10 March 2017

National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725,
Washington, DC 20230

Re: Request for Public Comment - The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (IoT)

To: Travis Hall

A nonprofit advocacy organization, CDT works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security and enable free speech online. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges.

CDT applauds the NTIA and its Internet Policy Task Force for the green paper titled 'Fostering the Advancement of the Internet of Things'. This report provides a comprehensive examination of the key issues that decision-makers in the public and private sectors must grapple with in order to realize the benefits of the IoT, while mitigating security, privacy and other risks.

Risk-based approach to IoT security

CDT agrees with the NTIA's approach to the security of IoT technologies. The report reads, "The range of IoT devices and applications, as well as the many potential attack vectors and harms, may preclude a single, prescriptive solution. Instead, many commenters advocated a risk- based approach to understand threats and vulnerabilities" (p26).[1]

A risk-based approach is in accordance with international best practice in digital security and with the approach of the Federal Trade Commission[2]. For instance, the Department of Commerce's own NIST Cybersecurity Framework is grounded in a risk management approach.[3] Moreover, the concept of assessing the economic risk of data security practices is one of the two key messages of the OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social

[1] *These commentators included: Infineon Technologies Americas Comment; the U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment; Software & Information Industry Association Comment.*
[2] Federal Trade Commission (2016), "Internet of Things: Privacy and Security in a Connected World", FTC Staff Report, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[3] *NIST (2017), "NIST Cybersecurity Framework", https://www.nist.gov/cyberframework*

Prosperity, to which the U.S. is a signatory. The recommendations posit "the need to adopt an approach grounded in risk management. Instead of being treated as a technical problem that calls for technical solutions, digital risk should be approached as an economic risk."[4]

Quantification of IoT

Essential to a risk-based approach is the derivation of probabilities of digital security incidents (which are caused by threats and vulnerabilities) as well as estimates of the range of possible economic and/or social impacts of these incidents. This approach is useful because it assists decision-makers in allocating resources toward mitigating security threats and vulnerabilities, and the incidents they contribute to, in a way that minimizes the potential negative economic or social impact of these incidents. A risk-based approach improves security outcomes by investing resources in security measures that mitigate the causes of the most potentially costly incidents. This is a win-win for companies and for consumers.

However, in the final passages of the report, under section 4.D.iii 'Quantifying the IoT Sector' (p51) it states that, "those who did [previously provided comments pertaining to whether, and how, the government should measure the IoT sector and its economic impact] suggested that quantification of IoT was not a high priority. Several commenters even advised against government measuring IoT at this stage." CDT disagrees. Quantifying the IoT should be a high priority in the public and private sectors, particularly in the developing IoT market, because it provides the foundation for a solid risk-based approach that improves security outcomes.

The NTIA proposes two 'next steps' in relation to measurement:

- Explore developing metrics to better understand the role of IoT in the industrial value chain and its contributions to GDP, exports, and other economic measures. The Department will establish a definition for the digital economy and develop estimates of the domestic output, value added, and employment associated with the digital economy.
- Conduct research to improve the measurement of information and communications technology-enabled goods and services (including IoT) in order to improve the estimate of GDP, particularly as it relates to the digital economy, and productivity.

These macroeconomic variables – such as output, value added and employment – will provide some understanding of the aggregate economic benefit of IoT technologies. However, these variables do not provide an understanding of the potential direct costs or indirect economic losses due to security issues with IoT technologies. Without an understanding of the probabilities of incidents and related costs/losses, decision-makers in the public or private sector will not be sufficiently informed in the development and implementation of a risk-based approach to improve IoT security. Indeed, the

[4] *OECD, 2015, "Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document", http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*

macroeconomic variables themselves will subsequently be determined largely by the security of these technologies, which will in turn be dependent on the effective implementation of a risk-based approach.

CDT recommends that the NTIA and U.S. Department of Commerce, in conjunction with private sector stakeholders, expand its examination of metrics to include those relating to the security of IoT devices. Such metrics might include, but are not limited to: the probability of incidents occurring due to certain classes of digital threat (e.g. malware, denial of service, etc); the likelihood of incidents occurring as a result of known vulnerabilities in IoT software and hardware; the potential economic impact (costs and losses) of digital security incidents to individuals, households, businesses and the national economy; and the net economic impact of more secure IoT devices vis a vis the status quo.

Only by collecting metrics such as these can a risk-based approach to IoT security be developed and implemented. This in turn provides a means by which decision-makers in the public and private sectors can determine which security measures, or public policies to spur development and/or adoption of security measures, for IoT technologies will yield the greatest net economic and social benefit (that is, cost-minimization and benefit maximization).

