Catholic University Journal of Law and Technology

Volume 24 | Issue 2 Article 5

2016

The Connected State of Things: A Lawyer's Survival Guide in an Internet of Things World

Antigone Peyton
Cloudigy Law PLLC

THE CONNECTED STATE OF THINGS: A LAWYER'S SURVIVAL GUIDE IN AN INTERNET OF THINGS WORLD

Antigone Peyton*

I. INTRODUCTION

The latest tech buzz centers on the Internet of Things ("IoT"), a concept that describes the network of everyday objects ("Things") that transmit and receive data while connected to the Internet.[1] The network includes Internet-connected cameras embedded in mobile devices that allow you to take and post pictures online with a few swipes of a finger.[2] It also encompasses home automation systems that connect one's lighting,[3] garage doors,[4] a security system,[5] the refrigerator,[6] and coffee maker[7] to its owner and their family and to one another.[8]

* J.D., George Mason University School of Law, 2002; M.B.E., Bioethics, University of Pennsylvania, 1999; B.S., Chemistry, College of William & Mary, 1996. Ms. Antigone Peyton is the founder and CEO of Cloudigy Law PLLC, an intellectual property and technology law firm located in McLean, Virginia. Ms. Peyton is an unabashed technophile focused on litigation and cutting-edge technology issues, particularly those involving social media, patents, trademarks, copyrights, and trade secrets. She is a frequent speaker and writer covering technological competence, IP, social media, and e-discovery issues. She can be found on Twitter or SnapChat at @antigonepeyton.

1 Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), http://onforb.es/1pjMF6h.

2 Stephanie Buck, *The Beginner's Guide to Instagram*, MASHABLE (May 29, 2012), http://on.mash.to/1U1QQ4i.

3 *Philips Hue*, PHILIPS, http://bit.ly/1S0lvuS (last visited Feb. 29, 2016) (describing personal lighting controls connected through Wi-Fi).

4 Grant Clauser, *MyQ Garage Smart Garage Door Opener Review: Protecting the Internet of Things in Your Garage*, ELEC. HOUSE (June 14, 2015), http://bit.ly/1U1QTNB.

5 Gail Dutton, *Home Security 2015: The Internet of Things (IoT) Brings Innovation and Danger*, FORBES (Apr. 8, 2015, 8:00 AM), http://onforb.es/21rKBp2.

6 Michael Kanellos, *Hold the Laughter: Why the Smart Fridge Is a Great Idea*, FORBES (Jan. 13, 2016, 12:40 PM), http://onforb.es/1MiRZw5.

7 Brian Bennett, *Why smart coffee makers are a dumb but beautiful dream*, CNET (Nov. 14, 2015, 5:00 AM), http://cnet.co/1QYy2N7.

8 Morgan, *supra* note 1.

Some IoT objects have "embedded intelligence" that can detect and react to changes in their physical state.[9] IoT also involves devices sold in a business-to-business context and machine-to-machine communications that enable businesses to track inventory, currency, functionality, and efficiency.[10] Though there is no widely accepted definition of IoT, the concept focuses on how computers, sensors, and objects seamlessly interact with each other and process data.[11]

The rise of IoT, which coincides with the rise of big data, leads to almost limitless possibilities for consumers seeking remote access and control options relating to their electronic devices and other objects.[12] It may greatly benefit consumers of healthcare; for example, insulin pumps and blood-pressure cuffs can connect to a mobile app and enable patients and doctors to record and monitor vital signs.[13] In a connected state, patients are no longer required to visit the physician's office for evaluation and monitoring, or stay in long-term care and health monitoring facilities.

IoT is also helping companies understand customer behavior, desires, and purchasing decisions to improve system efficiency.[14] Some special interests groups and companies are also obtaining actionable intelligence from large-scale patterns teased from massive data collections made possible by IoT.[15]

---

[9] Thomas H. Davenport & John Lucker, *Running on Data: Activity Trackers and the Internet of Things*, 16 DELOITTE REV. 5, 5-6 (2015), http://bit.ly/1UbTt2W.

[10] *See generally* Kevin Bonsor & Wesley Fenlon, *How RFID Works*, HOWSTUFFWORKS, http://bit.ly/22fdxpX (last visited Feb. 29, 2016) (explaining consumers, including some business, place Radio Frequency Identification (RFID) tags on products in stores or in transit to monitor inventory and status of production).

[11] *See* Morgan, *supra* note 1. (relating to the idea that "things" in the IoT generally do not include desktop or laptop computers, smartphones, and tablets, rather these devices are commonly used to control or communicate with these "things," which offer the consumer endless possibilities).

[12] Teena Maddox, *Research: 30 percent of organizations collecting big data*, ZDNET (Mar. 2, 2015, 9:38 PM), http://zd.net/1Wls10y; see generally *Big Data,* GARTNER IT GLOSSARY, http://gtnr.it/1RuD6gU ("Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation."); *See also* Jennifer Dutcher, What is Big Data?, BERKLEY SCHOOL OF INFO. (Sept. 3, 2014), http://bit.ly/27QRVAL (interviewing a variety of industry leaders and showing that there is a clear split as to the meaning of the term).

[13] *See* MEDICAL DEVICE PRIVACY CONSORTIUM, COMMENTS TO THE U.S. HOUSE ENERGY AND COMMERCE COMMITTEE CONCERNING "21ST CENTURY CURES" 2 (October 31, 2014), http://bit.ly/1Ln6CDP.

[14] Neil Patel, *How the Internet of Things Is Changing Online Marketing*, FORBES (Dec. 10, 2015), http://onforb.es/1Wls24x.

[15] *See Smart Meters*, SMART GRID, http://bit.ly/1M31BQK (last visited Feb. 21, 2016) (explaining how smart meters in the home enable energy providers to analyze consumer energy use, identify issues with appliances and meters, and help consumers become aware

Multi-nodal and enhanced connectivity of "things" will undoubtedly offer numerous other benefits to consumers and businesses as the technology trend grows and matures.

In 2009, the number of "things" connected to the Internet surpassed the number of people.[16] That was just the beginning of the IoT movement. In fact, everyone is living in a world that is moving inexorably towards wireless and wired connectivity between a variety of cool and mundane objects that people interact with every day.[17] The LinkedIn "Internet of Things Community" is over 11,000 members strong, and is growing every day.[18]

There are benefits and risks associated with IoT. These connected objects, combined with big data analytics, can make everyone's lives easier and safer yet more complicated, simultaneously.[19] For instance, IoT can help us predict and diagnose disease conditions with healthcare providers, predict dangerous weather patterns and energy usage cycles, and closely track the spread of a pandemic.[20] But IoT could also lead to car control and automated home system hacks, massive data breaches on a scale that is currently unimaginable, and unintentional sharing of large amounts of sensitive user health and behavior data.[21]

Additionally, IoT will have major implications for clients' business as technology adoption increases.[22] A practicing lawyer should understand these benefits and risks to help their clients and firms navigate business concerns. Practitioners must also consider emerging legal issues relating to IoT and be prepared to deal with the fact this is yet another area where the technology is leap-

---

of their energy usage); *see, e.g.*, Vincent Granville, *Great IoT, Sensor and Other Data Sets Repositories*, DATA SCI. CENTRAL (Oct. 25, 2015, 1:00 PM), http://bit.ly/1Ln3h7B (Scientists are also sharing information collected from a variety of sensors via Internet protocols and creating large data sets as a result of their collaboration).

16 DAVE EVANS, CISCO INTERNET BUS. SOLS. GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), http://bit.ly/1UtNnKe.

17 *See id.* at 3*; see also* Anthony Adshead, *Data set to grow 10-fold by 2020 as internet of things takes off*, COMPUTER WEEKLY (Apr. 9, 2014, 1:00 PM), http://bit.ly/1Wls7oR (reporting that almost 200 billion objects are currently connected to the Internet and able to automatically record, report, and receive data).

18 *Internet of Things Community*, LINKEDIN, http://bit.ly/1P8S6dm (last visited Mar. 1, 2016).

19 EVANS, *supra* note 16, at 6-7.

20 *See generally* U.S. FED. TRADE COMMISSION, FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at i-ii (2015), http://1.usa.gov/1SNBYVy.

21 ACCENTURE, THE INTERNET OF THINGS: THE FUTURE OF CONSUMER ADOPTION 6-7 (2014), http://bit.ly/1M2NElM.

22 *Id*. at 3 (reporting that 7% of consumers own a wearable IoT device and 4% of consumers own an in-home IoT device and concluding that mainstream consumer adoption of IoT devices and technology is inevitable).

ing ahead of the law. IoT raises a number of novel and interesting legal issues and practical complexities means tech-savvy lawyers, with a good grasp of the basic issues, will be well-positioned to provide thoughtful and constructive advice.

The IoT movement also calls for lawyers to roll up their sleeves and think creatively about how all these connected objects impact their practice. For instance, IoT could open new avenues related to litigation or even exonerate clients. However, mere participation in the IoT movement might violate a lawyer's duty to keep client confidences and other ethical obligations. This possibly leaves lawyers in a precarious situation. Nonetheless, the answer may be in plain sight, flying through the internes, waiting patiently in a client's smart phone apps, or living in the slack space on a mobile device hard drive.

Lawyers need to develop situational awareness, and talk with clients about the smart objects they interact. [23] The data those objects collect might demonstrate the extent of their physical injury and diminished capacity, provide an alibi,[24] indicate the physiological response to a sexual harassment incident, or provide evidence of a former employee's unauthorized access to company systems to steal data.[25] Consider the narrative that can be created once counsel obtains the right IoT data from a client or opponent. Practitioners cannot consider the options, however, until the right questions are asked. Practicing and aspiring attorneys must hone their technical competence and start thinking about how IoT will forever change the way law is practiced. Consider this the lawyer's survival guide and introduction to the "connected state of things."

II. THE INTERNET OF WHAT?

The basic premise behind IoT is that everyday objects can be turned into "smart" devices that exhibit improved operability, efficiency, and can communicate with and respond to their people masters remotely.[26] The IoT concept includes interaction with virtual objects, including virtual machines that have

---

[23] *See generally* U.S. FED. TRADE COMMISSION, *supra* note 20, at i-ii.

[24] DAVID W. HAGY, NAT'L INST. OF JUSTICE, NCJ 213030, INVESTIGATIVE USES OF TECHNOLOGY: DEVICES, TOOLS, AND TECHNIQUES 24-25, 28, 31-35 (2007), http://1.usa.gov/1NHMJZ2 (creating the example that an alibi can be proved or disproved by using the information from an IoT device associated with a victim, suspect, or third party witness by extracting the location or timestamp of the device when a crime or incident occurred).

