INTERNET OF THINGS
PRIVACY FORUM

Comments submitted to the National Telecommunications and Information Administration

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Docket No. 160331306–6306–01
Submitted May 23, 2016

Author: Dr. Gilad L. Rosner

This document is a response to the NTIA's request for comments on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things." The Internet of Things Privacy Forum is a non-profit organization whose mission is to produce guidance, analysis and best practices to enable industry and government to reduce risk and innovate responsibly in the domain of connected devices. The document is authored by Dr. Gilad Rosner, founder of the Forum, and an information policy, identity management and privacy researcher. Dr. Rosner is a member of the UK Cabinet Office Privacy and Consumer Advisory Group, which provides independent analysis and guidance on Government digital initiatives, and he has undertaken extensive research of the US FICAM and NSTIC policy initiatives. He is a Visiting Researcher at the Horizon Digital Economy Research Institute, and has consulted on trust issues for the UK government's identity assurance program, Verify.gov. Dr. Rosner is a policy advisor to Wisconsin State Representative Melissa Sargent, and has contributed directly to legislation on law enforcement access to location data, access to digital assets upon death, and the collection of student biometrics.

Questions posed by the NTIA in its request for comments in the Federal Register are italicized and then followed by responses. The IoT Privacy Forum is grateful for the opportunity to provide input to the Department of Commerce on these important topics.

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?
a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?
b. What are the novel policy challenges presented by IoT relative to existing technology policy issues, if any? Why are they novel? Can existing policies and policy approaches address these new challenges, and if not, why?

The Internet of Things bears resemblance to prior technologies, and it possesses some new characteristics as well. All of the features of the IoT – sensors, computing, networking, miniaturization, reduced manufacturing cost, and rapid prototyping, to name a few – have existed for years or decades. So, the major difference that the IoT portends is one of *scale*. That is, the amount of sensors in the human environment, the degree of data collection, the diffusion of computing power to network edges, and the number of commercial stakeholders are the novel characteristics of the IoT. The question of scale implies the following:

- A massive increase in sensors in the human environment means that data collection will occur in much greater amounts and more diverse ways. Location, identity, biometric, lifestyle, purchasing, and health information will be collected more in public and intimate spaces. Some of this will be volunteered, as in the case with fitness wearables, but some of it will come from private data collection in public spaces thanks to ever-reducing costs for cameras, microphones, accelerometers and other sensors, and greater network ubiquity.

- An increase in stakeholders will introduce new players into the market: manufacturers, programmers, service companies, intermediaries (e.g., IoT 'platforms'), networking services, and others. Some of these new entrants will be good at security engineering, and many will not. Ashkan Soltani, former Chief Technologist of the FTC, succinctly discussed this challenge in a 2015 blog post[1]:
  "Growth and diversity in IoT hardware also means that many devices introduced in the IoT market will be manufactured by new entrants that have very little prior experience in software development and security… Market dynamics underlying IoT is quite different from those found in the PC or Smartphone market. While IoT encompasses big and expensive devices like cars and smart televisions, there are also a large number of small and **extremely** low cost light bulbs, blankets, webcams, and routers – which might not receive the same level of warranty and support. Manufacturers may not be as incentivized to fix or patch vulnerability on a $30 webcam that they would on a $500 smartphone or $1000 laptop."
- Given the IoT's heterogeneous nature, a change in scale will not be traceable to a single sector, industry or technology. These scale changes will occur across markets, and as such will need to be considered within the regulatory context of those markets.

Existing approaches will be adequate for some issues, but privacy and security challenges will need policy and regulation to be updated and periodically reviewed. One legal foundation deserves particular attention: the reasonable expectation of privacy. Since the advent of the internet, this legal standard has been breaking down. As people have come to understand, in greater and lesser degrees, that the free services they enjoy on the internet are in fact paid for by the collection of data about them, spaces in which a person may reasonably assume privacy have been shrinking. The IoT means that more devices will encroach upon intimate spaces and track people more in public, which will only serve to further erode the concept of the reasonable expectation of privacy. As such, it is a legal framework in need of reconsideration.

3. With respect to current or planned laws, regulations, and/or policies that apply to IoT:

a. Are there examples that, in your view, foster IoT development and deployment, while also providing an appropriate level of protection to workers, consumers,

[1] Soltani, A. (2015 Feb 10). "What's the security shelf-life of IoT?" [blog post]. Available at https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot

patients, and/or other users of IoT technologies?

