Maryland Cybersecurity Council. I introduced a similar bill last year, but we have refined the bill to fit within existing Maryland consumer protections. Existing guidelines from the Federal Communications Commission recommend that the manufacturer of an internet connected device create a "reasonable security feature" for that device. Within that guidance, this bill clarifies that adopting a unique code for each device is a reasonable security feature to satisfy the policy intent of the FCC guidance. This legislation is also very similar to a law that passed in California in 2018, and went into effect this year. Similar legislation been enacted in Oregon and has recently been proposed in Illinois as well as by our neighbors in Virginia.

In other words, this bill simply codifies the best practices for cybersecurity protections for connected devices. Internet of Things (IoT) connected devices are simply physical objects capable of connecting to the internet. Most of these items are in our homes, like our televisions, refrigerators, home security systems, and washer-driers. These systems, protected only with a default password or other meager security device, can easily be hacked, weaponized and otherwise sabotaged.

As the fiscal note provides, the Consumer Protection Division remains responsible for enforcing and investigating consumer complaints. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. This is at the discretion of the Office of Attorney General. A merchant who violates MCPA is subject to a fine of up to $10,000 for each violation and up to $25,000 for each repetition of the same violation.

We've gotten some pushback from industry who want to see us explicitly exempt devices from MD regulation that are already regulated by federal rules. We think that's redundant, since the federal rules with contrary policy intent would already preempt state action in the space, but we're happy to clarify that with explicit language in our bill. That amendment is currently being prepared and we will provide it to committee counsel this week.

This legislation may seem to foresee futuristic problems, but the problems it aims to contain already exist, and we cannot hesitate or wait for the private sector to perfect their standards on their own. This proposed measure is an important function of state government in the 21st century. Denial of services attacks are just the beginning. There are implications with domestic violence, stalking, government overreach and the unknown. Our laws must try to keep pace with technology. Or the problems that technology creates will overtake our liberties and the means to get them back.

For this reason, I ask for a favorable report on SB 443, as amended.

CTIA_UNF_SB443
Uploaded by: Keegan, Gerard
Position: UNF

Testimony of
GERARD KEEGAN
CTIA

In Opposition to Maryland Senate Bill 443

Before the
Maryland Senate Finance Committee

February 19, 2020

Chair, Vice-Chair, and members of the committee, on behalf of CTIA®, the trade association for the wireless communication industry, I submit this testimony in opposition to Senate Bill 443, which would mandate that connected device manufacturers equip those devices with certain features. This bill is unnecessary in light of the wireless industry introducing CTIA's Internet of Things (IoT) Cybersecurity Certification program that protects consumers and wireless infrastructure nationally, while also creating a more secure foundation for smart cities, connected cars, mHealth and other IoT applications. The program is the first of its kind to be developed in collaboration with the nationwide wireless providers.

CTIA announced the IoT Cybersecurity Certification program in August 2018 and began accepting applications in October 2018. Leading wireless providers, technology companies, security experts, and test labs collaborated to develop the program's test requirements and plans. The program builds upon IoT security recommendations from the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST).

The program accepts all IoT devices that connect to a cellular network and validates whether they meet a set of security features. Device manufacturers may seek one of three types of certification, depending on the sophistication of the device and the security characteristics desired or needed for its use.

For more than 25 years, CTIA's Certification Working Groups have developed and managed

product test plans and certification requirements for devices, networks, and other wireless technologies, with over 70,000 certification requests handled to date by over 100 CTIA Authorized Test Labs. These programs ensure interoperability between wireless devices and networks, as well as set standards for a secure, high-performing, and innovative wireless ecosystem.

These types of industry programs are preferred to legislative mandates, such as SB 443, as they provide the industry the flexibility to quickly respond to changes on the cybersecurity front. This flexibility is vitally important to address any security concerns that may arise in a quickly changing field. For these reasons, CTIA respectfully asks that you not move SB 443.

Alliance_Auto_Innovation_UNF_SB 443
Uploaded by: Kress, Bill
Position: UNF

February 19, 2020

The Honorable Delores Kelley
Chair, Senate Finance Committee
3 East, Miller Senate Office Building
Annapolis, Maryland 21401

RE: SB 443 - SECURITY FEATURE FOR CONNECTED DEVICES - OPPOSE

Dear Senator Kelley:

The Alliance for Automotive Innovation[1] (Auto Innovators) is writing to inform you of **our opposition to SB 443**, which requires manufactures of connected devices to equip the connected device with certain security features.

SB 443 is similar to legislation passed in California. Like the California legislation, SB 443 imposes vague and open-ended requirements that will require manufacturers to grapple with its interpretation when designing product security features.