[25] Sophie Kleemna, *Woman Charged with False Reporting After Fitbit Contradicted Her Rape Claim*, POLICYMIC (June 25, 2015), http://bit.ly/1SNAeLY; Charles Babcock, *9 Worst Cloud Security Threats*, INFO. WEEK (Mar. 3, 2014, 10:25 AM), http://ubm.io/1P8OWq3.

[26] ACCENTURE, *supra* note 21, at 3.

digital attributes and changing personalities through use of artificial intelligence.[27] These objects are programmed to communicate via apps, text messages, browsers, and other tools that people use to interact with their environment and the objects that surround them.[28] They tend to communicate using embedded sensors and wired and wireless communication protocols as well as other systems, including Wi-Fi, Bluetooth, and a variety of specialized IoT protocols.[29]

Imagine a refrigerator that tells its owner when he or she needs more milk and a home thermostat that can be adjusted remotely using an app on a mobile device that gradually learns the user's behavior patterns relating to his or her preferred home climate at certain times of the day.[30] How about a networked house that connects power outlets to sounds systems, TVs, smoke detectors, security cameras, coffee pots, and the homeowner through a software app.[31] This connected home is reminiscent of the future portrayed in the 1960s cartoon *The Jetsons*, where robots and talking items support the Jetson family and their space-age home. But these homes already exist, and more are coming online every day.[32]

Consumers' drive for greater connectivity includes objects outside the home. Workers and service professionals are connecting remotely and communicating with their company's business equipment and office systems via mobile devices.[33] Consumers are buying networked cars[34] and walking around with

---

27 Steve Lohr, *The Promise of Artificial Intelligence Unfolds in Small Steps*, N.Y. TIMES (Feb. 28, 2016), http://nyti.ms/1nJtlhH.

28 *See* Angela Moscarito, *Your Printer Can Now Order Ink For You, Thanks to Amazon*, PC MAG. (Jan. 19, 2016, 11:35 AM), http://bit.ly/1SNF1gr; *see also A Smart Home Solution That Lives in the Cloud*, COMCAST, http://comca.st/22gtTv2 (last visited Mar. 7, 2016) [hereinafter COMCAST].

29 *See* Jose Pagliery, *OMG: 2.1 million people still use AOL dial-up*, CNN MONEY (May 8, 2015), http://cnnmon.ie/1U1VLCg.

30 Michael Gowan, *LG Smart Fridge Spots Spoiled Food, Orders Groceries*, NBC NEWS (Jan. 4, 2013), http://nbcnews.to/1V7n1yi (discussing a smart refrigerator that connects to the Internet and allows users to remotely access the refrigerator content list, keep track of their grocery list, and identify out-of-date products stored in it); Bernard Marr, *Google's Nest: Big Data And The Internet of Things In The Connected Home*, FORBES (Aug. 5, 2015, 10:52 AM), http://onforb.es/1M2RJq7 (discussing Nest Thermostat, which uploads usage data from individual devices via the Internet, allowing Nest to understand energy usage trends across community microcosms, cities, and even usage around the world).

31 *See*, *e.g.*, COMCAST, *supra* note 28 (describing the Xfinity Home technology, which allows users to monitor and control security cameras, smoke detectors, thermostats, lights, and motion sensors through web browsers or Internet connected devices like smart phones and tablets); Marr, *supra* note 30 (noting that Google is building the infrastructure for smart homes of the future that are fully networked by its own devices).

32 ACCENTURE, *supra* note 21, at 6-7.

33 *See* Moscarito, *supra* note 28 (explaining some office printers can automatically order a new toner cartridge from the manufacturer or authorized distributor when the toner levels in the printer are low and others can initiate a service call for repair if a critical error alert is

wearable fitness and health technologies strapped to their arms and embedded in their clothes.[35] Whether objects are manufactured for connectivity or retrofitted, IoT is taking the digital and physical world by storm.

III. LAWYERS' ETHICAL OBLIGATIONS IN A CONNECTED STATE

Lawyers must immediately consider their own confidentiality and competence obligations when analyzing the legal and practical issues relating to IoT. This means lawyers must develop technical knowledge and expertise, though the appropriate skills will depend on their substantive practice focus, firm infrastructure, and clients. In fact, this technical competency requirement is starting to surface in ethics opinions and in the rules governing legal practice in many jurisdictions. [36]

For instance, the American Bar Association's ("ABA") Model Rules of Professional Conduct ("Model Rules") for lawyers in the United States include Rule 1.1, which addresses the "client-lawyer" relationship and a lawyer's duty of competence to her client.[37] Specifically, "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[38] In 2012, the ABA updated the Model Rules and, for the first time, a comment to Rule 1.1 includes an explicit reference to technical competency requirements.[39] This amendment highlights the important role technology plays in the practice of law today.[40] In fact, a number of states have already

---

triggered); *see* Patrick Moorehead, *Hewlett-Packard Designates Printing a First-Class IoT Security Platform,* FORBES (Sept. 29, 2014, 8:03 AM), http://onforb.es/1QTcpkE (explaining others allow organizations to monitor their networked printer's security).

34 Micah Wright, *5 Inexpensive Connected Cars With Available WiFi*, THE CHEAT SHEET (May 28, 2015), http://bit.ly/1QYC6Np.

35 Ariana Eunjung Cha, *The Revolution will be Digitized*, WASH. POST. (May 9, 2015), http://wapo.st/1pHIEt5.

36 *See generally* MODEL RULES OF PROF'L CONDUCT r. 1.1 (AM. BAR ASS'N 2014).

37 *Id*.

38 *Id*.

39 ABA Comm. On Ethics 20/20, Res. 105C, AM. BAR ASS'N, at 1-2 (2012) http://bit.ly/1nJXy06. (explaining Comment 8 to Rule 1.1 by stating that lawyers should become educated regarding the benefits and risks associated with technology relevant to their practice); MODEL R. PROF'L CONDUCT r. 1.1, cmt. 8 (AM. BAR ASS'N 2014) ("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.").

40 Matt Nelson, *New Changes to Model Rules a Wake-Up Call for Technologically Challenged Lawyers*, INSIDE COUNSEL (Mar. 28, 2013), http://bit.ly/22f2D3A (suggesting that the accompanying ABA report requirement for technical competence is not a new re-

adopted this change and incorporated in their own ethics rules in varying forms.[41] Thus, practicing lawyers have now been told, explicitly, that they need to keep pace with "relevant technology" to comply with their ethical obligation to competently represent clients.

Practicing lawyers should understand how their own objects share information with each other and the rest of the world. Carelessness or lack of diligence in safeguarding clients' sensitive information could lead to security breaches and involuntary sharing of client confidences across connected objects and networks.[42] Lawyers should be educated regarding the technologies that support the practice, clients' businesses, and best practices that minimize risks and maximize benefits associated with IoT.[43] Additionally, technical competence is important to satisfy a lawyer's discovery obligations.[44] If lawyers do not know what data is created, saved, and transmitted, they will have a hard time preserving, collecting, and using it to further clients' interests and satisfy their duties as officers of the court. Whether it involves home automation, business object tracking, firm systems, or communication through mobile devices—lawyers must diligently learn how to use and collect data from connected devices with care.

IV. THE LEGAL FRAMEWORK

While IoT opens up exciting new possibilities for improving everybody's life, it also raises new questions regarding the rules relating to lawyer's interactions with "things", clients, and others who operate in the digital world. The legal issues surrounding implementation of IoT systems and interaction with IoT objects are diverse. For instance, purposeful connectivity and the rise of big data raise important concerns regarding individual civil rights, protection against discrimination, data leaks, and secret data collection by government and law enforcement.[45] Increased personalization and categorization allows for

---

quirement, rather it is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of his or her general ethical duty).

41 *See generally States Making Amendments to the Model Rules of Professional Conduct*, AM. BAR ASS'N, http://bit.ly/1Mjgx80 (last visited Feb. 28, 2016) (listing the states that have adopted the ABA Model Rules of Professional Conduct, with or without modification).

42 Antigone Peyton, *Kill the Dinosaurs, and Other Tips for Achieving Technical Competence in Your Law Practice*, 21 RICH. J.L. & TECH. 7, 23-24 (2015).

43 *Id*. at 7, 14.

44 *Id.* at 7, 10-14.

45 JACOB KOHNSTAMM & DRUDEISHA MADHUB, 36TH INT'L CONF. OF DATA PROTECTION & PRIVACY COMMISSIONERS, THE MAURITUS DECLARATION ON THE INTERNET OF THINGS 1-2 (2014), http://bit.ly/1M36gCm.

discrimination with respect to pricing, services, and opportunities.[46] Privacy, information governance, intellectual property, and security issues seem to regularly make the list of top IoT risks.[47] The objects do not necessarily have civil liberties or privacy rights.[48] This is simply a problem for the people who interact with them—especially lawyers.

As with many emerging technologies, the IoT market is sprinting and the legal and regulatory frameworks are playing catch up. Since IoT is a global movement, a variety of stakeholders around the world are considering appropriate controls for such a large and complex environment.[49] The goal is to implement appropriate laws, processes, and self-regulating standards that do not impose unnecessary constraints on the IoT market.[50] At this point, IoT-specific legislation seems premature, particularly given the fact that IoT generally operates in a geography agnostic manner and is not a country-specific technology. Self-regulatory programs designed for particular industries seem to provide more promise and flexibility. They might encourage the adoption of appropriate privacy, information governance, and security-focused practices and allow room for the movement to grow, change, and mature. Currently, there are no special laws that apply to IoT technology.[51] Only time will tell whether there is a need for these regulations.

A. Tempering Privacy Expectations

The proliferation of IoT devices and its expanded use of mobile communication technology that connects them lead to significant privacy risks.[52] These include security breaches and unintentional sharing of sensitive information

---

46 EXEC. OFF. OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 7 (2014), http://1.usa.gov/1RhNQzX.

47 *See generally* U.S. FED. TRADE COMMISSION, *supra* note 20, at ii (noting that IoT risks include exploitation of consumers by enabling unauthorized access to and misuse of personal information, facilitating attacks on other computer systems, and increasing privacy risks because of the collection of personal information on habits, locations and physical conditions over time); GIANMARCO BALDINI, ET AL., EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS (IERC), INTERNET OF THINGS: IOT GOVERNANCE, PRIVACY AND SECURITY ISSUES 17 (2015), http://bit.ly/21rPhew; *Opinion 8/2014 on Recent Developments on the Internet of Things*, EURO. COMM'N WORKING PARTY 9 (Sept. 16, 2014) http://bit.ly/1QTqcHY.

48 *Internet Privacy*, AM. CIV. LIBERTIES UNION, http://bit.ly/1Rizl8I (last visited Feb. 29, 2016) [hereinafter ACLU].

49 *Id.*

50 *See generally* BALDINI, ET AL., *supra* note 47, at 10; U.S. FED. TRADE COMMISSION, *supra* note 20, at ii (explaining the perceived risks to privacy and security could undermine consumer confidence in the technology and inhibit widespread adoption).

51 BALDINI, ET AL., *supra* note 47, at 13.

52 U.S. FED. TRADE COMMISSION, *supra* note 20, at ii.

with third parties.[53] Additionally, the patchwork protection afforded by national and local privacy laws leads to widespread confusion regarding privacy rights and a range of consumer expectations relating to connected devices.[54] Regulators have started to explore the privacy-related risks of IoT, but more education and standardization of IoT practices are clearly needed.[55]

Lawyers and their clients should understand where a connected device's data goes once it is created, who has access to it, and what data will remain private. Some IoT technology and systems architecture expose names and personal identifiers to third-party applications sitting on mobile devices and other objects in the network.[56] For instance, the Federal Trade Commission penalized TRENDnet, a company that produces wireless cameras—an IoT device—that beamed live and motion-captured video to laptops or phones, for its inadequate security practices.[57] In this case, a hacker exploited those privacy and security flaws, and posted links to live feeds of sleeping babies, children playing, and other private family activities on the Internet for the world to watch.[58]

Many IoT manufacturers, particularly those in the wearable fitness device sector, are collecting and sharing very sensitive user information generated by their devices.[59] Others build privacy into the design or engage in a de-identification process, so that a person's identity is not linked with the information that their IoT objects generate.[60] Some companies seek consent for use of the data, with certain restrictions.[61] Other companies use contracts to hide their business.[62] Often, the contract governing a consumer's relationship with their IoT data is confusing, couched in archaic legal terms, and so long that no

---

53 ERNST & YOUNG, DATA LOSS PREVENTION: KEEPING YOUR SENSITIVE DATA OUT OF THE PUBLIC DOMAIN 1 (2011), http://bit.ly/1QTpQkt.

54 U.S. FED. TRADE COMMISSION, *supra* note 20, at ii.

55 *See id.; see also* U.S. FED. TRADE COMMISSION, FTC STAFF REPORT, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 2-3, 28-33, 35 (2000), http://1.usa.gov/1Lnk62k (resulting guidelines from Commission analysis of the manner in which online entities collect and use personal information and safeguards designed to provide adequate privacy protections).

56 SUBHARTHI PAUL, ET AL., ARCHITECTURES FOR THE FUTURE NETWORKS AND THE NEXT GENERATION INTERNET: A SURVEY 7-8 (2009) (Wash. Univ. in St. Louis Dep't of Comp. Sci. & Eng'g, Paper No. 2009-69), http://bit.ly/1pHHQnO.

57 Complaint at 8, In the Matter of TrendNet, Inc., 2013 WL 4858250 (F.T.C. Sept. 3, 2013) (No. C-4426) [hereinafter *Complaint, In the Matter of TrendNet, Inc.*] (noting TRENDnet, Inc. agreed to sanctions that include a 20-year security-compliance audit program); *see also* Agreement Containing Consent Order at III, In the Matter of TrendNet, Inc., 2013 WL 4858250 (F.T.C. Sept. 3, 2013) (No. 122 3090).

58 *Complaint, In the Matter of TrendNet, Inc*., *supra* note 57, at 10.

59 U.S. FED. TRADE COMMISSION, *supra* note 20, at ii.

60 *Id*.

61 *Id*.

62 *Id*.

mere mortal dare read or attempt to understand it.[63] These contracts, unfortunately, are a common tool for obtaining consumer consent or providing notice the data is being used or sold to third parties.

One growing privacy issue relating to IoT involves collection of data by law enforcement or secret court order.[64] This leads to critical questions about how rigorously certain companies defend an individual's data privacy rights.[65] For instance, wearable device companies that collect data from users and store it in cloud services can be subpoenaed.[66] Most providers have 'Terms of Service or End User License Agreements,' which contain clauses stating that the company may release user data in response to legal requests, without prior notice or any notice of the request.[67] Google and Microsoft, for instance, both regularly receive requests from the U.S. Foreign Intelligence Surveillance Court ("FISC Court" or "FISA Court") for information on thousands of user accounts.[68] They also receive letters from the FBI demanding disclosure of certain subscriber information for use in national security investigations as well as search warrants, court orders, and subpoenas seeking information about their account holders and activities involving their products for use in criminal investigations.[69] Each year, these governmental and non-governmental requests for information increase.[70]

Contrary to popular belief, the Health Insurance Portability and Accountability Act ("HIPAA")[71] does not protect personal data resulting from voluntary

---

63 U.S. FED. TRADE COMMISSION, FTC STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE- RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 61 (2012), http://1.usa.gov/1U2a4GZ.

64 U.S. FED. TRADE COMMISSION, *supra* note 20, at i-ii.

65 Shelton Abramson, *FTC Internet of Things Report Outlines Privacy and Security Recommendations for Industry*, INSIDE PRIV. (Jan. 28, 2015), http://bit.ly/1U29Q2x.

66 Lucas Mearian, *Data from Wearable Devices Could Soon Land You in Jail,* COMP. WORLD (Dec. 8, 2014, 3:00 AM), http://bit.ly/1MiZ8wu.

67 *See, e.g., Privacy Statement*, SALES FORCE, http://sforce.co/1V7rml2 (last updated Oct. 1, 2014) ("Salesforce.com reserves the right to use or disclose information provided if required by law or if the Company reasonably believes that use or disclosure is necessary to protect the Company's rights and/or to comply with a judicial proceeding, court order, or legal process."); *see also Cloud Data Privacy FAQ*, AMAZON, http://amzn.to/1MiYRtr (last visited Feb. 23, 2016) ("We do not disclose customer content unless we're required to do so to comply with the law or a valid and binding order of a governmental or regulatory body.").

68 *Transparency Report*, GOOGLE, http://bit.ly/1M2VvzL (last visited Feb. 23, 2016); *U.S. National Security Orders Report*, MICROSOFT CORP., http://bit.ly/1P91QEv (last visited Feb. 23, 2016).

69 GOOGLE, *supra* note 68; MICROSOFT CORP., *supra* note 68.

70 *See, e.g.,* GOOGLE, *supra* note 68 (illustrating data requests jumped from 9,981 to 12,002 between 2014 and 2015).

71 *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996); *The HIPAA Privacy Rule*, *see also* U.S. DEPT. OF HEALTH & HUMAN SERVS., http://1.usa.gov/1pqlYgX (last visited Feb. 23, 2016).

use of a personal wearable device.[72] HIPAA and state health privacy laws generally only cover the activities of certain medical entities and "business associates" that work with them.[73] Wearable technology manufacturers are not a "covered entity" under HIPAA, and even if they were, there's an exception to this law for law enforcement inquiries, national security needs, and a number of other legal requests.[74] HIPAA also permits the police to use an administrative subpoena or other written request, with no prior court involvement, as long as they state the information they seek is relevant, material, and limited in scope, and that masked information is insufficient.[75] Individuals are simply notified about law enforcement access to medical and health records by a generic HIPAA-mandated notice of privacy practices that they receive from a health facility or physician before they are treated for the first time.[76] Importantly, these legal request disclosures occur without the individual's prior authorization or notification that it occurred, so long as the regulatory conditions for law enforcement disclosure are seemingly satisfied. [77]

A growing number of industry groups, companies, and agencies are taking a more active role in defining appropriate access to and use of sensitive information collected through consumers' interactions with the objects that surround them. [78] Some have called for data-minimization practices, a concept that companies should limit the data they collect and retain, and dispose of it when

---

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearing houses, and those healthcare providers that conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect health information privacy and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization…The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.
Id.

72 Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables,* 103 GEO. L.J. 1641, 1647 (arguing HIPAA is ineffective when protecting consumers' personal data in a commercial setting).

73 *See* 45 C.F.R. § 160.103 (2015).

74 *See* Final Rule, Modification to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5567 (Jan. 25, 2013) (explaining the Health Information Technology for Economic and Clinical Health (HITECH) Act and related implementing regulations, "covered entities" and any business associate are subject to these law enforcement access rules).

75 *See When does the Privacy Rule Allow Covered Entities to Disclose Protected Health Information to Law Enforcement Officials?,* U.S. DEP'T OF HEALTH & HUMAN SERVS. (July 23, 2004), http://1.usa.gov/1QYEWBX (noting that this Privacy Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information).

76 *Notice of Privacy Practices*, U.S. DEP'T OF HEALTH & HUMAN SERVS. http://1.usa.gov/22f6M7G (last visited Feb. 29, 2016).

77 *See* U.S. DEP'T OF HEALTH & HUMAN SERVS. *supra* note 75.

78 See U.S. FED. TRADE COMMISSION, *supra* note 20.

it's no longer needed.[79] A number of national and international agencies and special interest groups have started studying the special privacy implications of the IoT movement.[80] More attention is needed as IoT tends to involve highly personal data.

From a lawyer's perspective, the legal regimes that govern the collection, processing, use, and ownership of object data are important when determining whether counsel—or their clients—have a duty to protect data generated from IoT activities, keep this information secure and confidential, or preserve and produce it in a litigation.[81] Lawyers should also consider whether clients are authorized to sell or share IoT data with other companies and whether they have provided appropriate notice to consumers through their privacy policy or contracts governing the relationship.[82] Often consumers will expect their wearable device data is "off limits" until their lawyer or service provider tells them otherwise.[83] The sooner lawyers identify the important data their clients and their customers generate, and the connected "thing" they interact with every day, the better off their clients will be for purposes of evaluating the legal risks and their obligations to secure and protect that information.[84]

B. What Information is Being Governed?

Information governance relates to the rules, processes, policies, and controls implemented to manage information at a company level and support the organization's business, legal, regulatory, environmental, and operational requirements.[85] Companies are struggling with the obligation to make decisions regarding all of the digital information that is created in support of the business.[86]

---

79 Id.

80 *See* U.S. FED. TRADE COMMISSION, *supra* note 20 at i-ii; *see also* BALDINI, ET AL., *supra* note 43, at 10; KOHNSTAMM, *supra* note 45, at 2.

81 *Preparing for the eDiscovery Wave of the Internet of Things*, RECOMMIND (2015), http://bit.ly/1RK3dvs.

82 U.S. FED. TRADE COMMISSION, *supra* note 20, at 38.

83 Maureen O'Neill, *E-Discovery and the Internet of Things*, AM. BAR ASS'N (2015), http://bit.ly/1pq5GEP.

84 *Id*.

85 *See Information Governance* GARTNER IT GLOSSARY, http://gtnr.it/1fnnnLZ (last visited May 23, 2016).

> Gartner defines information governance as the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

Id.

86 BALDINI, ET AL., *supra* note 47, at 10.

Some information is created using the corporate systems, but increasingly, it is generated and shared via mobile devices, laptop computers, and remote cloud computing technology.[87] The intermingling of business and personal data adds yet another layer of complexity—these devices contain both business and personal information.[88]

Information governance becomes even more complex with the addition of IoT thrown into the mix.[89] The large number and wide variation in technologies and objects communicating in the IoT environment means that more creative governance solutions are needed. Currently, there are not any apparent existing legal frameworks or approved special rules or guidelines focused on IoT governance issues.[90] However, some of the governance issues that have already cropped up will undoubtedly drive rulemaking and standard setting in the future.[91] Those issues include a lack of processes and procedures for verifying the authenticity or identity of objects.

Consumers may wonder: Is that really my thermostat or another person sending a "power's off" alert? Imagine the risks if a hacker turned off an office smoke alarm or switched off the security cameras, and the system does not know of it. Also, the transparency and accountability requirements will have to be ironed out with respect to IoT businesses' collection, storage, use, and interpretation of data their objects create.[92] Companies making IoT devices will have to consider the anti-competitive implications of some of their design decisions, even if good governance or product maintenance considerations drive them.[93] Some IoT designs and safety features have already spawned lawsuits alleging anti-competitive behavior.[94]

Businesses and consumers are now creating much of their information in an electronic format.[95] Businesses have already discovered that allowing their employees to store information in idiosyncratic and inconsistent ways makes it incredibly expensive to find that information when it is needed for business or

---

87 LOPEZ RESEARCH LLC, AN INTRODUCTION TO THE INTERNET OF THINGS (IOT), PART 1. OF "THE IOT" SERIES 4 (2013), http://bit.ly/1Uu43RQ.

88 ERNST & YOUNG, CYBERSECURITY AND THE INTERNET OF THINGS 14 (2015), http://bit.ly/1pHu58L.

89 Paul Roberts, *IT Pros: Internet of Things is a Governance Disaster*, SEC. LEDGER (2013), http://bit.ly/1M2TJyB.

90 BALDINI, ET AL., *supra* note 47, at 43.

91 *See*, *e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 688, (7th Cir. 2015) (bringing a class action lawsuit against department store after credit card information was stolen during a cyberattack).

92 *See* BALDINI, ET AL., *supra* note 47, at 43.

93 *Id.*

94 Bruce Schneier, *How the Internet of Things Limits Consumer Choice*, THE ATLANTIC (Dec. 24, 2015) http://theatln.tc/1QYDGPf.

95 Julie A. Steinberg, *Fifty Billion Connected Devices Bring Tort, Software Law Clash*, BLOOMBERG BNA (Feb. 26, 2016), http://bit.ly/1RiAJs9.

legal purposes.[96] And there is no central filing system for IoT data.[97] As with e-mail and information exchange across enterprise, mobile, and cloud platforms, it is a system without order and processes, only much more expansive and broader scale. As the IoT market matures, society—from the people to government to lawyers—must decide who owns and controls the information, and who is responsible for securing and preserving the data as it travels through the networks, or when it is at rest on the object's chip or manufacturer's servers. Companies must also reconsider their retention schedules in light of the risks associated with collection and storage of IoT data and the increasing infrastructure burdens as more objects connect and more data creation occurs as the market expands.

C. Intellectual Property Protection Gone Wrong

Lots of people reproduce, use, and modify copyrighted works, without permission, simply because they are accessible using a web browser, on a peer-to-peer site, or posted on social media.[98] The Digital Millennium Copyright Act ("DMCA"), however, makes it unlawful to circumvent certain protections designed to prevent the unlawful copying of a digital work, including software or other technology that manages access to an IoT object like a car control system or a home security device.[99] The goals of this anti-circumvention law seem pure—to give companies the ability to protect their intellectual property, maintain the functionality and safety of their products, and support new ways of disseminating copyrighted materials to users.[100] But it can also be used to protect a company's market for related products, hide aspects of the device's func-

---

[96] Max Metzger, *Human error no.1 cause of data loss, say IT professionals*, SC MAG. U.K. (Sept. 25, 2015) http://bit.ly/1RhHX5U.

[97] Stephane Charbonneau, *Want to Secure Your Data? Start with Classification*, DATA CENTER J. (Feb. 29, 2016) http://bit.ly/1QYAtzg ("[U]nstructured data now makes up 80 percent of nontangible assets, and data growth is exploding.").

[98] *See generally* ADRIAN JOHNS, PIRACY: THE INTELLECTUAL PROPERTY WARS FROM GUTTENBERG TO GATES (2010) (discussing the history and legacy of stealing intellectual property, including modern pirating of digital materials).

[99] 17 U.S.C. §§ 1201(a)(1)(A), 1201(a)(3)(A) (2012) (defining what it means to circumvent a "technological measure" that controls access to a work).

[100] H.R. REP. NO. 105-551, pt. 2, at 23 (1998).

> A thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment. And a plentiful supply of intellectual property—whether in the form of software, music, movies, literature, or other works—drives the demand for a more flexible and efficient electronic marketplace.

Id.

tion to closer scrutiny, and provide financial gain for the company.[101] There are some exceptions to the anti-circumvention law, but they are hard to obtain, limited in time, narrow, and rarely granted.[102]

IoT highlights some interesting issues associated with works, including software code, subject to the anti-circumvention laws.[103] For example, cars are now connecting to the Internet and accessing satellite radio, navigation and traffic information, and displaying e-mail and phone contacts on the in-dash display.[104] These cars are run by a complex set of control systems managed by software that vehicle manufacturers argue is protected by the anti-circumvention statute.[105] Vehicle owners for years could not repair, modify, or tinker with those control systems for fear of violating the law and being subject to prosecution.[106] Also, owners could not take their cars to local repair shops for certain work, only "authorized dealerships" and third parties that paid for the technology and right to access these systems and repair certain types of vehicles.[107]

These types of restrictions can severely limit competition in the market for add-on technologies, device repair services, and repair tools.[108] It also makes it very difficult for security firms, owners, and others to uncover safety and security issues, including faulty code that affects vehicle breaking, random air bag deployment, sudden automatic vehicle acceleration, and security vulnerabilities that hackers can use to take over a car using the Internet connection and its internal network.[109]

---

[101] FRED VON LOHMANN, ELEC. FRONTIER FOUND., UNINTENDED CONSEQUENCES: TWELVE YEARS UNDER THE DMCA 1 (2010), http://bit.ly/1RhY4QK ("In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright infringement. As a result, the DMCA has developed into a serious threat to several important public policy priorities.").

[102] Amy Harmon, *Software Double Bind*, N.Y. TIMES (Aug. 31, 2001) http://nyti.ms/1P8VzIY. (relating to the DMCA exemptions are difficult to attain and limited in scope, which only apply to end users, not to the developers who make tools that facilitate the lawful exempt activities).

[103] *Coders' Rights Project Reverse Engineering FAQ,* ELEC. FRONTIER FOUND., http://bit.ly/1Uc1vbV (last visited Mar. 8, 2016).

[104] SIMON NINAN, ET AL., DELOITTE UNIV. PRESS, WHO OWNS THE ROAD?: THE IOT-CONNECTED CAR OF TODAY—AND TOMORROW 2 (2015), http://bit.ly/1pql30b.

[105] Jason Torchinsky, *Carmakers Want to Use Copyright Law to Make Working On Your Car Illegal*, JALOPNIK (Apr. 21, 2015, 12:05 PM), http://bit.ly/1TJgI4i.

[106] *Id*.

[107] Glyn Moody, *Dismantling the Repair Monopoly Created by the DMCA's Anti- Circumvention Rules*, TECHDIRT (Feb. 8, 2016) http://bit.ly/22gz5za (leading to the formation of the Digital Right to Repair Coalition in 2013 to combat the anti-circumvention restrictions imposed of automobile repairs and more recently renamed the Repair Association).

[108] Kit Walsh, et al., ELEC. FRONTIER FOUND., Comment In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C., Docket No. 1201, 19 (Feb. 6, 2015) http://1.usa.gov/1Mjfbu9.

[109] Kim Zetter, *Researchers Hacked a Model S, But Tesla's Already Released a Patch*,

A number of industry groups have called this law a blanket protection of business interests and noted that the law stifles research into automobile software and security audits.[110] Indeed, if independent researchers could have legally accessed the context-sensitive emissions control software running Volkswagen cars, they might have discovered the emissions problem sooner, and at lower cost.[111] A party that circumvents the protections risks prosecution, so unless there is an exemption in place, they access the code at their peril. Recently, the Librarian of Congress, who possesses the authority to grant exemptions, issued one for vehicle owners to circumvent access restrictions on cars.[112] This may lead to innovation and increased efficiency as owners "crack the code" and understand how their system controls and talks to the vehicle hardware, the in-dash entertainment system, and manages energy consumption. It may also expose system security vulnerabilities.[113] There are risks too—owners might make modifications that render a particular vehicle unsafe, environmentally unfriendly, or expose their car network to Internet-based hacks. Ultimately, some interesting results are likely once people realize that this exemption has been granted and start taking advantage of it.

Copyright law can also be used to block interoperability between connected devices.[114] For two devices to communicate, they need to distribute code and perform actions that involve sharing code.[115] If the owner of an object's code treats it as proprietary and blocks interaction, then the device may live in a gated community, where it acts on its own based on its own code's directions.[116]

WIRED MAG. (Aug. 6, 2015, 6:00 AM) http://bit.ly/1QTkhmi ("The researchers found six vulnerabilities in the Tesla car and worked with the company for several weeks to develop fixes for some of them."); Andy Greenberg, *Hackers Remotely Kill a Jeep On The Highway—With Me In It*, WIRED (July 21, 2015), http://bit.ly/1MiZSSb.

