The Internet of Things: Promises and Perils for Traditional Product Makers

Paul J. N. Roy
Julian Dibbell

Paul J. N. Roy
Chicago
+1 312 701 7370
proy@mayerbrown.com

Julian M. Dibbell
Chicago
+1 312 701 8237
jdibbell@mayerbrown.com

According to some reports, the Internet of Things originated in 1982, when computer scientists at Carnegie Mellon University added sensors to a campus Coke machine and connected it to the local network so they could check how many Cokes were left without leaving their workstations. Primitive though it was, that experiment offered a glimpse of the efficiencies that a world of similarly connected devices—an Internet of Things (IoT)—might someday bring. Today, the world's economies are brimming with Internet-connected devices, some 5 to 10 billion of them, growing toward a predicted total of 40 billion by the year 2020. At scales like these, the promise of IoT comes into sharp focus: Combining massive connectivity with the big data that flows from it, those billions of connected devices are sending constant updates on their use, and their users, back to businesses for analysis, with the potential for vast savings and profits to result.

The FTC outlined three main categories of measures that businesses should take to protect against privacy and security risks in connected devices: (i) security by design, (ii) data minimization and (iii) notice and consent.

In short, the Internet of Things is not just for computer scientists anymore. Nor, for that matter, is it just for technology companies. If anything, the IoT holds its greatest promise for businesses selling the kinds of relatively low-tech products—automobiles, manufacturing tools, home appliances, hospitality services—that are most likely to be transformed by an injection of smart, connected technology. But if the Internet of Things is a particularly compelling proposition for these types of businesses, it also exposes them to a peculiar set of risks.

Generally speaking, the perils of Internet of Things technology stem from the same core issues that create its promise: connectivity and data. Connected devices can be remotely hacked and turned against their legitimate users. Additionally, the massive collection of data invites misuse of that data, both by hackers and by the businesses that collect it. While these threats face any business that chooses to adopt IoT technology, the makers of traditional, mass-produced goods are in some ways particularly vulnerable to them. For one thing, such businesses are typically larger and more established than tech companies, with high profiles and broad consumer bases that make them especially attractive targets for hackers. At the same time, however, they typically lack the tech companies' native capacity to assess and defend against cybersecurity and data risks and lack experience dealing directly with consumers who normally purchase their products through third parties. Borrowing some of that expertise, whether by partnering with or hiring technology vendors, will often make sense for a conventional product maker venturing into IoT. But doing that in turn creates the potential for complications—cultural frictions, misallocated risks—that comes with any such relationship.

None of which is to say that conventional product makers should resist exploring the Internet of Things. But to make the most of its promise, they should take care to understand its perils—and how best to guard against them.

Knowing the Risks

Connecting products to the Internet of Things creates an array of legal risks, including enforcement actions by regulators like the Federal Trade Commission (FTC), lawsuits by other businesses and class actions by consumers. As varied as these risks may be, however, they all essentially revolve around the two core issues of connectivity and data.

CONNECTIVITY RISKS

The chief risk created by connecting a product to the Internet is that a third party—neither the authorized user of the device nor the business that produced and still communicates with the device—will use that connection to gain unauthorized access to the device.

The consequences of such an attack can be drastic. The intruder may gain not just access but control of the product, in which case the potential damage to life and property may be limited only by the nature of the product. Among threats to consumers, vulnerabilities in connected automobiles have lately made dramatic headlines, focusing on the ability of hackers to remotely cut the brakes or the power on some late-model cars. But there is evidence to suggest that the threats to business and manufacturing (where more than 40 percent of connected devices are deployed) are at least as formidable. Famously, for example, the first cyberattack to physically damage a connected device was the Israeli government's alleged deployment of the so-called Stuxnet computer worm to incapacitate an Iranian nuclear reactor. And last year, hackers managed to gain control of a German steel plant's blast furnace, doing serious damage to it in the process.

> Generally speaking, the perils of Internet of Things technology stem from the same core issues that create its promise: connectivity and data. Connected devices can be remotely hacked and turned against their legitimate users.

Moreover, physical damage is not the only kind of damage a cyberattack on a connected device can inflict. Sensitive personal data can be stolen directly from connected devices used by consumers. Trade secrets and other sensitive commercial data can be lifted from devices used by businesses.

Nor does the damage have to be done by third parties, or even with intent to do harm. Manufactured products have always been subject to dangerous malfunctions. In connected devices, the complexity of embedded software creates an added layer of susceptibility to malfunction. The fact that such software can be updated remotely creates further opportunities for things to go unintentionally wrong.

DATA RISKS

Seeking to maximize the value of the personal or commercial data collected from connected devices, businesses may collect kinds or amounts of data that the data subjects did not consent to share, or did not expect to share given the vagueness or generality of the language they did consent to. Businesses may also put the collected data to uses the data subjects do not believe they agreed to. Overstepping the bounds of consent in any of these ways can give rise to privacy violations (for personal data) or to breaches of trade secrecy or confidentiality (for commercial data).

Conversely, if data collected by a business shows ways to improve the safety or reliability of the product, and the business fails to perceive or to act on that evidence, that failure could be held against it in a later product liability suit.

Mitigating the Risks

In a recent report on the Internet of Things, the FTC outlined three main categories of measures that businesses should take to protect against privacy and security risks in connected devices: (i) security by design, (ii) data minimization and (iii) notice and consent. Taking effective measures across all three categories should weigh in a business's favor in any enforcement action by the FTC. It may also cut short any private claims brought for breaches of privacy or security.

SECURITY BY DESIGN

Businesses should ensure that security measures are built into the device from the outset, and that any outside vendors hired for the purpose can and do build them in.

> The chief risk created by connecting a product to the Internet is that a third party—neither the authorized user of the device nor the business that produced and still communicates with the device—will use that connection to gain unauthorized access to the device.

As part of such built-in security measures, businesses should also ensure that the device's software can be remotely updated for security purposes, and should secure any end-user consents required to do that lawfully throughout the life cycle of the device. That said, however, businesses should recognize the unique challenges involved in implementing remote updates of connected devices. Compared to more conventional computing devices, such as desktop and laptop computers or smartphones, IoT devices may be connected to the Internet sporadically. For connected devices that are particularly durable goods—tractors with product lives of 20 years, for example—the software or associated hardware embedded in the device may eventually become so obsolete that it cannot be updated at all. (Similarly, any outside vendor hired to manage the device's security may become unavailable before the device goes out of service.)

For these reasons, businesses should not rely entirely on the ability to update devices. Rather they should ensure that a device's on-board security is as robust as it can be before shipping, and anticipate the need to offer component retrofits to enable continued updates.

DATA MINIMIZATION

In collecting data through connected devices, businesses should collect and retain only as much of it as the business has an immediate use for. Minimizing the amount of data retained will minimize any risks associated with data retention, including data theft, misuse of data, and failure to act on data.

NOTICE AND CONSENT

Businesses should ensure that a connected device's end users have adequate notice of the uses their data will be put to and that they consent to that use.

This may be easier to do where the end users are other businesses rather than consumers. For one thing, consumers will be more likely to look for any relevant notice on the device itself, which, for devices without conventional interfaces, may not be an opportune place for it. Businesses, on the other hand, will tend to be more attentive to and sophisticated about any terms of use presented. Moreover, to the extent that the terms appear to claim rights not normally retained by the manufacturer of a conventional consumer product, such notice may create reputational costs for the business. Thus, for consumer-facing products, businesses should rely more on data minimization than on notice to offset the risk of exceeding the data subject's consent. ◆