CENTER FOR DEMOCRACY & TECHNOLOGY

Via e-mail to Christian Kurpiewski, Counsel, California Standing Committee on the Judiciary, at christian.kurpiewski@sen.ca.gov

Tuesday, May 2, 2017

The Honorable Hannah-Beth Jackson
Chair, Senate Judiciary Committee
1020 N Street, Room 2187
Sacramento, California 95814-1020

RE: Support for SB-327 Information Privacy: Connected Devices

Dear Chair Jackson:

The Center for Democracy & Technology is a nonprofit technology advocacy organization that works to advance digital rights for consumers through balanced technology policy, corporate policies, and technological tools. We support Senate Bill 327, which mandates certain security features and privacy disclosures for connected devices sold in California. The bill is a critical step towards imbuing Internet of Things (IoT) devices with reasonable privacy and security protections.

Internet connectivity in everyday consumer products has become commonplace. Today, products ranging from household appliances to children's toys collect and broadcast personal data. Though estimates vary widely, the number of devices constituting the IoT will likely exceed twenty billion worldwide by the end of the decade.[1] Many of these devices possess robust data collection and surveillance capabilities that defy consumer expectations and create security vulnerabilities that can be exploited by hackers.[2]

Last fall, numerous websites and online services were knocked offline for several hours by a distributed denial-of-service attack carried out by the Mirai botnet, malware which has ensnared more than 2.5 million IoT devices as of April 2017.[3] Recent ransomware attacks have locked hotel guests out of their rooms and shut off connected thermostats.[4] In the last six months alone, both connected toys and

---

[1] *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*, November 10, 2015, Gartner, http://www.gartner.com/newsroom/id/3165317.

[2] Comments of the Center for Democracy and Technology to the NTIA on Fostering the Advancement of the Internet of Things, March 14, 2017, *available at* https://cdt.org/insight/cdt-comments-to-the-ntia-on-fostering-the-advancement-of-the-internet-of-things/; *see also Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things*, January 14, 2016, Gartner, http://www.gartner.com/newsroom/id/3185623.

[3] Christiaan Beek et al., *McAfee Labs Threats Report April 2017*, April, 2017, McAfee Labs, https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf.

[4] Josephine Wolff, *The Ransomware Attack That Locked Hotel Guests Out of Their Rooms*, February 1, 2017, Slate, http://www.slate.com/articles/technology/future_tense/2017/02/the_ransomware_attack_that_locked_hotel_guests_out_of_their_rooms.html; Karl Bode, *Your 'Smart' Thermostat Is Now Vulnerable To Ransomware*, August 9,

intimate devices for adults have made headlines due to major problems with respect to consumer privacy and basic data management; the My Friend Cayla doll and the i-Que intelligent robot toy were found to be in violation of the federal Children's Online Privacy Protection Act (COPPA).[5] In March 2017, We Vibe settled a class action lawsuit for $3.7 million that accused the company of inappropriate data collection and sharing behaviors via its connected vibrators.[6]

These scenarios are not anomalies. They will continue to occur as long as there is a lack of sensible privacy and security protections for consumer devices in the IoT. As technologist Bruce Schneier has explained, connected devices are too often designed and built offshore, rebranded and resold at low cost to unsuspecting consumers without adequate consumer protections.[7] They lack critical security features and have immature data use and privacy practices. Consumers suffer the consequences.

The IoT industry faces a potential market failure because "smart" features and cost have been prioritized over security and privacy.[8] Sixty-two percent of consumers are worried about how the IoT will impact their privacy and fifty-four percent are worried about the security implications of connected devices.[9] Digital privacy concerns are increasingly inhibiting consumers' economic and other online activities; as the Federal Trade Commission has acknowledged, these concerns "permeate the IoT." Consumers want information and transparency into the data practices of connected devices.[10]

We believe SB 327 will encourage innovative solutions to the privacy and security concerns rampant in the IoT.