One technology that arguably falls under the heading of the IoT are vehicle event data recorders (EDRs), sometimes called "black boxes," which are used to gather information about a car in the event of a crash. These are similar to the black boxes built into aircraft for crash forensics. According to federal government researchers, 90% of all new cars and light trucks are equipped with EDRs[2]. While these black boxes are not consumer accessible, the do implicate consumer privacy. The federal researchers note:

> "Perhaps the most prominent concern about EDRs is their impact on personal privacy. While current regulations provide only that EDRs, if installed, track 15 specific data elements, technological advances may allow greater data collection. In addition, individual auto manufacturers are free to collect more data, or to collect data for longer time periods, than required under NHTSA's EDR rule. When combined with other technologies, such as onboard navigation systems and mapping apps, EDR data could be transmitted beyond the vehicle owner's control."[3]

Given this, it's important for regulation to address the issues of privacy and owner control so as to preserve consumer welfare and trust with these valuable safety systems. Seventeen US states have enacted laws relating to vehicle EDRs and privacy[4]. Montana's 2015 SB 0209 provides a good example of legislation that allows for the utility of vehicle EDRs while preserving both owner control and privacy, specifically in the context of insurance provisioning. SB 0209 states:

- The data on a motor vehicle event data recorder is exclusively owned by the owner or owners of the motor vehicle and may not be retrieved or used by any person other than an owner of the motor vehicle without the written consent of an owner"

Data can be retrieved without owner consent in cases of a search warrant, a need to provide emergency medical care, a court order but with a period to request a hearing, and "for the purposes of improving motor vehicle safety, security, or traffic management and provided that the identity of the owner or driver is not disclosed in connection with that retrieved data." The Montana statute requires therefore that the EDR data be de-identified. Importantly, this requirement supports the principle

[2] Canis, B. and Peterman, D. (2014). "'Black Boxes' in Passenger Vehicles: Policy Issues". Congressional Research Service. Available at https://www.fas.org/sgp/crs/misc/R43651.pdf

[3] Ibid, pp. 9-10.

[4] National Conference of State Legislatures. (2016). Privacy of data from event data recorders: State statutes. Available at http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx

of *data minimization*, one of the Fair Information Practice Principles (FIPPs) that underpins much of US privacy and data protection. In a 2008 formulation of the FIPPs, the Department of Homeland Security (DHS) stated this principle as: "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)"[5]. Montana lawmakers understood that the improvement of vehicle and road safety and traffic management did not mean that drivers should have identifying information about them collected. The question of how revealing black box data is now or could be in the future is mooted by the adherence to the principle that personal data should not be collected without consent or when it does not serve a given purpose. It shows that the information that can be generated by cars, which is socially valuable, can be collected and analysed without intruding upon the privacy of citizens.

The Montana statute also states:

- "An insurer may not condition the payment or settlement of an owner's claim on the owner's consent to the retrieval or use of the data on a motor vehicle event data recorder."
- "An insurer or lessor of a motor vehicle may not require an owner to consent to the retrieval or use of the data on a motor vehicle event data recorder as a condition of providing the policy or lease."

These two prohibitions reinforce the principle of owner control, and prevents a shift in informational power from owners to insurance companies. Privacy protection is in part about a person's ability to control information flows. Conditioning insurance settlement or the ability to purchase insurance on the access to EDR data is coercion – the Montana law prevents insurance companies from using its financial power to obtain this data simply because it is available or because they feel it will improve their business processes. The principle being upheld here is that more data means that citizens should be given more power and control over it through regulatory means.

4. Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to- device vs. human interfacing.

From a perspective of privacy and data protection, it's helpful to divide the IoT into personally identifiable information (PII) and non-PII gathering groups. While there

[5] See DHS Memorandum Number: 2008-01, Available at https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

is privacy scholarship that calls this division into question, it serves it least as a coarse but useful way to divide regulatory approaches and resources. For example, IoT technologies used in mining will generate very little PII, whereas consumer goods will generate a great deal.

5. Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant?

Scott Peppet of the University of Colorado Law School wrote a paper entitled, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent"[6]. This law review article is significant because it methodically lays out several privacy challenges posed by the IoT, and then proposes legal and policy remedies. Such a comprehensive treatment of these issues is rare. The paper has been included in this submission.

17. How should the government address or respond to privacy concerns about IoT?
a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

Privacy concerns specifically raised by the IoT include:

- Enhanced monitoring. As discussed above, the increase in the number of sensors in the human environment will lead to a greater degree of collection and analysis of human behavior and events.
- Unconsented capture: Devices in public, at work and in the home have the potential to collect data from people without their knowledge or consent.
- Collection of children's data: In line with the above point, children's data may find its way into data stores as easily as adult's.

IoT privacy concerns can be thought of under three headings:

- Amplifications of existing privacy problems. Issues such as inappropriate surveillance, unconsented capture, and the potential for data to be used to discriminate are not particular to the IoT. However, given the above discussion of increases in monitoring, the IoT has the potential to amplify these pre-existing privacy challenges.

[6] Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074

- IoT problems are ‘big data’ problems. The IoT is an input to large-scale data analysis. Ergo, the IoT can amplify the privacy challenges those systems pose[7].
- Privacy problems particular to IoT verticals, sectors or technologies. Privacy challenges tend to be specific to a given vertical, sector or technology. For example, the privacy risks posed by connected cars – revelation of location and driving style – are dissimilar to the risks posed by wearable medical devices, which include revelation of health, medicine regime, vital signs, or sleep patterns. As such, policy approaches must take this sector-specificity into account. Certain policies, like mandatory data breach notification, can be applied cross-sector. But others, such as the protection of sensitive health information, need sectoral approaches.

[7] See White House. (2014). Big Data: Seizing Opportunities, Preserving Values. Available at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf