Internet Of Things Is Not Immune From Internet Pitfalls

This article was originally published on Law360 on March 16, 2015.

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.

Investors, analysts, and tech enthusiasts alike are abuzz about the opportunities surrounding the "Internet of Things." The IoT represents the next frontier of Internet-connectable devices, with everything from watches and wristbands to refrigerators and light bulbs all being able to connect seamlessly to the Internet and interact with other devices.

The potential upside of such devices is nothing short of amazing: watches can display emails and other important information; lights can be turned on remotely and synced to music systems to create a home dance club; and your kitchen appliances can be programmed to alert you no matter where you are that you are low on butter.

Sadly, as with any other device that connects to the Internet, cyber-criminals are sure to quickly find exploitable security and privacy flaws in IoT devices, and thus transform them into yet another enabling tool for cybercrime.

This impending reality has not gone unnoticed in Washington, D.C. The Federal Trade Commission recently published a report outlining its privacy and security concerns related to the IoT. Rest assured that if the FTC took the time and energy to develop this report, it also means that they will be looking to make examples of IoT developers who do not make privacy and security a core function in their devices.

The worst thing an IoT developer can do at this time is ignore security and privacy concerns. For all the talk about cybersecurity generally, the development of IoT devices represents the first real opportunity to create a whole new class of products that are more secure from the start.

With that in mind here are some giant pitfalls that IoT developers can easily fall into, ruining their chances for creation of a successful product:

Not Paying Attention To Clear Messages From Regulators At Every Level of Government

Many people confuse legislative inaction with general inaction by government agencies. That simply is not the case. While Congress, state legislatures, and others endlessly debate new cybersecurity and privacy laws, regulators at all levels have been pressing ahead with new

rules using existing authority. This is not occurring by happenstance: Regulators are laser-focused on privacy and security. Ignoring the federal, state and international efforts to deal with IoT security and privacy issues would be a mistake.

Take, for example, the FTC, which in January 2015 issued a report, "Internet of Things: Privacy & Security in a Connected World." The report set forth a number of recommended steps businesses should take to enhance and protect consumers' privacy and security. Even though the report does not have the force and effect of law, it serves as a clear warning to IoT developers about the expectations of the FTC in this space. The report offers recommendations regarding data security, data minimization, privacy notices and consumer choice regarding collection of users' data.

IoT developers should also remember that regulatory agencies like the FTC are not shy about using broadly defined laws to address niche industry concerns. The FTC, for instance, has used its general consumer protection enforcement powers under the FTC Act, 15 U.S.C. § 45(a), regarding "unfair or deceptive acts or practices" to prosecute privacy and information security violations.

Last year, in its first action against a marketer of IoT products, the FTC approved a final order settling charges that TRENDnet engaged in lax practices that failed to prevent unauthorized access to sensitive consumer information, namely video and audio feeds from its home security cameras. IoT developers should not view the TRENDnet case as an "outlier," but rather as a sign of readiness to take enforcement actions should privacy and security failures abound. Other actions, like the encouragement of FTC commissioners to have state attorneys general monitor the IoT industry and to bring actions for privacy and security breaches under general state laws that may apply.

The FTC is not the only set of watchful eyes tracking the actions of IoT developers. California for instance has taken and active role in the privacy sphere by passing sweeping privacy legislation that can impact IoT devices. Additionally, companies cannot forget that the federal government is increasingly requiring information technology devices and systems to have high levels of security before they will be bought by the government. Federal procurement policy is rapidly changing to integrate security into contractual obligations, so companies that fail to have adequate security may see their government contract opportunities limited or even eliminated.

Valuing Reliability Over Security

An ironclad rule of capitalism is that if consumers don't like a product, they won't buy it. So it makes great sense that IoT developers focus their efforts first and foremost on creating IoT devices that customers will find useful and easy to use.

The value of security in IoT devices is much higher than many developers currently realize, however. This means that while many developers currently add security features at the final stages of development so as not to hinder ingenuity or reliability, that timeline will have to change. Implementing security at the end of the development process can result in security vulnerabilities slipping through cracks.

Instead, developers should consider security issues from the very beginning of product development—in other words, IoT "security by design." IoT stakeholders would also benefit from acknowledging the risk of a data breach or use of the IoT device to conduct a cyberattack inherent in a connected product and proactively developing an action plan in the event of a data breach or cyberattack.

With that point in mind, IoT developers should consider building in security from the start using the following principles:

- How can the company integrate security measures into the product as a way of enhancing the user experience?
- Has the company completed a privacy or security risk assessment?
- How will IoT devices be monitored for security vulnerabilities when they are out-of-date and new products are released?
- Does the company have a system in place to receive information about security flaws?
- How will software patches be released to users?
- What is the procedure for handling a data breach, and how will customers be notified?

Overlooking Internal Security Risks

Any well-thought-out security plan will include interior defenses as well as perimeter defenses. Indeed many cybersecurity experts agree that the "human factor" is often the most dangerous one when considering cyber risk profiles. In this case, this means IoT developers having on hand security policies that limit the possibility of internal mischief, as well as suffering harm thanks to the inadequate security practices of contractors and vendors.

Companies that handle data derived from IoT devices should consider the following issues about who has the data:

Who needs access to user data? Are there ways that access can be limited?

- Are there clear policies in place regarding employees' handling of user data? Do those policies have buy-in from all of the important stakeholders?
- Is the company providing reasonable oversight of employees' handling of user data?
- Has the company considered the data security policies of contractors and vendors?

Collecting as Much Data as Possible, Even When You Don't Need It

"Big Data" is all the rage—after all how can you "connect the dots" if you don't have dots to connect? The thinking further goes that if you collect enough dots, you will eventually find patterns that reveal useful—if not profitable—trends.

While that is entirely valid thinking, there is an underappreciated challenge associated with collecting as much information as possible—namely the more cybercriminals are constantly on the lookout for data to steal because they too can use Big Data analytics to create nefarious and illegal revenue generating operations. Further, companies often have so much data on hand that they don't necessarily manage it well, meaning that they repositories of information lying around that are likely unneeded for their own purposes, but could prove incredibly valuable to cybercriminals.

In the context of IoT devices, too much data presents a security and privacy threat. IoT devices could collect so much information that companies unintentionally sweep up "personally identifiable information," which then triggers legal and regulatory obligations for its protection. There are also the typical security concerns, namely that the information collected could be twisted into some sort of security threat (for example being used to create "social engineering" attacks).

With that in mind, IoT developers should consider the following components of a "data diet":

- Are the types of data being collected needed at this particular stage of design or implementation?
- Is de-identifying the data an option? Is there a legal obligation to de-identify consumer data?
- How long does the company need to keep the data to accomplish its objectives? When should the data be deleted?

There are other dangers that IoT developers can easily avoid with a little proactive planning, such as adopting clear and manageable security and privacy practices, and understanding notification and disclosure obligations imposed by federal and state laws, regulations, and contract language. If you want to avoid these pitfalls, start asking critical questions about the security and privacy implications of your IoT device from inception through implementation.

Whatever the case may be, the simplest point is that IoT developers must take security and privacy seriously as they bring their offerings to market. It still may be the "Wild West" when it comes to cybercrime, but regulators, legislators and law enforcement are all sufficiently on notice of the problem now, and newcomers to the scene will be viewed with suspicion. In other words, IoT developers are very likely to face high levels of scrutiny with respect to the privacy and security practices, so it will be worth their time and effort to get those policies right from the start.

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

Pillsbury Winthrop Shaw Pittman LLP