Protecting Competition and Innovation in Home Technologies

Hearing before the Senate Committee on the Judiciary, Subcommittee on Antitrust, Competition Policy, and Consumer Rights

June 15, 2021

QUESTIONS FROM SENATOR BLUMENTHAL

Questions for Professor Zittrain:

1. In your written testimony, you noted that "without trusted industry-wide buy in" on interoperability standards, "any new unifying standard risks becoming just yet another instrument in a cacophony." What approaches—legislative or otherwise—do you recommend to achieve trusted industry-wide interoperability?

   Regulators, including the Federal government, could establish standards for nondiscriminatory (but still secured and authorized) access to the basic control structures of smart devices. The proposed ACCESS Act is an example of an approach that could achieve this with major vendors of smart devices, including the structuring of trusted intermediaries to assist with private data management.

   More broadly, some standards for the communication and control of smart devices would represent a public good the way that Internet-related protocols are public goods – developed outside of any one vendor (indeed, noncommercially), and available to all. There is no need to mandate that networked devices use Internet protocol because it's such a well-established and useful standard. To become that required some fortuity and some hard work by people not operating under the usual conventions of dot-com competition. As it rightly does with other public goods, Congress could subsidize – with comparatively very little investment – the generation of and experimentation with such standards, possibly through National Science Foundation support for academic researchers who wish to engage in open development. Government procurement standards, could in turn promote the adoption of such devices: "buy American" could be complemented with "buy open."

   a. If I have Internet of Things products in my home, like Amazon's Alexa or Google's Nest products, how would interoperability requirements help me as a consumer?

      Interoperability requirements would help avoid consumer lock-in, which, as I described in my testimony, occurs when a necessarily cabined choice of phone or smart device snowballs into a permanent choice of a proprietary ecosystem over time. The ability to separate hardware devices from hardware hubs, and hardware from software, would allow consumers to control them through other vendors or other means. This would also help avoid a "monoculture" in

operations that could pose a systemic risk.

b. How would interoperability requirements help nascent competitors build new Internet of Things devices?

Interoperability requirements or practices would allow nascent competitors to build devices without incurring the significant cost associated with building control interfaces or hubs. In much the same way that someone can write a program that uses the Internet or simply functions on a smartphone without having to reinvent networking protocols, increased interoperability would simplify the product development process, allowing competitors to focus on what is to be offered as the most innovative contribution.

Similarly, competitors could experiment with new ways to control or manage devices, including that link them among devices from multiple vendors, and offer those control systems as their innovative contribution.

2. In your written testimony, you write that "as someone who historically has not broken the glass and pulled the fire alarm for every possible concern about digital privacy over the past thirty years, the Internet of Things stands to become a privacy apocalypse." You describe the ways in which microphones, cameras, and other sensors attached to Internet of Things devices can reveal detailed information about Americans' daily lives.

   a. What tools should Congress consider to protect consumer privacy in the Internet of Things marketplace?

   Congress should urgently intervene to require large platforms hosting massive amounts of public-facing personal data to take basic steps to secure that data against uses not contemplated by their users. For example, just as Facebook and Twitter rightly strip out geolocation data otherwise automatically embedded in the smartphone photos that their users post, they should perform basic tasks to safeguard user data against total-scale scraping and to render it less amenable to processing, such as through "adversarial perturbation" of photos to make them less susceptible to facial recognition or sorting algorithms without user consent. Smart devices that gather photos and other identifiable data could similarly work to protect against unexpected bulk uses.

   The nature and types of telemetry conveyed by smart devices to their vendors should be required to be disclosed up front the way that food must have a nutrition label. Devices should be required to have a "faraday mode" that severs all telemetry while preserving functions that do not require a link to the vendor to work.

   b. You write that Internet of Things products "opens up entirely new avenues of government-mandated monitoring, and in the United States the ground rules for such surveillance are as yet poorly understood, since they were developed around

communications technologies, that is, devices put into use only when one person is trying to communicate with others, such as telephones." Why does the Electronic Communications Privacy Act and other key surveillance laws not cover these devices? Should the Electronic Communications Privacy Act be updated to address Internet of Things technologies that might fall outside of the scope of "communications technologies" motivating the passage of that law in 1986, and if so, what changes do you recommend?

Congress should provide for a higher level of privacy protection for outside monitoring of devices that are not communications devices. The framework for monitoring traditional communications contains within it the idea that people communicating, when up to no good, is something that can facilitate crime – hence the idea of "conspiracy" as a separate substantive crime, and of accomplice liability. In the absence of these factors, the rights of people to simply exist in their homes or other places of repose without undue monitoring should be specifically secured. Previously, the effort required to surveill people in such circumstances was itself onerous enough to limit applications for surveillance. The Internet of Things inverts that, making monitoring through home web cams, televisions, or other devices potentially trivial. The law must respond.