State Privacy and Security Coalition, Inc.

July 18, 2017

The Honorable Eric Lesser
24 Beacon St.
Room 413-C
Boston, MA 02133

The Honorable Joseph Wagner
24 Beacon St.
Room 42
Boston, MA 02133

Re: Technology Industry Concerns with S. 179, an Act Relative to the Cybersecurity of the Internet of Things and Other Smart Devices

Dear Chair Lesser and Chair Wagner,

On behalf of our combined memberships, we write to express concern with S. 179, legislation requiring the Office of Consumer Affairs and Business Regulation (OCABR) to adopt regulations relative to the cybersecurity of the Internet of Things (IOT) and other smart devices. We are concerned that S. 179 is overly broad, duplicative, and would likely have unintended consequences. We therefore would urge against further consideration of the bill.

The growth of the IOT brings with it significant concerns about both consumer privacy and security considering the vast amount of information these newly-connected devices will collect and transmit. However, we believe there are already mechanisms in place to appropriately regulate the industry, and thus we agree with the Federal Trade Commission's (FTC) conclusion in their 2015 IOT Report that "there is great potential for innovation in this area, and that IOT-specific legislation at this stage would be premature."[1] The IOT is evolving so quickly and unpredictably that any state-level, industry-specific legislation could have unintended consequences that hamper the growth of this still-nascent industry.

Numerous federal and state laws are already in place to protect the privacy and secure the data of Massachusetts consumers. These include the *Children's Online Privacy Protection Act (COPPA)*, the *Electronic Communications Privacy Act (ECPA),* the Controlling the Assault of Non-Solicited Pornography and Marketing Act (*CAN-SPAM)*, the Commonwealth's Data Breach Notification and Consumer Protection laws, and common law legal doctrines protecting privacy and data security. Given the

[1] Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World at vii (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (2015 FTC IOT Report).

protections afforded by these laws, added regulation by the OCABR on IOT privacy and security is unnecessary and duplicative.

This legislation is unnecessary as privacy protections regarding Internet-connected devices already exist and are enforced robustly by the FTC. The FTC has been the chief regulator for privacy and data security for decades, and its approach has been to use its authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices. This framework is the ideal way to regulate the IOT, as the FTC's technology-neutral case-by-case approach has proven an effective way to ensure companies implement strong data security and privacy protections without stifling innovation. Relying on Section 5's "unfair or deceptive practices" clause and providing guidance through enforcement, the FTC's approach allows it to adjust its enforcement approach as technology evolves and industry best practices change.

Our member companies take privacy and data security protections very seriously, and design their products with these considerations in mind. We agree with the FTC's recommendation that "companies should build security into their devices at the outset, rather than as an afterthought,"[2] by implementing a security by design process. An example of this so-called security by design principle in practice is the increased use of encryption technology by our member companies, consistent with FTC guidance.[3] Further, the FTC's 2012 Privacy Report recommended industry best practices for protecting the privacy of consumer data.[4] Companies should follow the FTC's guidance on both security by design and privacy best practices in designing their products to protect their customers' information, or else they could find themselves in violation of Section 5 and bereft of their customers' trust.

We appreciate your thoughtful consideration of our concerns. For the reasons outlined in this letter, we urge against further consideration of S. 179. Please consider our group of associations as resources as you deliberate on this issue.

Sincerely,

Kevin Callahan
Director, State Government Affairs – Northeast
CompTIA

Tom Hopcroft
President & CEO
Massachusetts Technology Leadership Council

Carl Szabo
Senior Policy Counsel
NetChoice

Tammy Cota
Executive Director
Internet Coalition

Dustin Brighton
Vice President, State Government Affairs
Internet Association

Matt Mincielli
Executive Director, Northeast Region
TechNet

---

[2] *Id*. at 44.
[3] Federal Trade Commission, Start with Security: A Guide for Business (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
[4] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-tradecommission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (2012 FTC Privacy Report).

Jim Halpert
General Counsel
State Privacy and Security Coalition

cc: Members of the Joint Committee on Economic Development and Emerging Technologies
The Honorable Eileen Donahue