110 *See*, *e.g*., Kit Walsh, *Researchers Could Have Uncovered Volkswagen's Emissions Cheat if Not Hindered by the DMCA*, ELECTRONIC FRONTIER FOUND. (Sept. 21, 2015), http://bit.ly/1Uc5sNP; Parker Higgins, *Who's Driving This Thing? Anti-DRM Victories and Milestones: 2015 in Review*, ELEC. FRONTIER FOUND. (Dec. 27, 2015) http://bit.ly/1nJFDqt.

111 Martin Anderson, *DMCA may have protected Volkswagen from 'Defeat Device" Discovery, Claims U.S. Senator*, THE STACK (Oct. 15, 2015) http://bit.ly/1RhJyZg; *see* Walsh, *supra* note 110.

112 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944 (Oct. 28, 2015) (to be codified in 37 CFR part 201). (specifying the exemptions included security research, which covers vehicles and many other devices and, however, until the three-year exemption period ends, the public and independent security researchers can evaluate automotive software and software that protects a variety of IoT objects).

113 *See* Masnick, *supra* note 96.

114 Aaron K. Perzanowski, *Rethinking Anticircumvention's Interoperability Policy,* 42 U.C. DAVIS. L. REV. 1549, 1554-55 (2009).

115 *Id.*

116 Jacqueline Lipton, *The Law of Unintended Consequences: The Digital Millennium*

Even if an object's code is in a compiled, readable format, if another device accesses that code, the second device may be a tool for violating the anti-copying protections and the anti-circumvention statute. Recently, a federal appellate court decided that software application programming interfaces ("APIs")[117] are subject to copyright protection.[118] This decision could significantly impact device interoperability, limit interactions among IoT devices, and slow IoT market growth and object integration.

Finally, copy protections and anti-circumvention laws are being used in some circumstances to prevent creation of other devices or products that work with, or substitute for, a company's device.[119] Ink cartridge manufacturers use authentication chips and software technologies to ensure only authorized printer ink cartridges are being used with their printers.[120] And the manufacturer of a particular type of coffee maker used the same type of protections to ensure that their single-serve brewing systems use only authentic manufacturer single-serving pods—K-Cup pods.[121] These companies have fought several legal battles over their use of firmware to control the use and replacement of add-on products that interact with their devices.[122] The result has been spilt; some of these battles have been successful, others have not.[123]

The tension between a strong system of copyright protection and a variety of consumer and business interests will continue to play out in the courts. It will be interesting to see how the Federal Trade Commission and Congress respond and attempt to strike the right balance as the IoT market matures and the legal battles continue.

Copyright Act and Interoperability, 62 WASH. & LEE. L. REV. 487, 497 (2005).

117 *See Definition of API*, PC MAG., http://bit.ly/1V7sIMq (last visited Feb. 27, 2016)

> [Application Programming Interface ("API") is a] language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol. APIs are implemented by writing function calls in the program, which provide the linkage to the required subroutine for execution. Thus, an API implies that a driver or program module is available in the computer to perform the operation or that software must be linked into the existing program to perform the tasks.

Id.

118 Oracle Am., Inc. v. Google, Inc., 750 F.3d 1339 (Fed.Cir. 2014).

119 *The Anti-Circumvention Rules of the Digital Millennium Copyright Act - Changing the Digital Landscape*, STOEL RIVES LLP. (Mar. 1, 2002), http://bit.ly/1Ln744N.

120 Mike Josiah, WHAT DO YOU REALLY KNOW ABOUT CARTRIDGE CHIPS, UNINET 2-3 (2012) http://bit.ly/1pqcthQ.

121 Jennifer Abel, *Here's a list of ways around Keurig 2.0 Machine Restrictions,* CONSUMER AFFAIRS. (Feb. 4, 2015), http://bit.ly/1SNO4Op

122 Jade Smarda, *Fighting for Market Share*, FARUKI, IRELAND & COX P.L.L. (Mar. 11, 2014). http://bit.ly/1QTs6IC.

123 Jack Linshi, *Here's What You Need to Know About the War on K-Cups*, TIME (June 23, 2014) http://ti.me/1nJBId8.

D. The Security Dream

Anything connected to the Internet can be hacked.[124] Currently, there are no generally accepted security standards or protocols for IoT device operations.[125] IoT companies are not required to encrypt data that they collect and transmit.[126] Objects are often connected using default admin settings and passwords that are never changed, and regularly use passwords and credentials that can easily be discovered using conventional tools and open-source software.[127] One recent study of several popular IoT devices uncovered a variety of major vulnerabilities, including lack of encryption when sending data, insecure firmware that can be easily hacked, and weak or poorly protected access credentials.[128] Incredibly, 70% of the devices studied transmit data over unencrypted network services and 80% use simplistic passwords like "1234."[129] At least one cybersecurity firm has uncovered a cyberattack that involved over 750,000 phishing and spam e-mails launched from IoT "thingbots" including TVs, refrigerators, and connected multi-media centers.[130] Such an attack represents the beginning and not the end, and IoT is going to lead to many more hacks, on a larger scale, in the future.[131]

The safety and security issues relating to IoT are particularly concerning when the connected objects relate to critical services, such as fire alarms, radon detectors, and other health and safety monitors, that are implemented by automatic systems that do not require human intervention.[132] Cyber security certainly is as important for IoT as it is for other technologies and systems involving connected communication and safe digital transfer or storage of information.[133] A number of existing laws provide tools to ensure that IoT companies consider security and privacy issues as they create and connect new devices.[134] But at

---

124 Rachel Z. Arndt, *Now That Everything Is Connected, Everything Will Get Hacked*, POP. MECHS. (Apr. 11, 2014) http://bit.ly/1QSHQdu.

125 *Securing the Internet of Things: A proposed Framework*, CISCO, http://bit.ly/1QTosP3 (last visited Feb. 29, 2016).

126 *Id.*

127 *Id.*

128 Press Release, Hewlett-Packard, HP Study Finds Alarming Vulnerabilities with Internet of Things (IoT) Home Security Systems (Feb. 10, 2015), http://bit.ly/1pHr880 [hereinafter Hewlett-Packard].

129 *Id*.

130 Press Release, Proofpoint Inc., Proofpoint Uncovers Internet of Things (IoT) Cyberattack (Jan. 16, 2014), http://bit.ly/1TJtvDU.

131 Hewlett-Packard, *supra* note 128.

132 *In the privacy of your own home*, CONSUMER RPTS. (Apr. 30, 2015), http://bit.ly/1SNTs4b.

133 Omner Barajas, *How the Internet of Things (IoT) is Changing the Cybersecurity Landscape*, SEC. INTELLIGENCE (Sept. 17, 2014), http://ibm.co/1Uc4WPV.

134 *See* U.S. FED. TRADE COMMISSION, *supra* note 20, at viii (stating these laws include

some point, perhaps Congress will pursue flexible legislation that strengthens existing data security enforcement tools and provides for notifications to consumers when a breach occurs.[135] This type of legislation must also protect against unauthorized access to personal information collected by IoT devices and improper interference with the device's functions.[136]

Because IoT involves hyper-connectivity and meta-data analysis of collected information, IoT companies often create sensitive information about consumers, their behaviors, and make inferences regarding future behaviors that might put the consumers at greater risk in the event that a data breach occurs.[137] Consider how valuable an individual's home security and thermostat settings would be to someone who wants to understand another's patterns and find a good time to break into their home. Imagine that someone could hack a pacemaker and take control of its activities, putting him at risk of serious bodily harm and even death. Without certain reasonable security guarantees, people will be hesitant to adopt IoT solutions on a large scale.[138] Companies involved in IoT will need to develop appropriate security protocols for the objects they connect and the data they collect. They will also need to develop security enforcement mechanisms, de-identify users' data (if appropriate), and allow for context-awareness protections for the connected objects. While significant security improvements are needed, many of the security upgrades that have been applied to the world-wide-web could be used with IoT objects and their protocols for sending and receiving information.

V. CORPORATE OVERSIGHT OF CONNECTED DEVICES

Corporations have used IoT to control and monitor the use or behavior of the devices they sell and assert their intellectual property rights.[139] Some companies use IoT to lock down hardware ranging from electronic control units ("ECUs") that manage car systems to operating systems that manage mobile

---

the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children's Online Privacy Protection Act. Other laws might apply to IoT, depending on the industry, product, or activity at issue).

135 *Comparison of Four Data Breach Bills Currently Before Congress (114th Session),* CTR. FOR DEMOCRACY & TECH. 1 (Sept. 10, 2015), http://bit.ly/21s1MXD.

136 *Id*.

137 Brian Prince, *Consumers Ready for Internet of Things, But Fear Data Privacy and Security Implications: Survey*, SEC. WEEK (June 23, 2014), http://bit.ly/1pq9VjS.

138 Kelsey Flittner, *Surprised? Turns Out, Consumers Don't Trust IoT Security*, AUTH0. (Nov. 6, 2015), https://auth0.com/blog/2015/11/06/surprised-turns-out-consumers-dont-trust-iot-security/

139 John F. O'Rourke & Patrick Soon, *The Internet of Things and the Issue of IP Rights (Part I),* INSIDE COUNSEL (Mar. 28, 2014), http://bit.ly/21rXYWr.

devices.[140] There are problems and opportunities that arise from these activities, and the numbers of companies that are using IoT as a formal business tool are growing.

There are a couple high profile examples of brewing IoT problems. One of the more prominent examples is Keurig, a one single-serve coffee brewing machine received an IoT upgrade in 2014 that made it incompatible with competitors' single-serve coffee pods and the eco-friendly pods sold by that same manufacturer. [141] The new line of Keurig 2.0 machines would only operate when using authentic Keurig-brand K-Cup pod, which contains a special seal that the machine must sense before brewing a cup of coffee using the inserted pod.[142] Otherwise, a user would receive an error message and the machine would not operate.[143] This is a traditional digital rights management system applied to the coffee industry.[144] It could be a beneficial improvement for the users—the scanning system allows the machine to optimize brew temperatures for different types and sizes of cups.[145] But not everyone embraced these benefits and the changes Keurig made to its machines.[146] Not surprisingly, the customer and competitor backlash was immediate and intense, with customers proclaiming "you shouldn't have to hack your coffee."[147] Keurig's move also led to antitrust lawsuits[148] and special websites that offered hacks to circumvent the "authorized pod" sensing IoT technology.[149] In response, Keurig backtracked and reintroduced its old pods.[150] But it is still unclear whether competitors' pods of a similar shape will be accepted or rejected by the IoT brewing machines.

