'Smart' Ways To Avoid FTC Internet Of Things Scrutiny

Alysa Z. Hutnik

April 12, 2016

Connected devices have existed in the marketplace in one form or another for decades (think vending machines or weather sensors). Yet, a confluence of forces in recent years has helped spur a mass proliferation of technology in the "Internet of Things," and with it, the collection and analytics of big data. Demand is high to connect nearly everything to the Internet — from smart home platforms and connected cars, to wearable devices and even smart yoga mats. Analysts predict that the number of IoT devices will reach between 25 and 200 billion devices by 2020.

For such an ubiquitous topic, the IoT can be surprisingly difficult to describe. At a basic level, the IoT is an ecosystem of physical objects connected to the Internet generally featuring small, embedded sensors relying on wired and wireless technologies that collect and transmit data either passively or actively. The Federal Trade Commission, the nation's top consumer protection cop, defines the IoT as "the ability of everyday objects to connect to the Internet and to send and receive data," that includes both consumer- and nonconsumer-facing devices.[1] As the IoT has continued to grow into new and emerging areas, so too has FTC scrutiny.

In the *Law360* article, 'Smart' Ways To Avoid FTC Internet Of Things Scrutiny', partner Alysa Hutnik addresses recent enforcement matters and lessons learned from the FTC's report, "Internet of Things: Privacy and Security in a Connected World." She also provides a list of several key issues to consider when developing and marketing a connected or "smart" device.

To read the full article, please click here. Access may require a subscription.