FDCC Insights
DEFENSE LAWYERS. DEFENSE LEADERS.
A Journal for Defense and Corporate Counsel

DECEMBER 2016

THE INTERNET OF THINGS AND ITS IMPACT ON DATA RETENTION, E-DISCOVERY, PRODUCTS LIABILITY, AND CYBERSECURITY

MARISA A. TRASATTI & MATTHEW S. SARNA

Introduction

The Internet of Things ("IoT") is the movement to make the world "smart." It is comprised of machine-to-machine communicating devices, built on cloud computing and networks of data-gathering sensors. *See* Daniel Burrus, *The Internet of Things is Far Bigger than Anyone Realizes,* Wired, available at https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/. It is the seamless flow of data among the BAN (body area network), LAN (local area network), WAN (wide area network), and VWAN (very wide area network). You likely have already heard of and even potentially use several products that fall under the umbrella of the IoT in your everyday life. For example, the Nest Thermostat can interoperate and communicate with electronic devices all throughout your property, from the lights to the sprinklers. Like Fitbits, Nest Thermostats have been in the news over security concerns. *See Works With Nest*, available at https://workswith.nest.com/products (last visited Dec. 8, 2016).

Gartner, Inc. estimates that roughly 4.9 billion units of IoT devices were in use back in November 2015. By the year 2020, Gartner estimates that this number will expand to over 20.8 billion devices. *See* Immanuel Kim, *The Internet of Things: A Reality Check for Legal Professionals*, ABA Law Practice Today (Jan. 14, 2016), available at http://www.lawpracticetoday.org/article/the-internet-of-things-a-reality-check-for-legal-professionals/. According to a comprehensive study by the McKinsey Global Institute, the potential economic impact of the IoT could reach upwards of $11.1 trillion per year by 2025. *See The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute, pp. 23–24 (June 2015), available at http://www.mckinsey.com/business-functions/digital-mckkinsey /our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

MARISA A. TRASATTI
General Counsel of Sciton, Inc.
Baltimore, MA
mtrasatti@semmes.com

Marisa serves as General Counsel of the California-based laser company, Sciton, Inc., in addition to maintaining an office at Semmes, Bowen & Semmes in Baltimore, Maryland, where she has been a Principal for the past eight (8) years. Prior to assuming her position as General Counsel, Marisa's practice focused on civil litigation with an emphasis on products liability litigation, including cases involving drugs and medical devices. As General Counsel, she manages all civil, corporate, and regulatory matters domestically and abroad for the company. She is the Vice-President of the Maryland chapter of the Claims and Litigation Management Alliance, an active participant in DRI's Toxic Tort and Products Liability committees, and the immediate past-Chair of the FDCC's Drug, Device and Biotechnology Committee. She is the current Vice-Chair of the Publications Committee for the FDCC and has also been appointed FDCC's Corporate Counsel Symposium Co-Program Chair for 2017; the 2017 U.S. East Coast Coordinator of Membership Development and Retention Committee; 2017 Co-Program Coordinator and presenter at FDCC's Drug, Device and Biotechnology Winter Meeting; and 2017 Graduate Dean of Marketing for FDCC's Litigation Management College. Marisa is also active in her local community as President-Elect of the Maryland Defense Counsel ("MDC").

MATTHEW S. SARNA
Summer Associate, Semmes, Bowen & Semmes
Baltimore, MA
mwalshe@stonepigman.com

Matthew is a 3L at the University of Maryland Francis King Carey School of Law with a focus on corporate transactional and bankruptcy law. This past summer, Matthew worked as a Summer Associate at Semmes, Bowen & Semmes in Baltimore, Maryland. At Maryland Law, Matthew is an Executive Editor for the Journal of Business and Technology Law and the President of the Jewish Law Students Association. Matthew also competes for the Alternative Dispute Resolution Team, the Moot Court Board, and the Transactional Law Team.

The implications of the explosion of IoT devices into the economic marketplace are far-reaching. Accordingly, commentators have broken the IoT industry down into two distinct categories: the Consumer

Internet of Things and the Industrial Internet of Things ("IIoT"). Despite the contention that enterprises (as opposed to consumers) use the vast majority of new IoT devices, the media has focused mainly on wearable technologies like the Fitbit and home security systems as at the forefront of the IoT. *See* Steven E. Reynolds & Deepali Doddi, *The Internet of Things Could Put Trade Secrets At Risk*, Law360 (June 7, 2016), available at https://www.law360.com/articles/803994/the-internet-of-things-could-put-trade-secrets-at-risk. The Fitbit tracks every part of the user's day, including activity, food intake, exercise, body weight, and sleep, compiling this data and transforming it into actionable goals for the user. *See Fitbit Find Your Fit*, available at https://www.fitbit.com/whyfitbit (last visited Dec, 8, 2016).

The exponential rise of the IoT implicates several important areas of law. Pertinent to this analysis are the areas of Data Retention, E-Discovery, Products Liability, and Cybersecurity.

Companies use these data points to generate trends and learn how to better their services for their customers. The retention of large quantities of data, however, is a double-edged sword, and accordingly is subject to regulation.

Data Retention

A large portion of IoT devices interoperate through data-gathering sensors, which, in turn, rapidly collect data points about, for example, the air quality level in your home or heat signatures on your property. Companies use these data points to generate trends and learn how to better their services for their customers. The retention of large quantities of data, however, is a double-edged sword, and accordingly is subject to regulation.

As opposed to other countries, the United States does not currently have a mandatory data retention law. *See* United States, Electronic Frontier Foundation, available at https://www.eff.org/issues/mandatory-data-retention/us (last visited Dec. 8, 2016). The gap, however, has not been without attempts at regulation. In May 2011, the "Protecting Children from Internet Pornographers Act of 2011" was introduced to the House of Representatives. *Id.* The Act, H.R. 1981, would amend 18 U.S.C. § 2703, which defines the terms under which companies that store electronic consumer data must disclose it to the government. *Id.* The amended language would "require companies to turn over to the government without a warrant detailed information including customer's name, address, records of session times and durations, the length of service (including start date) and types of service utilized plus credit card or bank account number." *Id.*

At first glance, IoT devices may not appear to fall under the scope of 18 U.S.C. § 2703. The language of the statute, however, uses the phrase "electronic communication service," which is expressly defined as "any service which provides to users thereof the ability to send or receive wire or "electronic communications." 18 U.S.C. § 2510(15) (2015). Electronic communication is defined as follows:

> …Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include–
>
> (a) any wire or oral communication;
>
> (b) any communication made through a tone-only paging device;
>
> (c) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (d) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds, . . .
>
> 18 U.S.C. § 2510(12) (2015).

Although subsection (c), excepting tracking devices, removes a large subset of IoT devices from the equation, it is unclear whether an interoperable device like the Nest Thermostat which sends and receives electronic communications throughout the user's property, would fall under this statutory regulatory scheme. The United States Department of Commerce's National Telecommunications and Information Administration ("NTIA") has recently launched a probe into the data security implications of the IoT, specifically devices like the Nest Thermostat and wearable devices like the Fitbit. *See* Melissa Maleske, *GC Cheat Sheet: The Hottest Corporate News of the Week*, Law 360 (Aug. 5, 2016), available at http://www.law360.com/articles/825491/gc-cheat-sheet-the-hottest-corporate-news-of-the-week. The NTIA conducted a multistakeholder process in October 2016 to focus on cybersecurity, upgradability, and patching of IoT devices and applications. *See* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security. Additionally, the Consumer Product Safety Commission ("CPSC") is currently working on compiling a report to provide a "snapshot" of the potential emerging hazards of interoperable and wearable devices in the marketplace. *See* Emily Field, *CPSC Chair Kaye Eyes Safety Risks in New Technologies*, Law360 (Aug. 8, 2016), available at http://www.law360.com/articles/824104/cpsc-chair-kaye-eyes-safety-risks-in-new-technologies. These studies and reports will assist the legislature in its necessary expansion of the definitional scope of what falls under regulation and what data will be subject to disclosure.

E-Discovery

Taking a step sideways into the realm of litigation and the everprevalent e-discovery discussion, data retention can prove both beneficial and detrimental for products liability attorneys, depending on which side of

the courtroom they are on. For example, data compiled by the variety of fitness trackers available and still to be developed could prove useful in defending a personal injury claim. Litigators will have the ability to analyze a party's historical health condition data up to the minute before the alleged symptoms occurred or incident took place. *See* David F. Katz, et al., *The Internet of Things: Effective Techniques to Identify, Collect, and Present Electronic Evidence*, * 6, Defense Research Institute, (February 2016). Additionally, there are IoT devices currently being developed that will be able to gather data about the weather conditions while also gathering data about the stability of concrete in the foundation of buildings and roads. *See* Burrus, *supra* (explaining that IoT sensors implanted in cement will be able to monitor stresses, cracks, and warpages ("smart cement") or communicate icy conditions to the wireless internet in your car to alert the driver of unstable or unsafe driving conditions). Such devices may have instantaneously alerted the Maryland government and Rescue Services of the destructive stress building up on the roads and waterways in Ellicott City, Maryland prior to the flooding on July 30, 2016, and allowed for a quicker response time. *See* Mike McPhate, *Flood Rips Through Historic Maryland Town, Killing at Least 2*, NY Times (July 31, 2016), available at http://www.nytimes.com/2016/08/01/us/ellicott-city-flood-maryland.html. Soon, a necessary step in all products liability cases, and likely a substantial number of cases flowing from both criminal and civil law, will be to check and pull data from the several interoperating devices that were operating at the scene of the incident.

Soon, a necessary step in all products liability cases, and likely a substantial number of cases flowing from both criminal and civil law, will be to check and pull data from the several interoperating devices that were operating at the scene of the incident.

The expansive capability of device preserved data raises issues of spoliation claims. Katz, *supra* at 7. IoT data, unlike data on the hard drive of a desktop computer, often suffers from a lack of clarity as to who actually is in control of the data. *Id*. Interoperable devices may interact with several third-party software developers throughout the course of the day, creating extensions in the "data supply chain." *Id*. at 7–8. Prior to the 2015 amendment of Rule 37 of the Federal Rules of Civil Procedure, which governs sanctions associated with the failure to make disclosure or cooperate with discovery, attorneys would have been hard pressed to extensively map out the data trail in a desperate attempt to locate the party in control. The 2015 amendment, however, shifts the burden to the party seeking relief to show that the responding party did not take "reasonable steps" to preserve the electronically stored information ("ESI") in anticipation of litigation. *Id.* The revision provides a little more leeway for litigators who will have trouble tracking down the correct third-party operator in the data supply chain of IoT devices. Anticipating demands for IoT data, attorneys operating specifically in the products liability field should begin to familiarize themselves with the several technical data gathering components contained in today's popular IoT devices and how these types of ESI can be authenticated and used in litigation. *Id.* at 8; *see also United States v. Hassan*, 742 F.3d 104, 133-134 (4th Cir. 2014) (finding that evidence including Facebook messages surrounding a terrorism conspiracy was properly authenticated through certifications of records custodians of Facebook and Google, who verified that Facebook pages and YouTube videos *has* been maintained as business records in the course of regularly conducted business activities); *but see United States v. Vayner*, 769 F.3d 125, 131 (2d Cir. 2014) (reversing a conviction after finding insufficient verification of a Facebook page printout asserted to be the defendant's profile page).

Products Liability

Last year, hackers made the news after proving that they could remotely enter Fiat Chrysler's Jeep Cherokee on-board computer system and take control of vital car functions like steering, accelerating, and braking. *See* Danny Yadron & Mike Spector, *Hackers Show They Can Take Control of Moving Jeep Cherokee*, The Wall Street Journal (July 21, 2015), available at http://www.wsj.com/articles/hackers-show-they-can-take-control-of-moving-jeep-cherokee-1437522078 and *Jeep hackers show how to take control of vehicle moving at high speed*, Fox News (Aug. 4, 2016), available at http://www.foxnews.com/tech/2016/08/04/jeep-hackers-show-how-to-take-control-vehicle-moving-at-high-speed. Fiat Chrysler is now facing a lawsuit. *See Flynn, et al v. FCA US LLC*, Case No. 3:15-cv-855 (S.D. Ill. Aug. 4, 2015). The plaintiffs alleges that a security flaw in "infotainment" centers installed in RAM, Chrysler, Jeep, and Dodge vehicles made the system "exceedingly hackable" and permitted hackers to "remotely take control" of the vehicle's functions. The seventeen (17) count complaint *alleged*, among other things, negligence, fraud and breach of warranties. The defendants moved to dismiss based on the speculative nature of the damages. The court dismissed certain claims, but allowed others to go forward – namely, claims based on damages for overpayment for and the diminished value of the affected vehicles.

Surprisingly, another area of concern in the product liability sphere is children's toys. There is a lawsuit currently pending in Illinois federal court against VTech, the maker of learning devices for children. *See In Re: VTech Data Breach Litigation*, Case No. 1:15-CV-10889 (N.D. Ill. Dec. 31, 2015). According to the complaint, a hacker broke through VTech's security measures in November 2015 and obtained customer data from a customer database housed on web-linked VTech device. As is becoming a theme in these types of cases, the defendants moved to dismiss alleging that the plaintiffs had suffered no concrete injury. The motion to dismiss is currently pending. A similar potential invasion of privacy action against Mattel arising out of the allegedly unauthorized recording of children's voices by "Hello Barbie" (an interactive doll) was dismissed with prejudice earlier this year. *See Archer Hayes, et al v. ToyTalk, Inc., et al*, No. 2:16-cv-02111 (C.D. Cal. 2016).

Most recently, a purported class of plaintiffs filed suit in *Ross v. St. Jude*

Medical, Inc., Case No. 2:16-cv-06465 (C.D. Cal. Aug. 26, 2016), alleging that cardiac pacemakers and other devices manufactured by St. Jude were susceptible to security breaches. The St. Jude pacemakers and other devices transmit signals remotely to in-home monitoring equipment. The plaintiffs alleged that the remote monitoring capabilities were not secure, leaving the devices susceptible to a hypothetical "crash attack," which could cause the pacemakers to pace abnormally fast or slow and lead to severe health consequences. While this products case is in its early stages, it shows that plaintiffs are testing the waters of mass actions. *See* John Clabby & Joseph Swanson, *A Look At Manufacturer Liability For the Internet of Things*, Law360 (Oct. 4, 2016), available at https://www.law360.com/illinois/articles/846901/a-look-at-manufacturer-liability-for-the-internet-of-things.

Challenges to standing have been the best defense in the early cases testing manufacturer liability for the Internet of Things. *See id*. This is consistent with information-only data breach cases that came before. Arguably, however, there is more at stake in the Internet of Things cases. After all, the allegation that a life-sustaining pacemaker or a vehicle being driven on the road is susceptible to hacking is a much more frightening prospect than a breach of personal information. *See id*.

Arguably, however, there is more at stake in the Internet of Things cases. After all, the allegation that a life-sustaining pacemaker or a vehicle being driven on the road is susceptible to hacking is a much more frightening prospect than a breach of personal information.

