Internet of Things - Part 2: *Dogs, Cameras, and Cybersecurity*

Prepared by:
Matt C. Acosta and Sara Hollan Chelette
Jackson Walker LLP

LORMAN®
Published on www.lorman.com - August 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Internet of Things Part 2:
Dogs, Cameras, and Cybersecurity

Written by Matt C. Acosta and Sara Hollan Chelette – 6/28/18

I recently purchased an Internet Protocol (IP) camera to monitor my dog, Ruben, during those times that he has free reign of the house. Since "RubenCam" has been online, I'm not sure he has been any less rambunctious, but I'm certainly less anxious over whether—at any given moment—my things are making their way to the floor. It is reflective of the times that I put a significant amount of thought into the data security of my RubenCam before purchasing. Ultimately, my reduced anxiety prevailed over the risk of evildoers gathering classified information about my dog.

However, for many consumers the stakes are much higher, the data more sensitive, and yet for years little thought was given to its security. Surely device manufactures and the government had it covered, right? Based on current events, maybe not, but we are making some progress. And as it happens, devices such as my RubenCam have played a critical role in the ongoing journey to true cybersecurity in the age of the Internet of Things.

What Does the FTC Have Against Cameras?: The Murky Waters of United States Cybersecurity Regulation

IP cameras have served as one test case for U.S. cybersecurity regulation. Those within, or considering entering, the IoT space would do well to avoid the cybersecurity pitfalls experienced by early IP camera manufacturers. These devices were some of the first members of the IoT category and have been largely marketed for home and business security. For more than a decade, demand for these devices has steadily grown. A quick search on Amazon revealed over 30 different companies now selling these devices.

With increasing market presence comes greater responsibility. Or so says the Federal Trade Commission (FTC). Over the past several years, the FTC has taken a series of regulatory actions against IoT device manufacturers, including several against IP camera companies. Oddly, these cases are founded largely on allegations of false advertising rather than any breach of cybersecurity standards. This is primarily because a comprehensive set of cybersecurity standards don't yet exist in this country. One of the earliest of these enforcement cases was against TRENDnet, a manufacturer of an array of wireless surveillance equipment.[1]

TRENDnet sold its cameras under the tradename "SecurView" and advertised that they could be used to monitor "babies at home, patients in the hospital, offices and banks and more." Users of these cameras were required to establish a username and password in order to gain access to their personal encrypted feed. Nevertheless, in

January 2012 a few hundred of these cameras were hacked and their live feeds compromised.

The FTC filed a complaint against TRENDnet focusing on its *advertisements* that boasted the safety and security of its system. The FTC alleged, under its power to prevent misrepresentations to consumers, that TRENDnet "falsely represent[ed] that it had taken reasonable steps to ensure that its IP cameras and mobile apps [were] a secure means to monitor private areas of a consumers home or workplace." It also alleged that TRENDnet misrepresented that "it had taken reasonable steps to ensure that a user's security settings on its devices would be honored." Essentially, these complaints were based on TRENDnet's failure to bolster its data security by using freely available security and encryption software and failing to take reasonable steps to investigate potential security vulnerabilities, while all the while assuring customers of the safety and security of its system.

Shortly after the case was filed, an agreement was reached whereby TRENDnet was required to take a number of very expensive actions very quickly, including among other things:

- Remove advertising regarding the security of its products;
- Establish a comprehensive security program to address potential cybersecurity risks through a specific eight-point plan that includes requirements for dedicated data security personnel, code and security architecture reviews, active risk assessment and testing; and

- Obtain regular third-party security audits and submit compliance reports to the FTC for a number of years.

With its gaze now focused on IP cameras, the FTC next challenged D-Link, another camera manufacturer, and their advertised "secure" cameras.[2] Not one to take things lying down, D-Link pushed back, arguing that the FTC lacked the legal authority to police "misrepresentations" about the security of its IP cameras without first adopting specific standards lending guidance to device manufacturers. Unsurprisingly, the Court found that "[t]here can be no serious question that data security is a new and rapidly developing facet of our daily lives, and to require the FTC in all cases to adopt rules or standards before responding to data security issues faced by consumers is impractical and inconsistent with governing law." Many other courts have agreed.

To summarize, the FTC has the power to go after your company for breaching cybersecurity standards that don't exist. And the FTC's authority has only grown. It now has many tested arrows in its quiver to enforce its own—not entirely clear— view of cybersecurity compliance. The FTC has used this authority on numerous companies offering a wide variety of services, including creators of mobile applications, television manufacturers, hotels, and wireless router manufactures among others. These cases can serve as some of the best guidance for cybersecurity compliance in the United States. Thus, even though the waters are murky, there are still plenty of things that players in the IoT market can do to avoid the attention of the FTC. The first being, don't oversell the security of your devices.

Meanwhile, in Europe: The General Data Protection Regulation (GDPR)

Unless you have been ignoring all forms of news and social media, you know that the GDPR became effective on May 25, 2018. The GDPR is the European Union's (EU) current attempt to create generally applicable cybersecurity standards. It has a greatly increased territorial scope over previous European standards. These new regulations apply to those who are processing personal data in the context of businesses established in the EU, as well as to those *not physically present* in the EU who offer goods or services to, or monitor the behavior of, data subjects in the EU. "Data subjects" refers generally to those whose data is being collected. Thus, the GDPR would apply to a company that markets and sells an IoT refrigerator to data subjects in the EU, even if it is a U.S. company, because it has both offered goods to a data subject in the EU and is monitoring data subjects in the EU (e.g., it knows when you have run out of milk).

One particularly tricky area of GDPR compliance for IoT devices is how to properly communicate to data subjects what personal data is being collected, how it is being used, who it is being shared with, how long it being retained, and other GDPR-required disclosures that are typically made in a website's privacy policy. The Article 29 Working Party—the GDPR's regulatory Board—has recognized that any method chosen to provide these disclosures must be appropriate under the circumstances. Once again, this is a relatively murky standard. For IoT devices, it may be necessary to provide a privacy statement in hard copy instruction manuals, a link to a URL website address displaying

an online privacy statement, or even using a QR code that, when scanned, displays the required disclosures.

Further, because IoT devices are particularly intrusive (they may know more about your life than you do), the Article 29 Working Party has recognized that, in most cases, direct consent from consumers will be required. Obtaining consent can be challenging. It is far more difficult for a refrigerator to make the required disclosures and to ask a someone for consent than it is for a website or a mobile application. Thought must be given to what is "appropriate under the circumstances" of your particular IoT device and system.

The Article 29 Working Party has also made the following recommendations for all IoT stakeholders:

- Conduct Privacy Impact Assessments before any new applications are launched in the IoT;
- Only collect and process aggregated data; delete any raw data as soon as extracted for processing;
- Apply the principles of Privacy by Design and Privacy by Default;
- Give data subjects and users the right to be "in control" of their data; and
- The methods for giving information must be user friendly and understandable.

Penalties aren't light. Failure to comply with GDPR standards can result in administrative fines up to €20,000,000, or—in the case of an undertaking—up to 4 percent of the total worldwide annual turnover for the preceding financial year, whichever is higher.

The Takeaway

IoT devices and systems are subject to an expanding set of regulations both in the U.S. and abroad. The applicability and scope of these regulations can be unclear, and failure to comply, even if you have not experienced a single data breach, can be dire. It is critical for those in the IoT space to understand how these regulations apply to your business, develop a compliance plan, and continue to monitor the changing regulatory landscape. In the IoT world, cybersecurity must be on your radar regardless of whether your devices are dealing with data about credit card accounts, health and wellness, depletion of dairy products, or simply assisting with live-streaming dog videos over the internet. Don't get bit.

[1] TRENDnet, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 78 FR 55717-02, 2013 WL 4807346 (September 11, 2013)

[2] Fed. Trade Comm'n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, 2017 WL 4150873 (N.D. Cal. Sept. 19, 2017).