CORPORATE COUNSEL
An ALM Website
corpcounsel.com | January 10, 2019

Q&A with O'Melveny's Steve Bunnell: Cyber Risks Associated With Internet of Things

"I think there is a growing sensitivity among the Googles and Facebooks of the world. But I don't know if the people who make refrigerators are that concerned," says O'Melveny partner Steven Bunnell on the cybersecurity of the internet of things.

By **Dan Clark**

The internet of things is a term used for everything from cars to refrigerators that consumers can put their personal data into and connect to the internet. With more products connecting to the internet comes more issues for cybersecurity experts and data privacy attorneys.

Steven Bunnell, a partner in **O'Melveny & Myers**' Washington, D.C., office and the former general counsel of the Department of Homeland Security, spoke to Corporate Counsel about data privacy as it relates to the internet of things and types of litigation manufacturers could face as more household products are able to connect to the internet. This conversation has been edited for brevity and clarity.

Steve Bunnell, partner at O'Melveny in Washington, D.C.

Corporate Counsel: **Are the data privacy implications something that in-house attorneys for companies that create "smart" products are thinking about?**

Steve Bunnell: The privacy landscape is rapidly evolving with technology. Any one of these devices taken alone may not seem like a major intrusion into one's private realms. When you aggregate it all together, there is a pattern of life that can emerge and feel very "Big Brother-y." I think there is a growing sensitivity among the Googles and Facebooks of the world. But I don't know if the people who make refrigerators are that concerned. I think the popular feeling is that the collection and use of this data is going to evolve.

CC: With these "smart" products, should companies be worried about class action or other kinds of litigation if customers' data is hacked into?

SB: I'm not aware of any traditional class action involving these products. That doesn't mean there hasn't been some. There are a lot of issues that need to get sorted out in terms of the standing or injury-related issues. How concrete does the privacy harm need to be before it becomes legally actionable? Is it just the potential that your personal information is out there and someone could misuse it, or do you have to show that it has been misused? Related to that is a causation question. If there is some misuse, how do you know it came from that particular breach as opposed to another breach?

Those issues are out there generally. I think in the internet of things context they're even harder because the causation issues are more complicated and the audit trail that is left behind with these devices tends to be minimal. I think those cases may be a little bit further down the road in terms of the traditional privacy class action suits.

CC: What kind of suits do you think are more immediate with products like these?

SB: I think what is perhaps a little more immediate are internet of things issues that result in physical harm. The harm isn't that your personally identifiable information has been breached; for example, it's that the hospital emergency room has been shut down by an attack launched by a bunch of "smart" baby monitors that were hacked and were used to send messages to the hospital's computer all at the same time. Then a ransomware demand is made to the hospital. That is the kind of case that I would expect to see at some point in the near future. The internet of things is also the internet of potential physical harms. The stakes are now much higher for cyberattacks in this realm.

CC: Do you think that companies that create these products need to begin taking a more serious look at cybersecurity in those products?

SB: Absolutely. But how that is going to happen I think is the real question. Historically, these are not expensive devices. They're little computers in a sense, and they're very cheap. So there is no capacity to patch them or upgrade them the way you would a normal network. One of the real challenges is software patching once these items are out in the marketplace. I think there has been a lot of encouragement from the government and consumer groups to build security in the front end. That will increase the price of them.

The other challenge around them is that a lot of these devices are not produced in the U.S. DHS put **out a report** that is a reflection of this kind of nudging approach that the federal government has taken in this space. I think the effect of that over time is that it has a way of shaping the standard of care. Right now, the law in this space is kind of a reasonableness standard. What that means in practice is something that a judge or regulator has to figure out.

That's a common-law process as much as a dictated process, and I think it's sort of frustrating for companies because they don't have clear guidance on what is required of them. I think insurance companies will play an important role in this space. Using the incentive of perhaps lower premiums or the stick of refusing to offer coverage, insurance companies can shape cybersecurity practices in this area.

***Dan covers** cyber security, legal operations and intellectual property for Corporate Counsel. Follow him on Twitter @Danclarkalm.*