Testimony of
Michelle Richardson, Deputy Director
Center for Democracy and Technology, Freedom, Security, and Technology Project

before the
House Energy and Commerce Committee,
Subcommittee on Digital Commerce and Consumer Protection

Internet of Things Legislation
May 22, 2018

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. We believe the Internet of Things (IoT) has the power to enrich people's lives. Connected devices can add convenience, efficiency, transparency, and control to simple, everyday activities from vacuuming one's house, to providing cutting edge advances in medicine, and everything in between.

CDT does, however, have continuing concerns about the security of IoT devices and the privacy of the information they collect and transmit. To that end, we regularly work with federal agencies like the National Institute of Standards and Technology (NIST), National Telecommunications and Information Administration (NTIA) and the Federal Trade Commission

(FTC) to develop voluntary standards or best practices that will improve privacy and security.[1] We additionally work with Congress on oversight activities and legislation.[2]

Summary

CDT has always recommended that the government take a soft touch in shaping technology and has endorsed the use of voluntary standards, especially relating to cybersecurity. We have also recognized that the government may have a legitimate role in overseeing sectors that pose a unique threat to safety or products that are unreasonably beyond accountability to consumers. The draft State of Modern Application, Research, and Trends of IoT Act (SMART IoT Act)[3] begins to compile the information necessary to evaluate whether these private sector and government efforts are sufficiently addressing the security of the IoT ecosystem. It is a question that Congress has the authority and responsibility to ask.

To that end, we believe the lists of industry standard-setting efforts and government oversight activities that would be created by this bill can help inform the Committee's oversight and legislative plans. Our statement below recommends amendments to the SMART IoT Act to ensure that the resulting report both returns meaningful information by which Congress can evaluate the state of the field and that the study does not discourage agencies from continuing with urgent cybersecurity efforts that are currently underway.

[1] See for example, CDT Comments to NTIA/NHTSA Connected Cars Workshop, July 31, 2017, at https://cdt.org/files/2017/08/2017-0731-2-ConnectedCarComments.pdf, CDT Comments to NTIA on The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (IoT), Mar. 10, 2017, at https://cdt.org/files/2017/03/CDT_NTIA_IoT_comments_Mar2017.pdf, CDT Comments to FTC Workshop on IoT, June 1, 2013, at https://cdt.org/files/pdfs/CDT-Internet-of-Things-Comments.pdf.

[2] CDT Support for S. 1691, Cybersecurity Improvement Act, (115th Cong.), at www.warner.senate.gov, Testimony of Justin Brookman before the Senate Judiciary Committee, The Connected World: Examining the Internet of Things, Feb. 11, 2015, at https://cdt.org/insight/testimony-of-justin-brookman-before-senate-commerce-on-internet-of-things/.

[3] Draft dated May 15, 2018, at https://docs.house.gov/meetings/IF/IF17/20180522/108341/BILLS-115pih-TodirecttheSecretaryofCom.pdf.

The SMART IoT Act Should Address Whether the Private Sector is Implementing Voluntary Standards and Whether They are Improving Security

Section 2(a)(1) directs the Secretary to survey the IoT industry and create a list of 1) the sectors that develop or use IoT devices, 2) ways the IoT is developed and used, 3) public or private partnerships that promote the adoption of IoT devices, and 4) industry-based bodies who have or are developing standards for connected devices.

While this list will create an expansive primer of the IoT industry, the committee's oversight and legislative function will benefit most from understanding the status of voluntary standard setting efforts. The Committee may benefit from shifting the emphasis of this section from creating a comprehensive list of all actors in the ecosystem to obtaining information about whether existing standards have been implemented - even if that means scoping the sectors that the report would cover.

It is important to note that NIST and NTIA have begun this process.[4] NISTIR 8200 (Draft), for example, reflects an interagency working group's effort to catalog different international standards and whether they have been adopted. It does not purport to cover every possible guideline relevant to IoT, but estimates that most of the reviewed sectors have incomplete standards, and those that do exist have not been implemented. Exploring this deficit in more detail will provide more actionable information than just a list of the governing documents.