Cybersecurity

In 2015, the Federal Trade Commission ("FTC") released a fifty-five (55) page staff report detailing best practices for privacy and data security within the IoT. *See* Reynolds, *supra* n. 10; see also *Federal Trade Commission, Internet of Things, Privacy & Security in a Connected World*, FTC Staff Report (January 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (last visited Dec. 8, 2016). The Report provided guidelines for best practices to safeguard IoT devices and software from security breaches and to promote consumer privacy. Specifically, the Report suggests the following practices: (1) build security into the device at the outset, rather than as an afterthought of the design process; (2) train employees about the importance of security, and ensure that security is properly managed throughout the organization; (3) ensure that outside consultants or service providers are subject to and maintain the requisite level of security and provide for reasonable oversight of these consultants and providers; (4) consider a "defense-in-depth" strategy for systems with significant risk where multiple levels of security may be used to defend against security threats; (5) consider measures to keep unauthorized users from accessing a consumer's device, data, or personal information; and (6) monitor the device's life cycle and provide for routine security patches. *Id*. at 27-31; *See also FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, Federal Trade Commission (January 27, 2015), available at https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices. An important addition to these suggestions, which the FTC discussed at length in its report, is the development of policies to minimize the collection and retention of consumer data as much as possible without taking away from functionality. *See FTC Staff Repport, supra*, at 33–34. ("… companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data."); *see also Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values* ("White House Big Data Report") at 54 (May 2014) (Because the logic of collecting as much data as possible is strong and it is difficult to keep data anonymous, focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."). The general proposition becomes, the more data retained, the higher the risk of breach.

In 2013, the FTC first jumped into the debate concerning the legal issue of whether data security policies can match the stampede of IoT device expansion in an enforcement action against TrendNet, Inc. *See In the Matter of TrendNet, Inc.*, Docket No. C-4426 (F.T.C. Jan. 16, 2014), available at https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf (last visited Dec 8, 2016 and Dara Kerr, *FTC and TrendNet settle claim over hacked security cameras*, C/Net (Sept. 4, 2013), available at https://www.cnet.com/news/ftc-and-trendnet-settle-claim-over-hacked-security-cameras/). The FTC asserted that TrendNet's unsophisticated security measures allowed hackers to intercept feeds from its internet-connected camera surveillance systems. Hackers had infiltrated the software and were able to look directly into the homes where these cameras were installed to surveil. *Id*. While this example is narrow, the expansive interoperability of IoT devices will force companies competing in the IoT space to substantially revisit their security systems to prevent cybercrimes, from small hacks to large-scale breaches. In this respect, both the Uniform Trade Secrets Act and the federal Defend Trade Secrets Act require companies to take reasonable steps to keep their data and information secret in the context of trade secret protection. *See* Uniform Trade Secrets Act § 1.4 (1985); Defend Trade Secrets Act § 2(b)(1) (2016) (amending 18 U.S.C. § 1839(3) which defines the term "trade secret"). Enhanced security measure requirements will pose significant costs to enterprises and will likely drive economies of scale and push costs onto consumers.

Shortly after the FTC filed its IoT Staff Report in early 2015, the U.S. Senate Committee on Commerce, Science and Transportation held a hearing, titled "The Connected World: Examining the Internet of Things." *See* U.S. Senate Committee on Commerce, Science & Transportation, *The Connected World: Examining the Internet of*

Things, available at http://www.commerce.senate.gov/public/index.cfm/2015/2/the-connected-world-examining-the-internet-of-things (last accessed Dece. 8, 2016). Most of the panelists at the hearing agreed that Congress should "not stifle the Internet of Things before [Congress] and consumers have a chance to understand its real promise and implications." *See* Howard W. Waltzman & Lei Shen, *The Internet of Things* at p. 2, Mayer Brown (March 17, 2015), available at https://www.mayerbrown.com/The-Internet-of-Things. Contrary to the hands off view of Congress and best practice recommendations from the FTC, the European Union's Article 29 Data Protection Working Party released an opinion in 2014 which focused on compliance with EU privacy requirements. *Id*. at 3. Although non-binding, this stance reveals that the EU is taking a more hands-on approach to IoT regulation than the United States.

Conclusion

The IoT implicates a vast number of practice areas for attorneys, from e-discovery to cybersecurity. Law firms and legal professionals must begin to take proactive steps to familiarize themselves with the possible legal issues surrounding the expansion of IoT devices. The "next Industrial Revolution" is here, and the legal world needs to keep up. *See* Model Rules of Prof'l Conduct, Rule 1.1, *Competence* ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.") and Rule 1.1, Comment 8 ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.")