Connectivity TODAY AND BEYOND

THE FTC'S VIEW OF THINGS TO COME

By Adam D.H. Grant, J.D.

Mobile apps have literally changed how we interact with others, connect with the physical world, and learn about both. In college as a political science major, I learned about "world hegemony." My professors discussed how connected each country had become because of economic interdependence. We discussed how countries relied on each other for many things, including natural resources, financial backing and labor pools. While I would expect the same underlying principle still holds true, the proliferation of the internet and in particular mobile apps has added entirely new layers to such a theory.

On November 19, 2013, the Federal Trade Commission hosted an amazing hearing entitled: "Internet of things: Privacy & Security in a Connected World." The daylong hearing focused how advanced everyday technological devices such as appliances, consumer worn medical monitors, cameras and cars link with each other over the Internet via mobile apps. These everyday things can create, collect and transmit data to companies, other linked third parties and even health care providers. The panel observed, "a connected world raises the need for new, use-based approaches to data governance."

According to the presentation,

A CONNECTED WORLD RAISES THE NEED FOR NEW, USE-BASED APPROACHES TO DATA GOVERNANCE

cars connected to the Internet have been forecast to grow from 1 million in 2009 to more than 42 million in 2017. Jeff Haggins, Co-Founder and CTO for SmartThings observed that over 70% of the people worldwide have a smartphone. Mr. Haggins posited that this will lead to more mobile apps that control our physical world. A spokesperson from General Electric described a refrigerator that could sense a power outage and send a signal to your smart phone via an app and advise you if there is a potential food-safety hazard. The panel described a sleep sensor next to your bed, which detects your sleep patterns, anticipates when you will be waking up and transmits a signal to your coffee maker to start brewing your coffee. A medical monitoring device can be worn by a consumer and transmit real time information to a doctor's mobile device who can transmit instructions to order an increase in medication to address a condition. While not addressed in the presentation, in October, the Court of Justice of the European Union upheld a law requiring sheep and goats be fitted with tracking devices to record movements to deal with outbreaks of disease!

What became very clear during the presentations that such capabilities will and are revolutionizing every industry including, but not limited to: manufacturing, medicine, transportation systems, fitness, advertising and construction. In other words, the panel expanded upon the notion of "world hegemony" in the context of the interconnectedness involved in the gathering and sharing of personal data.

The panel quickly pointed out the personal benefits of the internet of things, when done correctly. The materials displayed at the hearing listed some benefits: support and improve our freedoms; make us safer, help us to be healthier; save time; save money; reduce waste; allow for extreme personalization; improve control; and provide greater choice. The panel also identified global implications such as optimization of resource management, the creation of jobs through standardization of best practices and increased health management and education and lower costs. All wonderful benefits, but they come at a price most consumers simply do not know.

As the panel progressed away from a description of how the data is created, it quickly moved into the privacy and security issues associated with the collection of such personal information. Senior Staff Attorney for Electronic Frontier Foundation quoted Justice Anthony Scalia, "In the home, all details are intimate." However, by using these connected devices in the home, virtually all things lose their intimacy and become public. Tien continued by expressing a very common held belief that very few consumers are aware of the depth of privacy issues associated with the use of such devices.

A key issue in discussing security involved a belief that there is very little push in the industry to truly make the data secure from unwarranted and unwanted uses. The FTC's core values associated with mobile app privacy are privacy by design, transparency, and providing the consumer with a clear choice. However, despite these core principles, many of the security breach issues, according to Tien, stem from consumer related actions. He particularly noted the consumer's propensity to be unaware of their surroundings when engaging in highly sensitive actions. For example, he suggested that consumers should generally avoid engaging in any banking activities as the sit in the local Starbucks and use the unencrypted wireless system.

Craig Heffner, a vulnerability researcher from Tactical Network Solutions explored other possible sources of security problems associated with mobile apps. Heffner, who joked that he "does not make things, he brakes them," (i.e., security) pointed out many smart phones do not have any security

OVER 70% OF THE PEOPLE WORLDWIDE HAVE A SMARTPHONE

because the vendors commonly leave back doors in the software. The vendors assert the reason for leaving the door open is to provide a means of providing tech support. The vendors argue that this common practice benefits the consumer. According to Heffner, the practice provides easy access to the most sensitive information contained on the phone.

Heffner also pointed out another reason for relaxed security; there is no financial incentive to increase the security. To the contrary, a company is financially incentivize to expand the features of a device and thereby decrease the security. Additionally, Heffner observed the human error associated with technology is another leading cause of security breaches. Heffner told an amusing story about a company that sold domain names to store data on its cloud. However, the company listed a domain name that it did not own. Heffner purchased the domain name and then explained he had the ability, by using the company's website, to obtain highly sensitive personally identifiable information from anyone who purchased the domain from him.

Vinton Gray "Vint" Cerf, the Vice President and Chief Internet Evangelist for Google, an American computer scientist, who is recognized as one of "the fathers of the Internet" shared his views of privacy. The very starting point for Cerf lead him to posit the question: "is privacy dead?" He then progressed to explain reasons for the loss of privacy. "Most of the experience with privacy is a result of our own behavior. Our social behavior is quite damaging to privacy".

"Technology has outraced our social intellect," Cerf said, pointing to the fact that the we are the ones to blame for the lack of privacy. In answering his question, Cerf said that privacy is not dead, but it has become harder to achieve.

The panel explored the privacy concerns associated with the consumers' use of health and fitness devices and apps. Anand Lyer, President and COO of WellDoc Communications outlined his concerns about the privacy and data security risks associated with the devices and apps. The first security concern for Lyer is the user. How many people have you shared your phone code with and who were standing around you at the time, are some of the questions he asked. Lyer found that the applications themselves do not engage in enough penetrating testing to insure security. He believes that 90% of mobile apps would fail if tested sufficiently. As with other panel members, he was critical of the number of times back doors are left open in the code. He recommended that best practices be followed when storing the data in a particular environment. Lyer found that the devices and the service providers failed to properly encrypt.

The hearing was enlightening and encouraging. Enlightening as I learned from some of the true leaders in our field about their vision for the future. Encouraging as I understood just how connectivity could be used for global benefits. My concept of world hegemony had been stretched to lengths I could not have imagined. The apps developed today connect us not just to each other, but to our physical surroundings…. and then back to us again. ❖

Adam Grant

Adam is the Chief Legal Contributor for App Developer Magzaine 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.

THIS WILL LEAD TO MORE MOBILE APPS THAT CONTROL OUR PHYSICAL WORLD