

**Internet of Things Workshop Report**  
**Separate Statement of Commissioner Maureen K. Ohlhausen**  
**January 27, 2015**

I concur in the issuance of the staff report on the Internet of Things (IoT) workshop.

As the report acknowledges, we are in the early days of this rapidly developing technology. I have often advocated approaching complex technologies and rapidly changing business models with an attitude of regulatory humility.<sup>1</sup> This means we must work to understand the likely benefits and risks of IoT technology, focus on actual rather than speculative harms, and evaluate the ability of our existing tools to deal with such harms before calling for new laws or regulations. This report makes some progress consistent with these goals, and therefore I generally support it, with a few caveats.

The staff report does five things well:

- The report opposes IoT-specific legislation, stating that such legislation “would be premature” because the industry “is in its relatively early stages,” and has “great potential for innovation.”
- The report focuses on devices sold to or used by consumers, particularly devices that collect sensitive consumer information, such as real-time location or health information. Although consumers will likely benefit greatly from industrial and other business uses of IoT technology, such non-consumer facing technologies present very different data security and privacy issues than do consumer-oriented devices.
- The report prioritizes security of IoT technology and the personal data collected as a primary concern. Some IoT devices have already experienced data security failures that have harmed consumers.<sup>2</sup> The report thus reiterates the Commission’s recent unanimous and bi-partisan call for data security legislation.<sup>3</sup>
- The report acknowledges the challenges that the IoT raises for the Fair Information Practice Principles (FIPPs), particularly the principles of notice and choice and data minimization. The report reasonably concludes that for many available consumer IoT applications, there are myriad ways to provide notice and choice for collecting consumers’ personal information. It also notes the findings of the White House and PCAST Big Data reports that there are types

---

<sup>1</sup> See, e.g., Comments of Commissioner Maureen K. Ohlhausen, Federal Trade Commission, to NTIA on Big Data, Consumer Privacy, and the Consumer Bill of Rights at 12 (Aug. 5, 2014), *available at* [http://www.ftc.gov/system/files/documents/public\\_statements/573921/140806bigdata.pdf](http://www.ftc.gov/system/files/documents/public_statements/573921/140806bigdata.pdf).

<sup>2</sup> By contrast, the privacy harms discussed in the report are thus far largely hypothetical.

<sup>3</sup> See Prepared Statement of the Federal Trade Commission, “Protecting Personal Consumer Information from Cyber Attacks and Data Breaches,” Before the Senate Committee on Commerce, Science, And Transportation, 114<sup>th</sup> Cong., Mar. 26, 2014, *available at* [http://www.ftc.gov/system/files/documents/public\\_statements/293861/140326datasecurity.pdf](http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf).

of data collection and use that notice and choice simply cannot address.<sup>4</sup> By acknowledging FIPPs' potential limits the report takes an important step forward.

- The report acknowledges that limiting certain data uses is a promising approach to protecting consumer privacy in IoT applications. Indeed, the report acknowledges the use-based approach in the Fair Credit Reporting Act (FCRA) and notes that the use-based approach informs parts of the Commission's current privacy framework, including its unfairness authority to challenge harmful uses of consumer data. In short, the report's discussion of use-based approaches joins the ongoing dialog on how to supplement FIPPs to promote innovation and protect consumers more effectively.

However, I do not support two of the staff report's recommendations.<sup>5</sup>

First, I do not support the recommendation for baseline privacy legislation because I do not see the current need for such legislation. The FTC's Section 5 deception and unfairness authority already requires notice and opt-in consent for collecting consumers' sensitive, personally identifiable information. It also protects against uses of personal information that cause substantial, unavoidable consumer harm not outweighed by benefits to consumers or competition. Furthermore, sector-specific laws, such as FCRA, provide additional protections for consumers. Thus, I question what current harms baseline privacy legislation would reach that the FTC's existing authority cannot.

Second, I am concerned that the report's support for data minimization embodies what scholar Adam Thierer has called the "precautionary principle,"<sup>6</sup> and I cannot embrace such an approach. The report, without examining costs or benefits, encourages companies to delete valuable data – primarily to avoid hypothetical future harms. Even though the report recognizes the need for flexibility for companies weighing whether and what data to retain, the recommendation remains overly prescriptive.

One final, more general caveat: The report misses the opportunity to explore fully the emerging tension between information technology (including IoT) and the FIPPs approach to protecting consumer privacy. The White House and PCAST reports raised these issues (as noted

---

<sup>4</sup> See Executive Office of the President, *BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES* at 54 (May 2014) (because "the logic of collecting as much data as possible is strong ... focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); President's Council of Advisors on Science and Technology, *REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE* at x-xi (May 2014) ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).")

<sup>5</sup> I share Commissioner Wright's concerns with the report's lack of a rigorous cost-benefit analysis regarding its recommendations for privacy legislation and data minimization. However, given the report's limited scope, I find its reiteration of the Commission's previous unanimous data security legislative recommendation and its generally modest recommendations – other than the disputes noted here – to be appropriate.

<sup>6</sup> ADAM THIERER, *THE INTERNET OF THINGS AND WEARABLE TECHNOLOGY* at 31 (Nov. 2014), available at <http://mercatus.org/sites/default/files/Thierer-Wearable-Tech.pdf>.

above), as have others, including some workshop participants.<sup>7</sup> The staff report acknowledges the conflict, but fails to grapple with it in a substantial way. We will need to address these issues in the relatively near future, and I look forward to playing a role in that effort.

Overall, the report advances the Commission's efforts to understand the benefits and risks of IoT technology and government's proper role in maximizing these benefits and mitigating these risks. For these reasons, I concur in the issuance of this staff report on the Internet of Things Workshop.

---

<sup>7</sup> See Remarks of Peppet, Transcript of Fed. Trade Comm'n Workshop, Internet of Things at 210-211 (Nov. 19, 2013) (advocating "drawing some lines around acceptable use" in addition to notice and choice), *available at* [http://www.ftc.gov/sites/default/files/documents/public\\_events/internet-things-privacy-security-connected-world/final\\_transcript.pdf](http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf); SCOTT R. PEPPET, REGULATING THE INTERNET OF THINGS, 93 Texas L. Rev. 85, 147, 149 (calling notice and choice "an ill-fitting solution" and proposing constraining "certain uses of Internet of Things data"); THIERER, *supra* n.6 at 48 ("[I]t is almost impossible to envision how a rigid application of traditional notice and choice procedures to IoT would work in practice.").