Building a Solid Foundation to Support The Internet of Things

by Merton A. Howard

The next building block in the connected world is being installed in a city near you. The opportunity to get in on the ground floor is exciting and innovative, but not without risk. Here, the City of San Francisco has partnered with SIGFOX to cover the City with a wireless network to be used by the Internet of Things (IoT). According to its October 27, 2015 press release:

"SIGFOX will deploy a dedicated IoT network that will provide low-cost, energy-efficient, and two-way connectivity for smart-city programs, as well as businesses in multiple verticals. A growing phenomenon in numerous cities across the world, the IoT connects physical objects and allows them to communicate, analyze, and share their data through sensors, network connectivity, and cloud software. San Francisco is the first of 10 U.S. cities in which SIGFOX will deploy its network by Q1 2016. SIGFOX, whose technology is already FCC certified, is currently operating or being deployed in 10 European countries and registers over 5 million objects in its network. By providing a disruptively cost-effective, energy-efficient, and simple way to connect the physical world to the Internet, SIGFOX enables the IoT to finally take off and connect large volumes of devices."

As for the City, Miguel A. Gamiño Jr., San Francisco's chief information officer and executive director of the Department of Technology, claims that "[t]his new network reinforces San Francisco's commitment to attracting startups and established companies in the emerging IoT space. It also allows the City to offer residents innovative new services and positions San Francisco as the leading smart city in the U.S."

This network has great potential to add to the foundation of the connected world, or IoT. The IoT connects physical objects embedded with sensors and actuators, allowing things to exchange data and communicate with each other. Garbage cans send notifications when full; an appliance calls for maintenance, or orders milk; a smoke alarm sends a text when the alarm goes off or it has a low battery; a beacon can locate a stolen item; a sensor placed on a valve provides an alert when a leak is detected. IoT applications are being used everywhere in every thing, from consumer personal fitness products, to farming equipment, Hello Barbie™ (who can have a two way conversation with a child), implanted medical devices,

transportation logistics, smart cities, and security cameras.

Companies participating in this rapidly evolving area should not overlook important regulatory and legal challenges in a world hungry for technology that is better, faster, smaller, cheaper, and connected all the time. Privacy and security issues are paramount, but there are other legal issues and risks to consider, including intellectual property protection, regulatory compliance, insurance, class actions, and product liability. Hacking is becoming more and more foreseeable, if not expected, so that risk must be managed. Other areas of concern include ownership and transfer of data, vendor contracts, terms of service, liability for first party property damage and data loss/corruption, and third party bodily injury and property damage claims. Moreover, there are product lifecycle challenges, including compatibility, updates, maintenance, repairs, corrective actions, and recalls. The bottom line is that IoT product manufacturers, distributors, and retailers face the same legal risks as any company in the chain of commerce for consumer products, medical devices, or industrial machinery. If the IoT is everywhere all the time, then IoT products and infrastructure will present more complex legal challenges than the traditional legal risks outlined above.

So what is a startup to do before it plugs into SIGFOX or any other network? In short, start with the basics. Take notice, get connected, and develop a plan for action. Look at the relevant government agencies, standards, and legal authorities. Identify the risks and adopt best practices on the front end, not after the fact. Get educated about privacy, security, and risk. Manage risk through best practices and insurance.

One place to start is with the government. While most government agencies have refrained from adopting new regulations for the IoT, a number of federal agencies have taken action or are quickly formulating positions based on their already existing authority. Most notably, the Federal Trade Commision (FTC) has advised that companies should build privacy and security into products and services at the outset, collect and keep only what is needed, provide clear and truthful notices and representations, and give consumers choices about data uses that are not obvious to them. These concepts are embodied in the January 27, 2015 FTC Report on the IoT, where the agency urges companies to adopt best practices to address consumer privacy and security risks. On its website, FTC provides additional guidance and advice for businesses about building security into products connected to the IoT, including proper authentication, reasonable security measures, and carefully considered default settings.

Other agencies that have taken notice include the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration (FDA). In 2012, NHTSA modified its research organization to focus on vehicle electronics, including cybersecurity. NHTSA established a new division, Electronic Systems Safety Research, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems.

In 2015, this new approach was tested when Fiat Chrysler Automobiles (FCA) submitted a safety recall report to NHTSA concerning a software security defect condition in approximately 1.4 million vehicles equipped with radios manufactured by Harman Kardon (Recall 15V-461). According to FCA, software security vulnerabilities in the recalled vehicles could allow unauthorized third-party access to, and manipulation of, networked vehicle control systems. Unauthorized access or manipulation of the vehicle control systems could reduce the driver's control of the vehicle increasing the risk of a crash or other harm. The story that led to this recall was featured in Wired: Hackers Remotely Kill A Jeep On The Highway – With Me In It. Today, hackers around the world seek to perform that same kind of disruption to all types of IoT products. Is your company ready to respond to the inevitable?

FDA has also taken steps to strengthen the cybersecurity of medical devices. This includes FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS)

Software." In July 2015, the agency issued its first cybersecurity alert. The alert concerned a connected pump, and warns health care facilities about security vulnerabilities in Hospira's Symbiq Infusion System (Version 3.13 and prior) that could allow unauthorized access to the device and interfere with its proper functioning. According to the alert, an unauthorized user could potentially access the pump remotely and alter the dosage it delivers, which could lead to overinfusion or underinfusion of critical patient treatments. Although the agency was unaware of any patient adverse events or unauthorized device access related to these vulnerabilities, FDA strongly encouraged health care facilities to transition to alternative infusion systems and discontinue use of this particular Hospira infusion pump.

Regulations, guidelines, and agency actions are starting places. But those government bodies move slowly compared to market forces and other legal pressures. A company wondering about how much time and money to put into IoT security and planning on the front end need only think about the long term cost of getting it wrong. Indeed, plaintiff class action lawyers are constantly watching and hunting for mistakes and opportunities to break new legal ground and win settlements. Hackers are doing the hard work for them. Meanwhile, consumers will be on the lookout for products that provide the proper balance of security and accessibility, at the right price. Those who find that balance will prosper. As cities such as San Francisco build out the foundational connections for the IoT, prudent companies will identify and address the legal risks within their initial framework, rather than wait for a text from the smoke alarm.

For more information, please contact:

Merton A. Howard, Partner
415-995-5033
mhoward@hansonbridgett.com