Dumb Devices Smarten Up, Widening Data Security Enforcement Net

Jimmy H. Koo

December 27, 2017

Traditionally “dumb” products, such as toasters and light bulbs, are increasingly gaining internet connectivity, becoming “smart” internet of things devices with ongoing data security obligations, privacy and security professionals and attorneys told Bloomberg Law.

“Devices that previously weren’t collecting consumer information now are, and as a result, the FTC may bring enforcement cases against companies that previously wouldn’t have faced privacy or data security enforcement cases,” Phyllis Marcus, a privacy partner at Hunton & Williams in Washington, told Bloomberg Law.

Businesses making IoT devices must build in and maintain reasonable security measures for their products to survive possible Federal Trade Commission scrutiny, attorneys said.

The FTC has brought more than 500 privacy and data security enforcement cases. It settled its first IoT enforcement action in 2014 and has since brought three additional IoT-related cases involvingASUSTeK Computer Inc.'s routers, D-Link Corp.'s routers, and Lenovo Inc.'s computers. ASUSTeK and Lenovo entered into no-fault agreements, but the D-Link case is ongoing. A typical FTC settlement involves long term changes to companies’ policies and practices, and agreeing to independent compliance audits for a 20-year period.

The projected increase in IoT devices will present more possible enforcement targets for the commission in the years ahead.

The number of connected devices in use worldwide is expected to rise from 8.4 billion in 2017 to 20.4 billion in 2020, with the present $94 billion IoT market expected to grow to $117 billion by 2021, according to Bloomberg Intelligence reports. It doesn’t take much to convert a dumb device into a smart device, Bloomberg Intelligence Analyst Woo-Jin Ho told Bloomberg Law.

This explosion of IoT devices and the breakneck speed of technological innovation mean that companies must regularly update their security measures and policies. Although most companies

have well-defined security measures and policies, a "constantly changing technological environment means they are often playing catch-up," Bloomberg Intelligence Analyst Jawahar Hingorani told Bloomberg Law.

For a hacker, an internet of things (IoT) device such as a smart phone is "a one-stop-shop to traverse interconnected applications and control vulnerabilities," Peter Tran, general manager and senior director in the worldwide advanced cyber defense practice at RSA Security in Boston, told Bloomberg Law.

Regardless of whether a company is a connected devices startup or a technology veteran, such as smart buildings promoter Microsoft Corp. or light bulb pioneer General Electric Corp., the FTC will hold them to the same reasonable security standard, Kevin Coy, a privacy partner at Arnall Golden Gregory in Washington, told Bloomberg Law.

But what constitutes reasonable security in terms of what the FTC requires of IoT makers remains undefined. The commission lacks general rulemaking authority, so companies and attorneys must figure their compliance obligation based on the language of enforcement actions and public statements by FTC commissioners and staff. This uncertainty as to what may be considered reasonable security can be frustrating for IoT companies, but it also means there may be data security wiggle room in the case-by-case approach.

Sensitive Data

Connected devices may collect extremely sensitive data, such as health data gleaned from wearable fitness trackers.

A common focus in IoT-related FTC enforcement cases is that these devices were collecting and handling the most sensitive information about consumers, FTC Division of Privacy and Identity Protection Associate Director Maneesha Mithal told Bloomberg Law. The first FTC enforcement action involved private video images from family home surveillance cameras, commonly known as nanny cams, that were made publicly available online.

Smart devices have the potential to put sensitive data even more at risk because they can expose vast amounts of such information.

Due to the sensitive nature and the large amounts of data collected, the FTC "perceives a greater amount of consumer harm resulting from inadequate privacy or security with a smart device than a dumb device," Elliot R. Golding, privacy and cybersecurity partner at Squire Patton Boggs LLP in Washington, told Bloomberg Law.

If a device is connected to the internet, it is most likely processing data, and companies must consider what security processes and controls are in place to protect that data, Tran said.

The FTC isn't demanding cybersecurity perfection from IoT companies, however. "The FTC has indicated an expectation of reasonable security built in by design and maintained during reasonable lifespan of the product," Lisa Ropple, privacy and data security partner at Jones Day in Boston, told Bloomberg Law.

Continuous Process

Even with reasonable security measures built into IoT devices by design, companies must address cybersecurity as a continuous process that needs to address constantly-evolving threats.

Companies should be wary of static baseline security for IoT, because it is hard to predict the kinds of security that will make sense in the future, Julian Sanchez, a technology, privacy, and civil liberties senior fellow at the Cato Institute, told Bloomberg Law.

Consumers rely on companies to patch vulnerabilities as new cybersecurity threats emerge, but companies normally don't continue doing so forever. Notifying consumers when security update services end is a basic obligation.

To account for the evolving nature of cyberthreats, companies should conspicuously notify consumers if they plan on discontinuing certain products or security updates, Ropple said.

The FTC is particularly worried about companies stopping security updates.

Companies need to "keep a finger on the pulse and roll out patches, and updates" for devices after purchase, and ensure that their consumer privacy and security promises are correct and maintained, Mithal said.