I. SB 327 Promotes Reasonable Security and Better Transparency in the IoT

SB 327 requires manufacturers of connected devices to deploy reasonable security measures, a provision that echoes existing law and data security enforcement. SB 327 also aims to provide transparency for Californians about the data practices of their connected devices by (1) mandating the

---

2016, TechDirt, https://www.techdirt.com/articles/20160808/07042735180/your-smart-thermostat-is-now-vulnerable-to-ransomware.shtml.

5 Complaint and Request for Investigation, Injunction, and Other Relief, In the Matter of Genesis Toys and Nuance Communications, (F.T.C. December 6, 2016), *available at* https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

6 Kimiko de Freytas-Tamura, *Maker of 'Smart' Vibrators Settles Data Collection Lawsuit for $3.75 Million*, March 14, 2017, New York Times, https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html?_r=0.

7 Schneier, Bruce. Statement to the House Committee on Energy and Commerce Subcommittee on Communications and Technology, and the Subcommittee on Commerce, Manufacturing, and Trade, *Understanding the Role of Connected Devices in Recent Cyber Attacks*, Hearing, November 16, 2016. Available at: http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-SchneierB-20161116.pdf (Accessed April 30, 2017).

8 *Id.*

9 Joao Lima, *Could consumer distrust kill IoT? Why calls for security, privacy and transparency should not be ignored*, April 12, 20016, Computer Business Review, http://www.cbronline.com/news/internet-of-things/consumer/could-consumer-distrust-kill-iot-why-calls-for-security-privacy-and-transparency-should-not-be-ignored-4859978.

10 *Id*.

inclusion of disclosure of how and when devices are collecting information through audio, visual or other means, and (2) by enhancing the disclosures and notices available to Californians at the point-of-sale for a device and prior to its purchase.

Improving the state of IoT security and advancing consumer education should be not be controversial, yet critics have been quick to assert that SB 327's provisions may harm innovation.[11] The proliferation of privacy and security incidents in the IoT, however, refute this argument. Market forces driving the adoption of more and more connectivity features have not been sufficient to encourage satisfactory privacy and security requirements. Measured legislative action, such as the provisions in SB 327, is a necessary and appropriate response to indifference by certain participants in the IoT and could, in fact, produce innovative solutions to privacy and security concerns across the IoT.

However, in order to mitigate undue burden on manufacturers, the bill could also include safe harbors for IoT manufacturers and vendors that participate in and publicly adopt standardized, meaningful industry practices. We also urge caution with respect to broad design mandates. While we believe it is incumbent upon IoT manufacturers and service providers to alert customers as to when devices are listening to them or otherwise capturing the content of their communications or sensitive information, we note that SB 327 requires broad notice and consent requirements prior to the collection of any information. With respect to data collection, we would support and recommend that SB 327 provide increased flexibility for manufacturers that wish to experiment with new methods of transparency and user control. For instance, Carnegie Mellon University's Personalized Privacy Assistant with IoT Infrastructure offers a potential model for offering better notice and control through a single mechanism.[12]

II. Preemption Concerns Are Exaggerated

Critics have also suggested that SB 327 is either duplicative of existing California privacy protections and/or may conflict with federal privacy regimes. The Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA), for example, protect personal health information held by covered entities and personal information from children under the age of thirteen, respectively. While both laws preempt state laws that are "inconsistent" with federal law, SB 327 does not appear to be inconsistent with the privacy and security protections afforded by these laws.

A. Children's Privacy Protections

COPPA requires operators to obtain consent for the collection and use of personal information for children under the age of thirteen, and it includes a limited preemption provision:

[11] Anne Hobson, *The Teddy Bear and Toaster Act Is Device Regulation Done Wrong*, April 19, 2017, TechDirt, https://www.techdirt.com/articles/20170418/12443837180/teddy-bear-toaster-act-is-device-regulation-done-wrong.shtml.
[12] *See Personalized Privacy Assistant Project*, Carnegie Mellon University, https://www.privacyassistant.org/iot (Accessed May 1, 2017).