Privacy issues posed by the IoT

The green paper notes at the onset that the IoT is different from existing technological issues because of its potential size and scope, and that these differences produce a "qualitative change in the stakes involved in connectivity" (p. 3-4). For these same reasons, the IoT also raises novel privacy issues. As the NTIA recognizes, concerns about potential privacy challenges posed by the IoT were second only to digital security, and yet the green paper states only that commenters and stakeholders are divided as to whether the IoT presents any novel challenges (p. 30).

This assessment is inadequate. For the same reasons that the scale, scope, and stakes of the IoT offer tremendous benefits and require a general policy response from government, they also necessitate a firm commitment to recognize the distinct privacy considerations involved.

The growing deployment of sensors and devices in homes, cars, even in humans, present new vectors for the ubiquitous collection and sharing of highly sensitive personal information over time, including health status and activity levels, personal habits, location, the presence of other individuals and other types of metadata. Consumers regularly report that they feel as if they have lost control over their information,[5] and the IoT exacerbates this problem by facilitating the further collection and sharing of data in a way that is mostly opaque to consumers. Further, the level of granularity with which data is collected allows entities to infer sensitive data from fine-grained sources of seemingly innocuous

[5] Lee Rainie, Pew Research Ctr., *The State of Privacy in Post-Snowden America* (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

sensor data.[6] In short, the IoT raises new questions as to what precisely constitutes personal information and private spaces.

Many of these novel issues are challenging existing legal frameworks. The Supreme Court, for example, has begun to acknowledge how digital and physical spaces can present different constitutional questions under the Fourth Amendment. The court recognized that physical papers and effects could be distinguished from the digital data generated by those objects in *Riley v. California*,[7] which followed the Court's decision in *United States v. Jones*, where the full court agreed that the warrantless use of a GPS device to track a suspect violated the Fourth Amendment. Writing in concurrence, Justice Sotomayor questioned whether individuals "reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[8]

The green paper recognizes the role for congressional action in addressing privacy in the IoT. However, absent baseline privacy legislation, no federal agency has the authority to mandate basic privacy protections. This includes even basic disclosures about how devices and sensor data are collecting, using, or sharing information. As a result, consumers are typically kept in the dark about how their information is being processed, and they can be denied effective or meaningful legal remedies where privacy violations occur or mistakes are made with respect to their information. The IoT may only amplify this tension.

Both real and perceived privacy risks threaten public trust in and adoption of IoT technologies. A 2016 study by the NTIA confirmed that privacy concerns inhibit Americans' economic and other online activities,[9] and as the Federal Trade Commission has acknowledged, concerns about the lack of privacy protections "permeate the IoT."[10] To address these concerns, the FTC has specifically encouraged industry to offer greater transparency and better user controls.[11] Where IoT technologies are presented as a "take it or leave it," however, individuals may be left with no real choice. We are encouraged to see multistakeholder recommendations for privacy and security in the IoT, recently

---

[6] *For example,* cell *phone gyroscopes – which sense the orientation and movement of a cell phone – are sensitive enough to ambient pressure changes that they can be used as microphones; see: Michalevsky, Y., Boneh, D., & Nakibly, G. (2014, August). Gyrophone: Recognizing Speech from Gyroscope Signals. In USENIX Security (pp. 1053-1067), https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-michalevsky.pdf. FTC Staff Report, 2015, "Internet of Things: Privacy and Security in a Connected World," https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*

[7] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[8] United States v. Jones, 132 S. Ct. 945, 956 (Sotomayor, J., concurring) (2012).

[9] Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[10] FTC Staff Report, *supra* note 4, at 51.

[11] *Id.* at 50-51.

released by the Broadband Internet Technology Advisory Group (BITAG) as well as open certification and risk assessment efforts.[12]

Though it is likely that the Federal Trade Commission will continue to lead on privacy policy and enforcement, CDT recommends that the NTIA and Department of Commerce continue their ongoing efforts to engage stakeholders and to pursue consensus-based global standards, starting from the premise that the privacy challenges raised by the IoT are novel. The Department is well positioned to highlight efforts within industry to promote privacy, which includes addressing basic Fair Information Practice Principles and adopting privacy by design across the full lifecycle of IoT devices, products, and services.

We thank the NTIA for the opportunity to provide comments on this report and look forward to working with the Administration in its efforts to foster the advancement of the internet of things.

Sincerely,

Benjamin C. Dean
Ford/MDF Technical Exchange Fellow

Joseph Jerome
Policy Counsel, Privacy & Data Project

Michelle De Mooy
Director, Privacy & Data Project

Joseph Lorenzo Hall
Chief Technologist

[12] *Consumer Reports, "Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security", (March 6, 2017)* *http://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/; Online Trust Alliance, "Coalition Releases Connected Device Requirements," (January 5, 2017),* *https://otalliance.org/news-events/press-releases/ota-calls-iot-cyberattacks-%E2%80%9Cshot-across-bow%E2%80%9D*.