Circles and The Internet of Things

This article was originally published on Fox Business on June 5, 2014.

by Brian E. Finch

Brian E. Finch
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is co-leader of the firm's Global Security practice.

Growing up, the sacred text in our house was Consumer Reports, a/k/a "Consumers". Nary a television, home appliance, or automobile could be purchased without consulting the infallible guide to what was worth some hard earned dollars.

Personally, my obsession with Consumer Reports continues through today. Whenever I am thinking about buying an item or signing up for a service, I look online to see what got the coveted "recommended" ranking and what received the black circle kiss-of-death.

I was extremely interested then when I saw the recent issue of the magazine that took a look at internet connected devices for your house. In an article entitled "Run Your Home From Your Phone", the magazine examined a range of "smart" devices such as televisions, door locks, home alarm systems, and even washers and dryers. Just the type of reviews I expected and look for.

What really, caught my eye, however, was one of the factors Consumer Reports examined as part of its product review. Up front the article stated:

> *"At Consumer Reports, we put our experts in the labs and our investigative reporters to work to see which products can make your life easier, which fail at their basic function, **and which may leave you vulnerable.**"*

This was a fascinating and welcome acknowledgment of the rarely addressed security concerns linked to perpetual connectivity. Remote access to home appliances, devices, and other systems can bring a great amount of convenience, but they also can present a security gap ready for exploitation.

The Consumer Reports article noted some particular concerns, including:

- Merely securing your WiFi network is insufficient. You also need to make sure to check and enable the security settings of any devices added to your network.
- Privacy issues could lead to valuable information being sent to persons with malicious intent. Consumer Reports noted concerns about hackers checking to see whether your appliances had been set to "vacation mode" to know when you are out of town, or learning your daily schedule in order to tell when you are most likely to be out of the house.

These concerns are not academic. Consumer Reports noted that in one instance a coordinated attack led to "about 100,000 products, such as routers, TVs, and at least one connected refrigerator, sent out more than 750,000 phishing e-mails over

two weeks." The attack, detailed by security consulting firm Proofpoint, was apparently enabled by weaknesses in their basic protections or setup of the various devices.

To some, these kinds of vulnerabilities may be a surprise. Others are likely well aware of the potential problems posed by "smart" devices. In either case what is clear is that some sort of action needs to be taken by manufacturers, consumers, and news sources like Consumer Reports.

Let's break down what each vertical should be thinking about:

Manufacturers

When companies, especially smaller companies and start ups, are trying to navigate the valley of death between a great idea and profitability, security of their products tends to be at the bottom of the priority list. The N.Y. Times wrote an insightful article about this earlier this year, noting how start-ups are learning the perils of not making security a top concern. One person quoted in the article lightly noted that "[f]or many companies, a security breach would almost be a nice problem to have in some cases. It means you have enough customers for someone to care."

While a humorous, and in some ways true statement, it is reflective of the fact that many technologies being created today in an environment that focuses on reliability and usability, not security. That dynamic should change, and the sooner the better. Companies need to start integrating security concepts into their products at the earliest phases of design. If security is an afterthought, it almost assuredly will be marginally effective.

Similarly, companies also need to think about security from multiple perspectives, and that includes with respect to sourcing of components. Using inadequately vetted components can lead to products being released with vulnerabilities or malware embedded in them. This is not an unusual problem: defense contractors have faced this problem for years, as have some more sophisticated information technology vendors.

In the non-cybersecurity world, even marquis brands like luxury automobiles have faced this problem. One of my favorite car manufacturers, Aston Martin, had to issue a recall after discovering that counterfeit parts had been used in the assembly of its car, leading to possible problems with the gas pedal.

The bottom line then is this: security should be mixed into the DNA of "smart" products going forward.

Consumers

Somewhat in the vein of *caveat emptor*, or "buyer beware", consumers need to think about security when they purchase products or services. Much like a manufacturer, consumers need to consider the security of products, especially "smart" products, when making purchasing decisions.

What needs to be considered will obviously vary from product to product, but still consumers should ask some basic questions before they invest in new technologies, including smart technologies. Here are some examples:

- Does the product have any native security features?
- What does it take to activate/implement those features?
- What kind of cyber threats do those security features protect against?
- How well does the product integrate/interface with other security protections the consumer has available?
- What is the process for updating security features, and how often are security updates made available?

The last point can be an especially vexing one. Security updates or "patches" are often only available when a manufacturer releases them. It would seem to be good business sense for companies to quickly release security patches, but history has shown that not every company is fleet of foot in that regard. This is especially true when a third party is part of the process for releasing patches.

Consumers need to take all of these factors into account when making purchasing decisions going forward.

News Media

Every news outlet loves to have product review stories. Often colorful and insightful, the reviews often focus on issues such as ease of use, reliability, integration with other technologies, and of course whether the product is a value.

In the era of the "Internet of Things" and "smart devices", I would strongly encourage the media to start adding security to the list of features regularly reviewed. Product reviewers (who often are more technically adept

than the average consumer) should consider what level of security is offered by the product as well as whether it performs as intended.

Security Should Be Second Nature

The value of being connected to devices no matter where you are is clear. Being able to remotely turn on lights, monitor your home, or otherwise control devices you own can tremendously boost the convenience factor of your daily life.

However, you cannot take advantage of such tools without thinking about security. It has to be an integral part of the product, and people should be able to easily tell its security strengths and weaknesses.

This is not "helpful" information: it is in fact critical data to be collected. Just as cars are evaluated for their safety, products designed for perpetual connectivity to the world should be similarly evaluated. Failing to do so will not serve the consumer's interest, or ultimately the manufacturers.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | +1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP