wiley

NEWSLETTER

The DOJ Addresses The Internet of Things, National Security and Surveillance

October 2017

On October 10, Deputy Attorney General Rod Rosenstein, the No. 2 official at the U.S. Department of Justice, delivered remarks expressing concern about the Internet of Things. He made clear that the federal government remains committed to getting electronic data to solve crimes, and observed that the tech community must be prodded to strike a different balance: "Technology providers are working to build a world with armies of drones and fleets of driverless cars, a future of artificial intelligence and augmented reality. Surely such companies could design consumer products that provide data security while permitting lawful access with court approval."

A few areas stand out for the IoT and the tech industry.

First, Mr. Rosenstein expressed serious concerns about IoT security. In describing the 2016 Mirai botnet attack, he found "especially worrisome" that the attack "used simple Internet-connected devices, such as cameras and digital video recorders. Those so-called 'Internet of Things' devices" he said, "are easily susceptible to control by hackers because of the widespread use of default passwords and other failures to secure them." From that attack and others, DOJ has drawn the lesson that "our digital infrastructure ... can be hijacked and used against us as an attack vector. The possibilities for such attacks will grow. Estimates reveal that 6.3 billion Internet-connected devices were used in 2016. The total may reach 20.4 billion by 2020. Imagine the possible attack vectors if all of those devices employed default passwords." This sentiment is consistent with prior federal government observations that raise concerns about the broad security implications from IoT devices' widespread use.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Second, the Deputy Attorney General observed that innovation may outpace law and be inconsistent with public safety. "The digital infrastructure is not always constructed with adequate regard for public safety, cybersecurity, and consumer privacy," Mr. Rosenstein said. He also observed that "the tools we use to collect evidence run up against technology that is designed to defeat them," including but not limited to encryption and corporate decisions to store "evanescent" data overseas.

Third, he characterized the interests and behavior of tech executives as counterproductive. "Technology companies operate in a highly competitive environment. Even companies that really want to help must consider the consequences." This is true, given litigation risks, challenges in protecting shared information from public disclosure, and the possibility of public criticism here and abroad. The Deputy Attorney General laments that "the government's efforts to engage with technology giants on encryption generally do not bear fruit. Company leaders may be willing to meet, but often they respond by criticizing the government and promising stronger encryption." He predicts that "[t]echnology companies almost certainly will not develop responsible encryption if left to their own devices. Competition will fuel a mindset that leads them to produce products that are more and more impregnable."

The private sector should be attuned to DOJ's views on these issues as they develop innovative products and services, knowing that they may be called on to assist the government. As DOJ made clear in its litigation against Apple for help unlocking an iPhone, it will not shy away from using all the tools at its disposal to promote its view of public safety. At the same time, DOJ, as well as state and local law enforcement, should consider how to engage and find common ground with the private sector on these tough issues.