Similar to the single-cup brewing market, the printer market is driven by

---

140 Valerie Scarsellato, *Get There Faster: IoT and ECU Consolidation Drive Auto Innovation*, INTEL (July 10, 2014), http://intel.ly/1Xr5Bes.

141 Fred Barbash, *Keurig's K-Cup Screw-up and How It K-Pitulated to Angry Consumers*, WASH. POST (May 7, 2015), http://wapo.st/1pHrOu9.

142 *See* Josh Dzieza, *Inside Keurig's Plan to Stop You From Buying Knockoff K-Cups,* THE VERGE (June 30, 2014, 12:29 PM), http://bit.ly/21rUOlf (noting Green Mountain Coffee owned several key patents covering the single-cup brewing pods, but they expired in 2012).

143 See Dzieza, *supra* note 142.

144 *Id*.

145 See Barbash, *supra* note 141.

146 Josh Dzieza, *Keurig's Attempt to 'DRM' its Coffee Cups Totally Backfired*, THE VERGE (Feb. 5, 2015, 1:32 PM), http://bit.ly/1QYI0Ov.

147 *Id*.

148 *See In re* Keurig Green Mountain Single-Serve Coffee Antitrust Litig., No. 14-md-02542-VSB (S.D.N.Y. June 5, 2014).

149 Drew Prindle, *A Competitor Found a Permanent Way to Brew Off-Brand K-Cups in Keurig 2.0 Machines*, DIG. TRENDS (Feb. 2, 2015), http://bit.ly/1Uc2MzP.

150 See Barbash, *supra* note 141.

sales of follow-on products, specifically via replacement ink cartridges.[151] Many printer original equipment manufacturers ("OEMs") have implemented technologies to ensure that their very expensive printers, which are sold at or below the manufacturing cost, are not filled with non-OEM ink cartridges.[152] These technologies include special chips embedded in the authorized cartridges, which the printer must sense before it authenticates and accepts a new cartridge.[153] They also involve communications between the printer and the authorized cartridge distribution partner when the printer senses that its toner levers are low and the cartridges will need to be replaced. Though one appellate court has ruled that circumvention of an ink cartridge authentication system to allow use of other ink toner cartridges with a printer does not violate the DMCA, printer manufacturers continue to use microcontrollers and other technologies to limit the parts and follow-on products that can be used with their devices.[154] As the IoT market grows, other companies, particularly manufacturers, will likely use similar strategies to limit competition in the market, manage user interactions, and improve the user experience and service records for their devices.[155]

One creepy example of the IoT revolution is Mattel's talking Barbie doll.[156] Mattel recently released a talking toy that can "engage in two-way conversation" via an embedded microphone and a Wi-Fi connection that's engaged when a child holds down a button on the dolly's belt.[157] When someone talks to Barbie, the conversation is recorded and sent to a server back at the company that makes the voice recognition technology powering this Barbie.[158] There, speech recognition software—think of the Barbie version of Apple's Siri[159]—

---

[151] John C. Dvorak, *The Secret Printer Companies are Keeping From You*, PC MAG. (Sept. 6, 2012), http://bit.ly/1QYI54A.

[152] *Id.*

[153] *Id.*

[154] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 564 (6th Cir. 2004) (alleging Static Control reverse-engineered the chip technology used by Lexmark to identify "valid" toner cartridges that could be used in its printers, then sold these chips to other toner manufactures who made generic toners that were lower cost and useable in the Lexmark machines, which resulted in this lawsuit).

[155] *See also* The Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004) (holding that manufacturer of replacement garage door openers did not violate the anti-trafficking provision of DMCA and plaintiff manufacturer failed to prove that owners access to openers was unauthorized or that its rights were infringed under the Copyright Act).

[156] *See generally* HELLO BARBIE MESSAGING Q&A, MATTEL (2015), http://bit.ly/1Uc9rtH ("Hello Barbie is the first fashion doll that can have a two-way conversation with girls.").

[157] James Vlahos, *Barbie Wants to Get to Know Your Child*, N.Y. TIMES (Sept. 16, 2015), http://nyti.ms/250Kw06.

[158] *Id.*

[159] *See Siri*, APPLE, http://apple.co/1M39Egr (last visited Feb. 27, 2016) (explaining Siri

interprets the child's statements and sends back a pre-programmed response.[160] That is right, the doll "talks" with and to the child. At least one advocacy group sought to avoid the launch of this doll, and privacy pundits have learned that Mattel's partner, Toy Talk, stores all of the children's conversations and the conversations of others who interact with the doll.[161]

Whether the company is acting as a "listener," controlling the object or its "behaviors," or limiting the people or other objects that its products "interact with," these activities have significant ramifications for a lawyer's investigatory focus in the litigation context. Suppose this series of hypotheticals, a lawyer might send a subpoena to ToyTalk seeking the audio records from its client's Barbie doll for use in a domestic abuse case. A personal injury lawyer might be interested in the data a manufacturer collects from their client's wearable fitness device. An insurance carrier might seek records reflecting the information an auto manufacturer collects through a connection with an in-dash entertainment system and the data relating to car speed and breaking that resides in the vehicle control system. Perhaps the technology could tattle-tale on the driver, stating she was checking her e-mail while driving 70 miles an hour or being inattentive, or feeling angry and upset after finding out her boyfriend was cheating. Regardless of the source, the information that IoT companies collect and share are giving lawyers rich new evidence stores that should be explored in an effort to ferret out interesting information that impacts their case.

VI. WEARABLE IOT DEVICES

Wearable IoT devices include a wide range of medical devices and health and fitness products, including casual wearable fitness devices, like the Apple watch or Fitbit, and connected pacemakers and insulin pumps. Some reports indicate that over 28% of consumers will own wearable IoT technology by the end of 2016.[162] Wearable fitness devices now monitor geolocation as well as heart rate, pulse, calorie consumption, sleep patterns, and other biological data.[163] Most wearable devices monitor very sensitive personal and health data.[164]

---

voice-recognition software).

[160] Bruce Horovitz, *High-Tech 'talking' Barbie bad idea, group says*, USA TODAY, (Mar. 11, 2015, 2:45 PM), http://usat.ly/1S0lnLW.

[161] *See Children's Privacy Policy*, TOYTALK (last revised Jan. 11, 2016), http://bit.ly/1QTsF5d (explaining that Mattel and ToyTalk have responded to these concerns by confirming that the recorded conversations will not be used to advertise or market products to children and noted that parental consent is required to set up a Hello Barbie account and can set various presets and preferences).

[162] ACCENTURE, *supra* note 21, at 3.

[163] *See e.g.*, FITBIT, FITBIT CHARGE HR PRODUCT MANUAL, http://fitbit.link/1U2dZn8 (last visited Feb. 27, 2016) (describing different monitoring aspects of the Fitbit device).

And the devices are constantly storing data that users unconsciously create when going about their day.[165] They also transmit the data to the manufacturer or another entity for analysis.[166] This data may be used in a court of law. [167]

The information wearable fitness and health devices collect can be highly relevant in determining what might have happened to an individual at a particular time. Wearable technologies and the data they collect have already been used in a few lawsuits.[168] For instance, a Fitbit, which is a wearable object that tracks health-related information, has been used as evidence of an individual's diminished physical activity resulting from a work-related injury in a Canadian personal injury case.[169] The plaintiff was injured when she was working as a personal trainer, and she used her Fitbit data to prove she deserved compensation for the injury to show that her post-injury activity levels were lower than the baseline for someone of the same age and profession.[170] With the help of a startup analytic company that aggregates Fitbit data and prepares analytical reports, her lawyers contrasted her personal data with the general population's health and wellness data gleaned from other Fitbit device users.[171]

Arguably, insurers and employers seeking to deny injury and disability claims could just as easily use wearable devices that collect health information to support their position. It is generally seen as illegal for employers and insurers to force people to use the wearable devices.[172] But, if individuals decide to use them voluntarily, an individual might see a request seeking court-ordered production directed to the manufacturer or for the device or application that stores or reports wearable device data.

The fact that wearable device data may have evidentiary value should come as no surprise given the fact that evidence from self-tracking devices has already found its way into the courtroom.[173] Courts have used data from GPS devices and apps used for tracking bike rides in cases involving bike accidents.[174] Some police departments routinely use surveillance technology like

---

164 Langley, *supra* note 72 at 1642.

165 Kate Crawford, *When Fitbit is the Expert Witness*, ATLANTIC (Nov. 19, 2014), http://theatln.tc/22fb92A.

166 *Id.*

167 *Id.*

168 Parmy Olson, *Fitbit Data Now Being Used*, Forbes (Nov. 16, 2014, 4:10 PM), http://onforb.es/1pqdl6e.

169 Crawford, *supra* note 165.

170 *Id.*

171 *Id.*

172 Tracy L. Moon Jr. & Beth P. Zoller, *How to Manage Wearable Devices at Work*, XPERTHR, http://bit.ly/1QTWAdq (last visited Feb. 29, 2016).

173 Crawford, *supra* note 165.

174 Patrick Brady, *Prosecution Rest in LA Road Rage Case. Defense will Call Witness on Monday,* VELONEWS (Nov. 3, 2009), http://bit.ly/1WlOPgB. (reporting that in vehicle/bicycle accident case, an accident reconstruction expert analyzed GPS files from the

Automatic License Plate Readers ("ALPR"), mounted on police cars or on objects like road signs and bridges, to photograph thousands of plates per minute and track motorists' movements.[175] Private companies are also collecting license plate photos and geo-tagged images to sell that data to law enforcement, insurers, and financial institutions.[176] They consider this analogous to taking photographs in public and disseminating the information, an activity protected by the First Amendment.[177] This is one aspect of a larger trend towards surveillance of private citizens' activities.[178] One of the differences between these types of technologies and the wearable devices lies in the fact that wearable tracking is voluntary—whether the user's authorization comes from an informed position is debatable.[179]

Importantly, many wearables and the software that collects and analyses their data interpret the wearer's daily activities in comparison to predetermined baselines and standards set by the manufacturer. [180] For example, Fitbits monitor sleep patterns, determine how many hours a user sleeps, and determines the quality and efficiency of that sleep.[181] That information might be useful for an employer defending itself against a worker's compensation claim, particularly if the sleep analysis reports that the worker was "sleep deprived" at the time of the accident. The wearer would be compared to the "average" sleeper as determined by the manufacturer's algorithm.[182] So regardless of her personal optimal sleep duration or the outside forces that might have impacted her sleep the night before the accident occurred she would be categorized and measured against a population baseline. Other wearable devices collect different data, work differently, and use different algorithms and standards to analyze data and report trends and health information in comparison to the general popula-

---

cyclists involved in an altercation with an enraged vehicle driver with a pattern of incidents involving cyclists).

