

Implications from CES

2014: Balancing Privacy and The Internet of Things

By, Adam D.H. Grant

The 2014 International Consumer Electronics Show (CES), clearly demonstrated that the “Internet of Things” (IoT) is no longer the industry buzzword of a few years ago, but is now well entrenched as a market reality. What remains unclear is just how policy makers and legislatures will react to what appears to be the next step in the digital age.

As the expected 150,000 people walked through the show’s record 1.861 million square feet of exhibit space, vendors demonstrated just how connected we could be to our environment. Tiny sensors embedded in the handle of a tennis racket measures a player’s strokes, topspin and just about everything else that happens when a player strikes a ball. Innovations also include embedding a chip the size of a grain of rice into a basketball which allows your home’s wireless network to sense the basketball and make recommendations to you for games or tv programs. As a parent, I will refrain from commenting on the use of a basketball inside the house! However, as a parent I can also appreciate the ability to control the use of your crockpot via a mobile app to insure dinner will be ready for the family at the end of the day.

By 2050, analysts project, there will be 50 billion internet-connected devices, or five gadgets for every man, woman and child. According to Scott McGregor, president of Broadcom, as the possibilities “you’re going to see an explosion of devices.” Whether it involves, pets, livestock, sports equipment, watches, light bulbs, if you can think of it, someone has likely put a sensor on it and connected it to the internet. According to Patrick Moorhead, principal analyst for Moor Insights & Strategy, “We’re seeing an acceleration of uses with the consumer Internet of things. You could have done many of these things before, but the battery life might have been one hour. Now it lasts a week.”

The real question is whether policy makers and legislatures across this country will

let the Internet of Things flood gates open up or restrict the flow to a trickle as the law races to keep up with this ever changing river of information. Over the past two years in particular, the FTC and various state Attorneys General, most notably Ms. Kamala Harris in California, have questioned whether this torrent of connectivity is good and if so, just how good. While consumers are rushing to embrace any device that has a sensor, a chip, or some sort of networking capability, lawmakers are proceeding with a higher degree of trepidation. Policy and law makers fear the safety, security, or privacy-related problems are lurking beneath the surface.

At CES, during a panel discussion entitled, “The Internet of Things and the Home of the Future,” the FTC Commissioner, Maureen K. Ohlhausen, addressed this tension in her opening remarks. Ms. Ohlhausen made the case for regulatory humility and the need to focus on how the new technologies empower consumers in important new ways. “The Internet has evolved in one generation from a network of electronically interlinked research facilities in the United States to one of the most dynamic forces in the global economy, in the process of reshaping entire industries and even changing the way we interact on a personal level,” she commented.

In referencing a recent book, she directly addressed the concern stating, “Although *The Circle* is fictional, the novel reflects a real concern shared by many about a loss of privacy. Because interconnected devices and services often collect and share large amounts of personal information, policymakers and members of the tech community must be sensitive to consumer privacy and data security issues. It is thus crucial that companies offering these products as part of the Internet of Things act to safeguard the privacy of users to avoid giving the technology a bad name while it is still in its infancy.”

Ms. Ohlhausen even gave a concrete example of the reason for her concerns. She noted, that in September, the FTC settled a case against TRENDnet, which sold its Internet-connected SecurView cameras for purposes ranging from home security to baby monitoring. Although the company claimed that the cameras were secure, according to the FTC, they actually had faulty software that allowed unfettered online viewing by anyone with a camera's Internet address. As a result, hackers posted live feeds of nearly 700 consumer cameras on the Internet, showing activities such as babies asleep in their cribs and children playing in their homes. The FTC found that TRENDnet's practices were both deceptive and unfair. She concluded that the type of consumer harm the FTC saw in the TRENDnet case—surveillance in the home by unauthorized viewers—fed concerns about the Internet of Things overall.

Ms. Ohlhausen noted that the traditional notice and choice paradigm becomes even more complicated for devices with a limited or no user interface. For example, activity trackers such as the FitBit Force and the Jawbone UP have only very basic user interfaces on the device itself. Other connected devices, such as smart lightbulbs, may not have any consumer-facing user interface at all. Addressing consumers' privacy concerns over such devices will present business, engineering, and policy challenges that will require constant innovation from all involved.

The panel discussion that followed Ms. Ohlhausen's opening remarks got into the weeds of this hot topic. In particular, Adam Thierer, a senior research fellow at the Mercatus Center at George Mason University described the future of the Internet of Things as a grand battle of two alternative worldviews: the "precautionary principle" and "permissionless innovation." He described the "precautionary principle" as a belief that new innovations should be limited or disallowed until the developers can prove that

they will not harm. "Permissionless innovations" he suggested, refers to experimentation with new technologies and business models should be the default position. Unless such innovations cause serious harm, the natural progression of things should be permitted and problems, if any, can be addressed later.

Using Mr. Thierer's competing principles it is clear where things are heading. All vendors at CES 2014 clearly would desire the "permissionless innovation" as it would provide the industry unlimited possibilities, without the impediments of "what ifs." Conversely, Ms. Ohlhausen and the FTC would certainly prefer the "precautionary principle" as a means of insuring consumers will, at least to some extent, still have a reasonable expectation of privacy in some aspect of their lives. As 2014 unfolds and these new products are unleashed into the market, we will undoubtedly witness a balance between legal precautions and permissionless progress.



Adam Grant

Adam is the Chief Legal Contributor for App Developer Magazine and is a partner with Alpert, Barr & Grant, A Professional Law Corporation.

With over 20 years of experience, he supports the firm's litigation practice with expertise in complex business disputes, mobile app law, privacy and embezzlement issues, construction law and real estate matters. He has litigated in both state and federal courts.