> No State or local government may impose any liability . . . in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.[13]

As both the California Attorney General and the Federal Trade Commission have explained in complementary amicus briefs to the Ninth Circuit on the scope of COPPA preemption, COPPA contemplates a significant role for the states in protecting children's online privacy.[14] Moreover, when a federal statute expressly preempts only "inconsistent" state regulation, California law is only preempted where it might stand "as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[15] SB 327 would only be preempted if it established different requirements or directly conflicted with COPPA. Moreover, any preemption would not apply to general consumer products but only with respect to toys, devices, and connected products that are directed to children.

Further, COPPA already requires toy manufacturers provide clear privacy notices, obtain verifiable parental consent prior to collecting children's data, and put in place reasonable security measures.[16] As a matter of best practice, industry has also been instructed to provide notices at point-of-sale where appropriate, deploy flexible and creative forms of notice into toy design, and ensure meaningful choice mechanisms.[17] In our view, SB 327 is consistent with COPPA.

B. Health Information and Device Security

It is even less clear how SB 327 might be preempted by law protecting health information that applies to narrow classes of covered entities and their business associates. The U.S. Department of Health & Human Services (HHS) has explicitly stated that the HIPAA Privacy Rule provides only a floor of privacy protections.[18] Where state laws provide greater privacy protections or privacy rights, they are not generally preempted. The HIPAA Security Rule directs covered entities to implement reasonable security measures that take into consideration the organization's size, its operating infrastructure, the costs of

---

[13] 15 U.S. Code § 6502(d).

[14] Brief for Amicus Curiae Federal Trade Commission in Support of Neither Party, Jo Batman, et al. v. Facebook, Inc., (9th Cir. 2014), *available at* https://www.ftc.gov/system/files/documents/amicus_briefs/jo-batman-v.facebook-inc./140321batmanfacebookamicusbrief.pdf.

[15] Brief for the State of California as Amicus Curiae in Support of Neither Party, John Schachter, et. al v. Facebook, Inc., Case No. 13-16918, https://epic.org/amicus/facebook/fraley/Amicus-California.pdf, citing Metrophones Telecomm., Inc. v. Global Crossing Telecomm., Inc., 423 F.3d 1056 at 1073 (9th Cir. 2005).

[16] *Complying with COPPA: Frequently Asked Questions*, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Questions (Accessed May 1, 2017).

[17] KIDS & THE CONNECTED HOME: PRIVACY IN THE AGE OF CONNECTED DOLLS, TALKING DINOSAURS, AND BATTLING ROBOTS, December 2016, Future of Privacy Forum, https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf.

[18] Office of Civil Rights, *Does the HIPAA Privacy Rule preempt state laws?*, March 12, 2003, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html.

security measures, and the potential risks to protected health information – in other words, the same reasonable security test deployed by the Federal Trade Commission and referenced in SB 327.[19]

Further, HHS acknowledged last year that enforcement gaps exist in HIPAA, specifically with respect to protecting consumer privacy and security among wearable fitness trackers and other online health applications. "[C]onfusion persists," HHS reported, conceding that federal law and regulation has "not kept pace with these new technologies."[20]

III. Conclusion

SB 327 establishes much needed common sense protections for Californians' personal information. The privacy and security protections afforded by the IoT are in many respects contingent upon the practices of the worst actors. Californian's privacy and security over their information can be undermined by devices to which they are completely unaware – this has been termed the challenge of the "Internet of Other People's Things."[21] Ubiquitous connectivity have created market forces that cannot resolve this challenge, and the resulting information asymmetries demand additional privacy rights for Californians and new regulatory requirements on business actors eager to innovate in ways that ignore or undermine baseline privacy and security protections.

SB 327 may help tip the scales back in favor of consumers, and for this reason, CDT supports this important measure. Please contact us with any questions or to schedule a follow up discussion.

Sincerely,

Joseph Jerome
Policy Counsel

[19] Office of Civil Rights, *Summary of the HIPAA Security Rule*, U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/ (Accessed May 1, 2017).
[20] *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*, July 2016, U.S. Department of Health and Human Services, *available at* https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.
[21] *See* Chris Preimesberger, *Can We Secure the 'Internet of Other People's Things'?*, April 29, 2015, eWeek, http://www.eweek.com/security/can-we-secure-the-internet-of-other-people-s-things; Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 Idaho Law Review 639 (2015).