Client Alert

pillsbury

Corporate & Securities - Technology

Corporate & Securities | Antitrust & Competition

Privacy, Data Security & Information | Cybersecurity Task Force

February 12, 2015

How to Fail in the Internet of Things

By Brian Finch, Roxane Polidora, Catherine Meyer, Lindsay Lutz and Philip Shecter

Innovation is prized in the growing space of the Internet of Things (IoT). But an innovative product design is not enough, and potential pitfalls abound. As demonstrated in a report published by the Federal Trade Commission (FTC), privacy and security need to be at the forefront of developers' minds. Here are five lessons on what **not** *to do when developing a connected product.*

The Internet of Things is an expanding ecosystem of everyday objects that are embedded with technology, allowing them to connect, communicate and transfer information about users and their surroundings to each other. IoT products boast beneficial effects such as increasing economic productivity and efficiency, encouraging robust innovation, and tailoring user experiences. However, by virtue of being connected to the Internet, IoT products also carry privacy and security risks. On January 27, 2015, the Federal Trade Commission published a report focusing on privacy and security concerns for IoT devices sold to consumers.

Given the growing interest in how embedded computing advancements affect security and privacy issues, this Alert identifies what developers, investors and entrepreneurs should avoid when entering the IoT market.

1. Ignoring Washington, Sacramento and the European Union.

Much has been written about how privacy and security laws are outdated and have not been able to keep pace with rapidly changing technology. While legislatures may not have succeeded in updating statutes, regulators are laser-focused on privacy and security. Ignoring the federal, state and international efforts to deal with these issues would be a mistake.

Indeed, the FTC has made embedded computing a top focus. In January, the FTC issued a report, *Internet of Things: Privacy & Security in a Connected World*, that recommended steps businesses should take to enhance and protect consumers' privacy and security.[1] While the report is not formal legislation, it serves as a 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. The FTC also recommends that data security legislation be enacted by Congress.

[1] FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 27, 2015).

Even without IoT-specific legislation, developers should understand how technology-neutral laws are being enforced in the IoT context. 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 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.[2] Failure to comply with the FTC report's recommendations could result in FTC enforcement activity. FTC Commissioner Brill has also encouraged state attorneys general to monitor the IoT industry and to bring actions for privacy and security breaches under general state laws that may apply.[3]

While the IoT industry is in its early stages and IoT-specific legislation has not materialized, stakeholders in IoT devices should also keep abreast of developments in general data security and privacy legislation. Certain states like California have taken active roles in the privacy sphere and have passed sweeping privacy legislation that can impact IoT devices. Consumer class action plaintiffs and their attorneys are clearly paying attention to these developments, as evidenced by the onslaught of cases being filed. 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.

To the extent the IoT device is marketed internationally or if it is intended for travel, developers should also be familiar with privacy and data security regulation in other countries in which they are operating and where the IoT device is likely to be used. The European Union, for instance, has very restrictive privacy laws and, under new amendments, Member State regulators have the ability to issue fines up to 5% of global revenues.

2. Treating security as an afterthought.

It may be tempting to add security features to a device at the final stages of development so as not to hinder ingenuity or innovation in the early stages. This approach, however, may allow for more security vulnerabilities to slip through the cracks than if security were considered at every stage of the design cycle. 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 cyber-attack inherent in a connected product and proactively developing an action plan in the event of a data breach or cyber-attack.

In the TRENDnet case mentioned above, the FTC alleged that faulty software for home security cameras left the live feed from the cameras open to online viewing by anyone with the camera's Internet address.[4] When, according to the complaint, a hacker exploited this flaw and posted links to the live feeds to certain cameras (including babies asleep in their cribs and young children playing), it appears that the company did not have a way to repair the security flaw without forcing users to visit the website and download a software patch.[5]

[2] Press Release, FTC, FTC Approves Final Order Settling Charges Against TRENDNet, Inc. (Feb. 7, 2014).
[3] Julie Brill, FTC Commissioner, Remarks at Conference of Western Attorneys General (July 21, 2014).
[4] FTC Press Release, *supra* note 2.
[5] *Id.*

Stakeholders should think about these security issues from the start:

- 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?

3. Overlooking internal security risks.

While a "security by design" approach to developing an IoT product is essential, it is not foolproof. Developers need to think about security threats not just by hackers, but by their own employees and vendors. As the FTC report explains, companies must ensure that "personnel practices promote good security" and that "product security is addressed at the appropriate level of responsibility within the organization."[6] In addition, companies should consider the security practices of their 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?

4. Collecting as much data as possible, even when you don't need it.

Data collection is a powerful tool for analyzing behavior, developing innovative products and providing valuable insights to users. Collecting and retaining large amounts of consumer data, however, can present a more attractive target for data thieves. When a large variety of data is collected, it also increases the risk that some of the data that is collected will be used in ways contrary to consumers' expectations.

While data minimization in the IoT context is challenging because a new use for data may be just around the corner, the FTC has encouraged companies to have data practices and policies that impose reasonable limits on consumer data collection and retention in light of that company's business needs. One option to reduce privacy concerns is to immediately de-identify the collected data so as to minimize harm if there is a data breach.

[6] FTC, INTERNET OF THINGS, *supra* note 1, at 29.

Developers should consider:

- 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?

5. Believing that what users don't know won't hurt them.

The IoT presents many challenges to traditional consumer protection methods of notice and choice. For certain data collection that is consistent with the consumer's expectations, providing choices for every instance of data collection may be overly burdensome to the consumer and not necessary to protect privacy. However, where the data being collected is sensitive in nature or beyond what a user might expect to be collected, developers should consider methods to provide users with notice and choice regarding data collection. The provision of notice to consumers about what data is being collected and with whom it is being shared is governed by a labyrinth of privacy regulations.

As to providing notice and choice to users, developers should consider:

- Is data collection limited to data consistent with the context of the consumer-device interaction?
- Are the company's privacy policies and terms and conditions of use customized, up to date, clear, prominent and written in a way that is understandable to consumers? Has the company resisted the urge to cut and paste "boilerplate" policies used by others in the space?
- When and how are notifications regarding collection of data provided?
- In what situations will the company request users' express consent before their sensitive data is collected?
- What options will users be given to control privacy settings?

****

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.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Brian Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Roxane Polidora (bio)
San Francisco
+1.415.983.1976
roxane.polidora@pillsburylaw.com

Catherine Meyer (bio)
Los Angeles
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Lindsay Lutz (bio)
San Francisco
+1.415.983.1255
lindsay.lutz@pillsburylaw.com

Philip Shecter (bio)
San Francisco
+1.415.983.1006
philip.shecter@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.