[175] Conor Friedersdorf, *An Unprecedented Threat to Privacy*, THE ATLANTIC (Jan. 27, 2016), http://theatln.tc/1V7umO5 (noting one private company has taken approximately 2.2 billion license-plate photos to date, and each month it captures and permanently stores 80 million more geotagged images).

[176] *See id.*

[177] David Sirota, *Companies test their First Amendment Right to Track You,* THE OREGONIAN (Mar. 8, 2014, 7:10 AM), http://bit.ly/1P93fuR.

[178] ACLU, *supra* note 48.

[179] Alan Martin, *Step and save: The Truth about Wearables and Health Insurance*, WAREABLE (May 21, 2015), http://bit.ly/1QSJbkO.

[180] Samuel Gibbs, *The future of wearable technology is not wearables – it's analyzing the data,* GUARDIAN (Jan. 6, 2015, 4:18 PM), http://bit.ly/1nJKtnD.

[181] *See What should I know about sleep tracking?*, FITBIT, http://fitbit.link/22gK4IR (last updated Mar. 7, 2016) (explaining Fitbit sleep-tracking technology).

[182] *Id.*

tion.[183] All of this means that before wearable evidence is used in a case, lawyers, experts, and the courts need to understand what they mean and the limitations inherent in its analysis.

Prosecutors and defense counsel seeking incriminating or exculpatory evidence can also use them where each side can.[184] In a Pennsylvania rape case, the Fitbit data contradicted the statements of the alleged victim by showing that at the time of the crime, she was awake and walking around, though she claimed she had been attacked in her sleep.[185] Now she is facing misdemeanor charges because her story has been contradicted by her Fitbit data.[186] Meanwhile, some wearables, like Google Glass, transmit location information, take photos and videos, and perform web searches.[187] Imagine if a person who witnesses a crime while wearing this device took pictures of the perpetrator and the scene after the crime occurred?[188] Unlike surveillance technology, humans tend to look at something interesting or important.[189] Technology like Google Glass might help them record valuable eye-witness evidence. The device would contain evidence like photos and geolocation information with time stamps that police could use to investigate and prosecute the crime and civil litigants can use to pursue their cases.

VII. CONNECTED CARS

Another category of IoT technology relates to connected transportation. Today, many cars have sophisticated software that connects the driver to many remotely managed features including real-time navigation, mapped points-of-interest, dash-based Internet search, streaming music, and mobile device app connectivity.[190] IoT implicates a wide variety of technologies involved with

---

183 *See Fitbit Compatible Apps*, FITBIT, http://fitbit.link/22gK4IR (last visited Feb. 29, 2016). (listing over 30 apps that are compatible with the Fitbit devices); s*ee also Thermos Hydration Bottle with Smart Lid,* FITBIT, http://fitbit.link/1RiLRoO (last visited Feb. 29, 2016) (announcing a partnership with Thermos involving a smart lid hydration bottle and app that allows users to automatically track their water intake).

184 Crawford, *supra* note 165.

185 Mariella Moon, *Fitbit tracking data comes up in another court case,* ENGADGET (June 28, 2015), http://engt.co/1QTm8HR.

186 Brett Hambright, *Woman staged 'rape' scene with knife, vodka, called 9-1-1, police say*, LANCASTER ONLINE (June 19, 2015), http://bit.ly/1RK7Vcv.

187 Ryan Goodrich, *Google Glass: What It Is and How it Works*, TOM'S GUIDE (Oct. 14, 2013, 9:38 PM), http://bit.ly/1M3aZDS.

188 Kashmir Hill, *Google Glass Will Be Incredible For The Courtroom*, FORBES (Mar. 15, 2013, 5:02 PM), http://onforb.es/1RK7YVO. The court used Strada biking data, security camera video, traffic accident reconstruction expert, and eyewitness testimony in a pedestrian/biker accident in preliminary hearing. *Id.*

189 *Id.*

190 *Smartphones on wheels,* ECONOMIST, Sept. 6, 2014, http://econ.st/1UcdRRn.

running and monitoring connected cars, including connected control systems, Event Data Recorders ("EDRs"), and other vehicle telematics.[191] Vehicle control software may use proximity sensors to identify collision risks and automatically engage the brake, survey blind spots and report objects, and park a vehicle without driver assistance.[192] And a number of well-known tech companies are currently testing driverless cars and intend to offer self-driving cars in the near future.[193] These cars will be connected to the Internet, share data about their location and traffic conditions, and will likely make an interesting and growing target for hackers.

Particularly in light of the Volkswagen emissions scandal,[194] the connected control systems on vehicles are of great interest to the public. Vehicle manufacturers have fought long and hard to ensure that backyard tinkerers, competitors, and independent repair shops cannot access the software on their control systems or modify it.[195] Consumers and other interested parties have sought exemptions to the DMCA's anti-circumvention provisions relating to the repair, diagnosis, and modification of software running on vehicles.[196] Essentially, these protections allow manufacturers to exert a lot of control over how the end user interacts with the software and it prevents owners and third parties,

---

191 49 C.F.R. § 563.5 (2015). ("[An Event Data Recorder is] a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event…intended for retrieval after the crash event.").

192 *See* STEVEN H. BAYLESS, ET AL., INTELLIGENT TRANS. SOC. OF AM., CONNECTED VEHICLE INSIGHTS: TRENDS IN ROADWAY DOMAIN ACTIVE SENSING 2-4 (2008), http://bit.ly/1SO8YNn (discussing advancements of vehicle control software).

193 *See*, *e.g.*, Alice Truong, *Tesla Just Transformed The Model S Into A Nearly Driverless Car*, QUARTZ (Oct. 14, 2015), http://bit.ly/1RiFkKH; Cadie Thompson, *There's One Big Difference Between Google and Tesla's Self-Driving Car Technology*, TECH INSIDER (Dec. 5, 2015, 12:00 PM), http://bit.ly/1P8YjpK; Feann Torr, *Next-gen Audi A8 Drives Better Than You*, MOTORING AU (Oct. 22, 2014), http://bit.ly/1QYIXGG; Tom Risen, *Uber, Lyft Poised to Win On Driverless Cars,* U.S. NEWS (Nov. 13, 2015, 4:05 PM), http://bit.ly/1QSJzzv.

194 Russell Hotten, *Volkswagen: The Scandal Explained*, BBC NEWS (Dec. 10, 2015), http://bbc.in/1pHsi3n (discussing the current law by which the Librarian of Congress grants an exception, any researcher who directly accessed the fraudulent emissions software on the Volkswagen cars could be exposed to a lawsuit for violation of the DMCA anti-circumvention provision.).

195 *See, e.g.,* Darin Bartholomew, John Deere, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, at 5 (2015), http://1.usa.gov/1RhQoxX (arguing that users own the vehicles or equipment are authorized to operate it, but they only have a limited license to the software that controls it).

196 *See*, *e.g.*, Pete Bigelow, *Automakers to gearheads: Stop repairing cars,* AUTOBLOG (Apr. 20, 2015, 10:31 AM), http://bit.ly/1WlTPBR; Parker Higgins, et al., *Victory for Users: Librarian of Congress Renews and Expands Protections for Fair Uses*, ELEC. FRONTIER FOUND. (Oct. 27, 2015), http://bit.ly/1U2h0DO.

like independent, non-dealership repair shops from diagnosing problems, servicing, or modifying a vehicle. The automobile manufacturers, in turn, have argued that this type of interference with the vehicle management software can lead to serious safety issues, violate their copyright rights and other interests in the hardware and software, and lead to modifications with unintended consequences.[197] For the next three years, certain owner activities relating to vehicle control systems have been exempted from the anti-circumvention restrictions in the DMCA.[198] Additionally, certain security research involving vehicles is subject to a similar exemption.[199]

One significant issue with connected cars is their vulnerability to hacking.[200] Nothing brought the IoT security issues home more than the recent news that two Black Hat security conference presenters had successfully hacked a Jeep.[201] The security researchers found an exploitable vulnerability in the vehicle's entertainment system and used it to send commands to its dashboard functions, steering, brakes, and transmission system rendering the driver powerless. [202] They were also able to perform surveillance on the vehicle from the comfort of their own remote computing device.[203]

All of these troubling risks are made possible by the fact that automakers are turning vehicles, in essence, into "smartphones" using communication technology that controls the entertainment and navigation systems, enables phone calls, and provides a Wi-Fi hotspot.[204] That communication technology provides the access, and from there hackers can start rewriting code that controls all aspects of the vehicle's functions and communication with the car's internal computer network—which connects the engine and wheels to the control sys-

---

197 *See* Ford Motor Co. v. Autel US Inc., No. 2:14-cv-13760 (E.D. Mich., Sept. 29, 2014) (noting that this is an automaker filing suit against a diagnostic equipment company that allegedly hacked into an automobile's diagnostic software system in order to improve the diagnostic software.).

198 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,953-55 (Oct. 28, 2015).

199 Higgins, *supra* note 196.

200 *See*, *e.g.*, STEPHEN CHECKOWAY, ET AL., COMPREHENSIVE EXPERIMENTAL ANALYSES OF AUTOMOTIVE ATTACKS SURFACES 4-5 (2011), http://bit.ly/1U2i4Yq; Razvan Muresan, *Auto Makers' Strategy of Turning Cars into Four-wheel Smartphones will Bring Enterprise Security into Focus,* BITDEFENDER (Oct. 30, 2015), http://bit.ly/1RKj8d5; Greenberg, *supra* note 109.

201 *Id*; *see also* Press Release, Fiat-Chrysler Automobiles, FCA US LLC Releases Software Update to Improve Vehicle Electronic Security and Communications System Enhancements (July 16, 2015), http://bit.ly/1QSTW6y (discussing that hackers released the details relating to their exploitation of a vulnerability involving the Chrysler Uconnect technology at a Black Hat conference, which would allow remote GPS tracking of hacked vehicles and remote control of the dashboard).

202 Greenberg, *supra* note 109.

203 *Id.*

204 *See* Muresan *supra* note 200.

tems.[205] The Jeep incident is not the first time someone has engineered a remote car hack—several years ago a team of university researchers hacked a sedan over the Internet and disabled the locks and brakes remotely.[206]

Recently, the auto industry issued privacy principles and set up a new group to share cyber security information between companies.[207] Nonetheless, much more focus on the issues raised by connecting cars to the Internet is sorely needed. While some legislators have noticed the successful research hacking and have attempted to press the automakers and obtain assurances that they are taking security issues seriously,[208] ultimately stronger legislation may be the answer.[209] However, this might only come after consumers and manufacturers feel the impact of connected car hacks on a massive scale.

