PAUL HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

November 2013

The Internet of Things: The FTC Considers Privacy and Security in a Connected World

BY LISA A. NOWLIN

The Internet of Things refers to the network of communications between everyday devices and between those devices and their owners, manufacturers and others. Emerging "smart" devices include self-driving cars, self-monitoring refrigerators and smart toasters. There are currently more devices connected to the Internet than there are people in the world. Cisco predicts that by 2015, more than 25 billion things will be connected to the Internet, and more than 50 billion in 2020. With the Internet of Things comes a new set of privacy and security issues to be grappled with. After soliciting public comment on the issue, the Federal Trade Commission (FTC) invited practitioners and researchers to participate in a workshop on November 19, 2013, to discuss the consumer privacy and security issues posed by the rapidly expanding Internet of Things.

Connected devices can provide convenience, can enable people to do things they could not otherwise do, and can save lives. A connected oven allows you to start preheating your oven remotely on your way home from work. A self-driving car can provide new mobility and independence to a blind person. And a connected pacemaker has the potential to alert emergency services should the individual's heart stop.

The FTC workshop discussed three major challenges the agency sees as presented by the proliferation of these devices. The first is the ubiquitous collection of vast consumer data. As connected devices enter every facet of our lives, the types and the quantity of data collected are unprecedented. The second challenge is how these new troves of data will be used and shared. And the third challenge is the security risks posed by connected devices.

A brief summary of the workshop panelists' comments on each of these issues, on recommended ways to address them and of the FTC's announced intentions is set out below.

Privacy – Collection and Use

As one workshop speaker put it, the Internet of Things creates an infrastructure of surveillance. As more and more aspects of our lives are monitored, it is possible to compile data to create a startlingly complete profile of a person. For example, by reviewing the data collected by a smart grid, a connected electrical grid that collects information to utilize energy more efficiently, it can be inferred when you woke up, where in the house you are, how many people are in your house, etc. Another example is a Fitbit, a physical activity monitoring device. In addition to literally monitoring your every

move, the CTO of the CIA recently stated that Fitbit can tell with 100% accuracy who you are by your gait.

As data-collecting devices become more and more common in consumers' lives, we will need to grapple with issues such as who owns the intimate data collected by connected devices, what is done with this data, who the data is shared with, and how much control consumers have over what happens to the data.

Laws and policies may need to evolve as well. Currently, when connected devices are hacked, it does not trigger state data breach disclosures. One recurrent topic was the possibility of data being shared with insurance companies. Can your car insurance company require cars they insure to have black boxes in them? Some states have passed laws against this, but it is an open question in most jurisdictions. What about health insurers accessing consumers' Fitbit information and raising premiums due to lack of physical activity?

Security Risks

Any device connected to the Internet of Things is subject to being hacked. Connected devices typically have very little security, because the devices are not seen as high risk by the manufacturers or by the consumers. Due to the consumers' general lack of concern about security with these devices, there is little financial incentive for manufacturers to make the devices more secure. Most devices rely on the security of the home Wi-Fi network to which they connect as their sole source of security.

The security risks associated with connected devices can be very serious, even lethal. A hacked pacemaker can be turned off or a hacked insulin pump can provide an overdose of insulin. The vulnerability of medical devices was made part of popular culture thanks to an episode of the popular Showtime series *Homeland*, in which the vice president—who sported a pacemaker—is assassinated through a remote hack. Indeed, former Vice President Richard Cheney had the wireless feature of his pacemaker disabled precisely for that reason.

A University of Washington professor at the FTC workshop described his research team's tests remotely hacking into two cars. Many new cars have over 100 connected computers—the system that locks and unlocks the doors may have four or five alone. Once the car was hacked, the research team could start the car, disable the brakes, locate the car, turn on the Bluetooth microphone, and turn off the anti-theft device, among other things.

While these may be extreme examples, hacks of more mundane devices can still be inconvenient and result in breaches of privacy. Having one's thermostat or Fitbit hacked would likely not be life threatening, but could be inconvenient, potentially expensive, and would provide a stranger with large amounts of personal data.

Potential Responses

While best practices are still being developed in the rapidly innovating Internet of Things, there were a few principles on which the private-sector panelists appeared to agree. An oft-repeated phrase throughout the day was "security by design," meaning that security must be hardcoded into the device and software. The layers of security to be considered involve the user (password), application (software), environment (physical security at the data center), device (hardware), network (what the device connects to) and service (every touch point with the customer, such as customer service).

It was noted that many of the issues and vulnerabilities that connected devices are encountering are not new and have been encountered with the Internet before. The solutions are available but are often not implemented in connected devices due to a lack of expertise or a lack of care on the part of the manufacturer. Looking to security early in the process will be much more efficient and cost-effective than trying to implement it after the fact.

Other recommendations identified by panelists included shifting the burden of privacy off of consumers, providing consumers control over their own data and providing transparency about how data is collected, used and shared. One hurdle associated with these newly connected devices is how to provide notice and consent on devices that do not have screens or other user interfaces amenable to that type of interaction.

The FTC's Next Steps

At the end of the workshop, the FTC dispelled any rumors that it might be preparing new regulations on this issue, but it did announce that it is preparing a report on best practices for privacy and security for connected devices. The agency hopes the report will encourage industry to adopt those practices in its development of these new devices. Whether those recommendations will prove welcome or controversial—and to whom—is as yet unclear. The FTC invites the public to submit comments until January 10, 2014.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

San Francisco

Thomas Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Lisa Nowlin
1.202.551.1752
lisanowlin@paulhastings.com