However, SB 443 lacks a critical exemption included in California's legislation. California's law states that its provisions do not apply to a device "the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority." Automobiles fall under this exemption because they are already covered by cybersecurity best practice guidance published by the National Highway Traffic Safety Administration.[2] Additionally, the auto industry has taken proactive measures to protect consumer privacy by developing the automotive "Privacy Principles" which commit automakers to take certain steps to protect the personal data generated by their vehicles.[3] The Principles' fundamentals are based on the Federal Trade

---

[1] Formed in 2020, the Alliance for Automotive Innovation is the singular, authoritative and respected voice of the automotive industry. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents the manufacturers producing nearly 99 percent of cars and light trucks sold in the U.S. The newly established organization, a combination of the Association of Global Automakers and the Alliance of Automobile Manufacturers, is directly involved in regulatory and policy matters impacting the light-duty vehicle market across the country. Members include motor vehicle manufacturers, original equipment suppliers, technology and other automotive-related companies and trade associations. The Alliance for Automotive Innovation is headquartered in Washington, DC, with offices in Detroit, MI and Sacramento, CA. For more information, visit our website http://www.autosinnovate.org.

[2] https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[3] https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf

1050 K Street, NW
Suite 650
Washington, DC 20001

AutosInnovate.org

Commission's (FTC) Fair Information Practice Principles (FIPPs), which, in turn, rest on privacy practice frameworks used in the United States and around the world for over forty years. These Privacy Principles have been expressly adopted by the vast majority of the auto industry and are enforceable by the Federal Trade Commission (FTC).

Additionally, given action at the federal level, SB 443 is not necessary to protect consumers in Maryland. For example, the FTC, which has broad authority over consumer product safety under section 5 of the FTC Act, issued the Internet of Things Privacy & Security in a Connected World guidance document in 2015. The FTC has also taken enforcement action against connected device manufacturers, thus developing a set of regulatory expectations for manufacturers with respect to cybersecurity. Similarly, the FTC and the National Highway Traffic Safety Administration (NHTSA) held a workshop on security and safety of autonomous vehicles in June 2017, in part to discuss developing standards.

While the California law has serious problems with its overbroad and vague language, the exemption noted above provides a crucial level of clarity for manufacturers which is missing in SB 443. At a minimum, SB 443 should be amended to include this same exemption.

Thank you for your consideration of the Auto Innovators' position. Please do not hesitate to contact me at jfisher@autosinnovate.org or 202-326-5562, should I be able to provide any additional information.

Sincerely,

Josh Fisher
Director, State Affairs

Richard Tabuteau_UNF_SB0443
Uploaded by: Tabuteau, Richard
Position: UNF

MARYLAND TECH COUNCIL

TO: The Honorable Delores G. Kelley, Chair
Members, Senate Finance Committee
The Honorable Susan C. Lee

FROM: Richard A. Tabuteau
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman

DATE: February 19, 2020

RE: **OPPOSE** – Senate Bill 443 – *Consumer Protection – Security Features for Connected Devices*

OPPOSE – Senate Bill 957 – *Maryland Online Consumer Protection Act*

The Maryland Tech Council (MTC) is a collaborative community, actively engaged in building stronger life science and technology companies by supporting the efforts of our individual members who are saving and improving lives through innovation. We support our member companies who are driving innovation through advocacy, education, workforce development, cost savings programs, and connecting entrepreneurial minds. The valuable resources we provide to our members help them reach their full potential making Maryland a global leader in the life sciences and technology industries. On behalf of MTC, we submit this letter of **opposition** for Senate Bill 443 and Senate Bill 957.

Senate Bill 443 requires a manufacturer of a "connected device" to equip the device with a reasonable "security feature". A connected device is considered to have a reasonable security feature if it is equipped with a means for authentication outside of a local area network that includes either a preprogrammed password that is unique to each connected device or a process that requires the user to generate a new means of authentication before the user is granted access for the first time. Senate Bill 957 requires businesses that collect a consumer's personal information to provide clear and conspicuous notices to the consumer at or before the point of collection. It requires a business to comply with a request for information within 45 days after receiving a verifiable consumer request.

Though MTC recognizes the importance of protecting online consumer data and providing certain security features for connected devices, the matters that Senate Bill 443 and Senate Bill 957 address should and must be resolved on the federal level. Meaningful consistent compliance by industry would be more reliably satisfied with a uniform nationwide solution. This bill would have the effect of imposing millions of dollars of compliance costs on tech businesses and would harm the State's economy more than it would protect consumer privacy. We understand that the tech industry is working with the Sponsor on amendments and are hopeful that consensus can be reached. However, as currently drafted, MTC urges an unfavorable report for Senate Bill 443 and Senate Bill 957.

For more information call:
Richard A. Tabuteau
Pamela Metz Kasemeyer
J. Steven Wise
Danna L. Kauffman
410-244-7000