VIII. EDISCOVERY OF IOT INFORMATION

Lawyers and clients should consider what preparations to take now so that they are ready when IoT-related e-Discovery issues arrive. IoT objects will present many challenges in the e-Discovery context. There are limitations on wearable devices and other IoT objects and the information they collect, however, the technology is becoming more sophisticated, accessible, and shareable every day.[210] When information is shared among multiple objects—a watch, a smartphone and a cloud computing system, the preservation issues are complex.[211] Also, some of this information can be ephemeral and distributed across multiple platforms and provider systems.[212] While the Federal Rules of Civil

---

[205] *Id.*

[206] CHECKOWAY, *supra* note 200 at 4-5.

[207] ALL. OF AUTO. MFR., INC. & ASS'N OF GLOB. AUTOMAKERS, INC., CONSUMER PRIVACY PROTECTION PRINCIPLES: PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES 2-3 (2014), http://bit.ly/21s60ON.

[208] SEN. ED MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 1 (2015), http://1.usa.gov/1Lnf2uR; Andy Greenberg, *Here's The Letter A Senator Sent to 20 Auto Makers Demanding Answers On Car Hacking Threats*, FORBES (Dec. 4, 2013, 11:28 AM), http://onforb.es/1QSYEkG; Andy Greenberg, *Senate Report Slams Automakers for Leaving Cars Vulnerable to Hackers*, WIRED (Feb. 9, 2015, 11:11 AM), http://bit.ly/250FRvh.

[209] Grant Gross, *Senators to Push Privacy, Security Legislation for IoT, Connected Cars*, PC WORLD (Feb. 11, 2015, 1:15 PM), http://bit.ly/1SO9Lhu.

[210] Press Release, Consumer Tech. Ass'n, IoT Will Drive Consumer Tech Industry to $287 Billion in Revenues, an All-Time High, According to Consumer Technology Association (Jan. 4, 2016), http://bit.ly/1RiRa7G.

[211] Minsung Jang, et al., *Personal Clouds: Sharing and Integrating Networked Resources to Enhance End User Experiences* 1, 3 (2014), http://b.gatech.edu/1pke0W7.

[212] Ali Gholami & Erwin Laure, Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments 1 (Jan. 7, 2016) (unpublished manuscript), http://bit.ly/1TJHp9a.

Procedure provide some flexible guidance for dealing with this technical revolution, and counsel against "a limiting or precise definition of electronically stored information,"[213] companies that store data from IoT devices will need to develop guidelines for preserving, collecting, and producing it when the duty arises.

Additionally, lawyers will need to understand how courts analyze the possession, custody, and control issues in the IoT context. These questions will be complicated, and they may involve an analysis of the relative cost and burden associated with owner focused or manufacturer focused production obligations. [214] For example, if an owner must jailbreak her device and hire an expensive expert to retrieve data off her wearable device, but the manufacturer can export her data with relative ease, courts should be considering such practical realities when deciding their respective obligations.[215] Moreover, access controls, privacy restrictions, and contractual obligations will play a role in determining the appropriate process for engaging in e-Discovery of IoT data.[216]

One of the practical problems relating to IoT information is that each of the device manufacturers collect data in their own way. And health tracking platforms do the same. It may not be cleanly preserved or collected without undertaking significant efforts at a significant cost. This makes it particularly difficult to develop standard processes for preserving, collecting, reviewing, and producing information from a wide variety of wearable devices using their APIs or built in data reporting and download features. It also makes it hard to aggregate data from different devices and standardize it to obtain big data metrics based on the data collected from all wearable devices. Given these issues, the cost associated with collecting and using this type of data could be prohibitive, given the value of a case and the damages at stake. [217] This is a prime area in which companies and e-Discovery vendors can innovate and create a strong market for flexible services and solutions involving a wide range of data from IoT devices. Undoubtedly, more lawsuits involving IoT data are coming, as more lawyers and litigants realize that the data is discoverable, relevant, and useful evidence that can support their case. It will be interesting to see how the market responds to IoT discovery issues.[218]

---

213 FED. R. CIV. P. 34.

214 FED. R. CIV. P. 26.

215 *Opinion 8/2014*, *supra* note 47, at 4.

216 KARIN RETZER, ET AL., MORRISON FORESTER, DATA PROTECTION MASTERCLASS: CYBERSECURITY & DATA PROTECTION CONCERNS- CURRENT AND UPCOMING RISKS 33 (Dec. 2, 2014), http://bit.ly/1pkepb7.

217 JAMES N. DERTOUZOS, ET AL., RAND CORP., THE LEGAL AND ECONOMIC IMPLICATIONS OF ELECTRONIC DISCOVERY: OPTIONS FOR FUTURE RESEARCH 3 (2008), http://bit.ly/1P98FGb.

218 DAVID Z. KAUFMAN, AM. BAR ASS'N, THE DUTY TO PRESERVE EVIDENCE 18-19 (2006), http://bit.ly/1MjcIjg.

IX. IOT OBJECT AS WITNESS

As wearables and other IoT objects find their way into the courtroom with more frequency, lawyers and the courts will need to determine how we will use them and their data as "witness" evidence. Alternatively, perhaps these sources treat it more like forensic evidence, and give it the same weight and credibility as scientific analysis or the results reported by an expert witness.[219] Not unlike scientific researchers or forensic experts, wearable technologies collect data, interpret it, and reflect it in reports that provide information about the user experience.[220]

It will be interesting to see what happens when a witness's sensory experiences—his or her sight, sound, feeling, taste, etc.—clash with the data reported by their wearable device. For example, if a biker testifies that they were traveling down a hill towards an intersection at about 15 miles per hour, but their wearable device or Strava app reports the speed down the slope at 25, as determined by a complicated three-dimensional GPS reading and reporting algorithms—the debate becomes which "witness" will the jury give more credit. Both systems for reporting experiences are fallible and fraught with errors. But if courts decide to prioritize or weigh IoT data-driven evidence over eyewitness statements or expert analysis, then legal experts must ensure that the algorithms used to analyze IoT data are understood and their imperfections are disclosed. [221] As one commentator notes, if devices are viewed as partial witnesses, counsels must understand that they carry biases and have their own worldview, based on their relationship with their environment.[222]

There is a significant risk that information generated by IoT objects, like the Fitbit data and its sleep analysis, would carry more evidentiary weight than the owner's own experience and view of her sleep patterns or alertness at the time an injury occurred.[223] As with forensics results, there is a significant risk that judges and jurors will conclude that device data does not lie or have an imperfect memory.[224] When wearable object data is being collected and interpreted by analytics companies using proprietary algorithms, counsel, judges and juries will need to understand what is happening under the hood, whether the results reported are reliable, and what evidentiary weight they should be given the context. The interpretive tools used to report IoT data are often highly subjec-

---

219 Crawford, *supra* note 165.

220 PRICEWATERHOUSECOOPERS LLP, THE WEARABLE FUTURE 31 (2014), http://pwc.to/1pqjijA.

221 Crawford, *supra* note 165.

222 *Id.*

223 *Id.*

224 *Id.*

tive or an imperfect fit for a number of users because of their crude analysis methods or the individual's health status and biology. This is but one area where possibilities are far ahead of the law on witness-style testimony from things connected the Internet.

Unfortunately, only time will tell whether this type of IoT information is seen as objective and unbiased evidence in the courtroom. If IoT evidence does not meet the requirements for introduction of scientific or forensic evidence, then it must be excluded.[225] If introduced, it may be given too much weight or credence in light of its significant limitations. Careful rules must be developed for use of this information by lawyers and in litigation.

Courts will also have to figure out how the Fifth Amendment protects the right against self-incrimination when the incriminating evidence involves user data created by a wearable device or communicated to a mobile computing device by an IoT object. In addition, the Sixth Amendment provides the Constitutional right to confront a witness who will offer evidence against the accused in a criminal prosecution. Inevitably, issues that involve "confronting" your wearable device or the ways companies know the best way to interpret the data it collects will arise. These situations pose fundamental philosophical questions regarding the witness who must be available for "confrontation," [226] which also involves issues with defining who should interpret the data—his device, the manufacturer, the service provider that collects and analyzes the data, or the company that provides the algorithms used to interpret it. The case law is going to be messy and inconsistent as courts start to dig into these concepts, consider the obstacles to use of IoT evidence in the courtroom, and sort the Constitutional issues and concerns. Additionally, as more and more litigants seek to collect information from wearables and other IoT objects for use in litigation, people's relationship with their wearables is likely to change. The lasting implication will yet be seen, once IoT objects can be used as "involuntary informants."

X. OUTLOOK: SURVIVING AND THRIVING IN A IOT WORLD

Some have called IoT a third major revolution—one built on the industrial revolution and the Internet revolution.[227] Lawyers and their clients are becoming more reliant on IoT to manage, monitor, and control their objects, interact, and work on the substantive aspects of their job. This means that Lawyers must hire good people who understand IoT technology and develop their own tech-

---

225 *See* FED. R. EVID. 702.

226 *Cf.* U.S. CONST. amend. VI.

227 *See* Elizabeth McGinn & Ty Yankov, *Treading Beyond the Iota of Fear: eDiscovery of the Internet of Things,* 20 ELECTRONIC COM. & LAW REP. 562, 562 (2015).

nical skills and knowledge. This guidebook provides a summation of basic information, legal issues, and practical concerns that should be considered. But, this resource needs to be applied to the real world, for each client, and in the context of each connected collection of objects, companies, and people.

Perhaps the day is coming when eyewitness testimony will become nearly irrelevant and will be replaced by the information devices provide about another's location, health, conscious state, and activities at any given time. But while IoT can reveal truths, those truths must be understood in context, in all their fallible or limited glory. This means that lawyers and their clients need to understand how their IoT objects work, what information they collect, where it is stored, how long it is stored, and who is obliged to keep it safe. Only after there is understanding of how the system works, then experts may make strategic decisions about legal risks, e-Discovery options and obligations, and appropriate use of IoT data in court.

A tech-savvy lawyer knows how to get the right evidence in the right format from her client or opponent. The IoT technology movement is a critical opportunity to continue a lawyer's self-education journey and learn more about the implications of IoT on lawyering in the Information Age. Welcome to a brave New World.