[4] NISTIR 8200 (DRAFT), Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), at https://csrc.nist.gov/publications/detail/nistir/8200/draft, NTIA Multistakeholder Process: IoT Security Upgradability and Patchability, draft list of standard setting organizations at https://www.ntia.doc.gov/files/ntia/publications/handout-standardstargeted_0426.pdf.

We understand that some may chafe at the suggestion that the government should conduct such an evaluation. But the conclusion that government intervention is unnecessary or unwise is premised on industry adopting practices that deliver a sufficient level of security. And even if the review was to find a suboptimal adoption rate, it does not follow that direct government regulation would be the first or best response.

Agency Work to Oversee Critical IoT Sectors and Create Neutral Standards and Guidance Must Continue While the Bill's Study is Conducted

CDT also recommends that the bill clarify that the study for which it calls should not discourage existing agency IoT workstreams. Agencies are developing guidance now on IoT devices that pose risk of injury or even death in the case of a significant security failure. For example, guidance on connected cars or medical devices could prevent serious injury and should not be delayed.

This includes the work of NIST to develop guidance on managing IoT cybersecurity and privacy risks within federal information systems.[5] This effort to more explicitly map NIST's risk management framework and security and privacy controls on to government systems is critical. The US government has repeatedly acknowledged that cyber threats have become one of our country's most pressing national security concerns and designing government systems that can

[5] NIST, Considerations for Managing IoT Cybersecurity & Privacy Risk (Draft), at https://www.nist.gov/sites/default/files/documents/2018/04/13/iot_program_discussion_draft_april_2018.pdf.

better withstand attack or penetration is a priority of both the White House[6] and the Department of Homeland Security.[7]

In fact, NIST's privacy and security engineering guidance should be quickly embraced by federal agencies and the IT Modernization Board so that going forward, new government devices or services are created at the outset with state of the industry controls. While there may be debate over whether and how different companies should adopt NIST standards or guidance, it should be noncontroversial that the government follows its own advice on how to develop more secure systems.

The Energy and Commerce Committee Should Use the Results of the Study to Advance Standards for Consumer Products that Aren't Overseen by Other Agencies

As currently scoped, the SMART IoT Act will return information on an incredibly diverse range of devices and systems that are used by many different constituencies ranging from sophisticated corporations to everyday consumers. Coupled with the bill's review of federal jurisdiction, one would expect to find that consumer facing products like home devices or wearables to be in a sweet spot of under-regulation and this committee's jurisdiction. Congressional committees and federal agencies that regulate products that could cause acute physical or financial harm have added cybersecurity to the list of factors or components that

[6] EO 18,833 Enhancing the Effectiveness of Agency Chief Information Officers, May 15, 2018 at https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-effectiveness-agency-chief-information-officers/, American Technology Council, Report to the President on Federal IT Modernization, December 2017, at https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf, EO 13,800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11 2017, at https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[7] Department of Homeland Security, Cybersecurity Strategy, May 15, 2018, at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

they oversee. Yet there are many everyday devices whose security failures are more likely to result in a breach of personal information or contribute to a botnet that spreads malware that are falling through the cracks.

Consumer products also suffer from unique security weaknesses. They may be operated by lay users who are not equipped to make informed choices about what products to buy or how to reduce security risks that the products pose. These products may have complicated supply chains with components created by companies outside of US jurisdiction or companies that are unconcerned about reputational harm that can result from serious security failures. Consumer IoT devices may also be abandoned by manufacturers before the end of their life cycle because there is little to no recourse for everyday consumers whose devices no longer receive necessary updates.

As CDT discusses in its recently published report *Strict Products Liability and the Internet of Things*,[8] consumers face a dearth of meaningful options; they often do not have access to digestible information to guide their purchasing decisions, products can include inherently exploitable designs, and consumers usually do not have legal recourse when things go wrong. It has created a particularly unaccountable slice of the IoT market that this Committee should pursue.

Conclusion

CDT thanks the Committee for the chance to speak about the SMART IoT Act. Recent years have seen a new depth and breadth to IoT security failures - cars that inexplicably

[8] Benjamin Dean, CDT, April 2018, at https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

accelerate, medical devices that over-administer medication, webcams that are hacked into botnet service--and we appreciate Congress' interest in studying the problem. We look forward to working with you further on oversight and legislative options for developing a more secure IoT.