Minnesota Journal of Law, Science & Technology

Volume 19 | Issue 2 Article 5

6-2018

# Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things

Jane Kirtley

Scott Memmel

# Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things

**Jane E. Kirtley* & Scott Memmel+**



---



* Silha Professor of Media Ethics and Law, and Director, Silha Center for the Study of Media Ethics and Law, Hubbard School of Journalism and Mass Communication, University of Minnesota; Affiliated Faculty Member, University of Minnesota Law School.

+ PhD Student and editor, Silha *Bulletin*, Hubbard School of Journalism and Mass Communication, University of Minnesota.

## I. INTRODUCTION[1]

One morning in April 2015, a father walked into his three-year-old son's room, probably expecting to hear the sounds of his son talking or playing, or other "ordinary" household sounds.[2] Instead, the child's father heard an adult male voice come through the baby monitor, saying "Wake up little boy, daddy's looking for you."[3] On other occasions, the child's father had heard the voice on the monitor say, "Look someone's coming," and "Someone's coming into view."[4] The family later determined that the baby monitor had been remotely hacked by a stranger, which also allowed the individual to control the camera on the baby monitor, therefore allowing the hacker to spy on the

1. The title of this article is a reference to E.M. Forster's 1909 science fiction novella, THE MACHINE STOPS, which depicts a dystopian world where all the needs of individuals are provided by the omnipotent, global "Machine." E.M. FORSTER, THE MACHINE STOPS (1909), http://archive.ncsa.illinois.edu/prajlich/forster.html. Portions of this article include material adapted from "Global Privacy and Data Protection," a chapter published in the course handbook for the Practising Law Institute's (PLI) COMMUNICATIONS LAW IN THE DIGITAL AGE 2017 conference held November 9-10, 2017. The author of the chapter, Prof. Jane Kirtley, granted to PLI non-exclusive rights to publish the chapter in COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, retaining the right to republish the contents elsewhere. JEFFREY P. CUNARD ET AL., PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017 (2017).

2. Crimesider Staff, *Baby Monitor Hacker Delivers Creepy Message to Child*, CBS NEWS (April 23, 2015, 9:08 AM), https://www.cbsnews.com/news/baby-monitor-hacker-delivers-creepy-message-to-child/.

3. *Id.*

4. *Id.*

family.[5] Two years earlier, a family in Texas reported very similar events: a hacker had been spying on and speaking to their two-year-old daughter.[6] The hackers were able to do so because the baby monitors were connected to the internet and a smart phone app that allows parents to monitor their child.[7]

Baby monitors are one of numerous devices that are part of the Internet of Things (IoT), a network of "smart" devices that can connect to the internet. The Federal Trade Commission (FTC) defines the IoT as "devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet," creating a network.[8] These devices or sensors are increasingly sold commercially to consumers, but can also be "sold in a business-to-business context, such as sensors in hotel or airport networks."[9] The IoT can also encompass "broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency."[10] Examples of IoT devices include smart cars, home appliances, thermostats, wearable devices, medical devices, and more.[11]

---

5. *Id.*; *see also* Yael Grauer, *Security News This Week: Turns Out Baby Monitors Are Wildly Easy to Hack*, WIRED (Sept. 5, 2015, 7:00 AM), https://www.wired.com/2015/09/security-news-week-turns-baby-monitors-wildly-easy-hack/ ("When security firm Rapid 7 tested nine widely available internet-connected baby monitors for security vulnerabilities, the results weren't pretty. 'Eight of the nine cameras got an F and one got a D minus,' security researcher Mark Stanislav told Fusion's Kashmir Hill.").

6. Ryan Grenoble, *Hacked Baby Monitor Caught Spying On 2-Year-Old Girl in Texas (UPDATE)*, HUFFINGTON POST (Aug. 14, 2013), https://www.huffingtonpost.com/2013/08/13/hacked-baby-monitor-houston-texas-parents_n_3750675.html; *see also* Jessica Willey, *Hacker Targets Houston Family's Baby Monitor*, ABC 13 (Aug. 13, 2013, 12:03 PM), http://abc13.com/archive/9201651/.

7. *Seen at 11: Cyber Spies Could Target Your Child Through a Baby Monitor*, CBS N.Y. (April 21, 2015, 11:28 PM), http://newyork.cbslocal.com/2015/04/21/seen-at-11-cyber-spies-could-target-your-child-through-a-baby-monitor/.

8. Jane E. Kirtley, *Global Privacy and Data Protection–2015*, *in* 1 PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2015, at 655, 674 (2015); FED. TRADE COMM'N, STAFF REPORT ON THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

9. *Id.*

10. *Id.*

11. Andrew Meola, *Internet of Things: Devices, Applications & Examples*, BUS. INSIDER (Dec. 19, 2016, 1:44 PM), http://www.businessinsider.com/internet-of-things-devices-applications-examples-2016-8.

On January 29, 2017, *Forbes* reported that the IoT market was predicted to reach $276 billion by 2020, with "predictive maintenance, self-optimizing production, and automated inventory management" as the top three uses of IoT technology.[12] On February 7, 2017, Gartner predicted that 8.4 billion IoT devices would be in use globally in 2017, rising 31 percent from 2016.[13] On October 24, 2017, IHS Markit estimated that there were nearly 27 billion IoT devices worldwide in 2017, three times the estimate of Gartner.[14] IHS Markit predicted the number of devices would jump to over 30 billion by 2020.[15]

Despite the rapid growth of the devices, and the potential benefits they offer, the IoT raises significant security and privacy concerns. The most significant challenge is to determine whether a self-regulatory regime will be sufficient to address these concerns, or whether comprehensive or sectoral legislation or regulation will be necessary to ensure that the public interest in protecting personal privacy and data security will be addressed, and that adequate remedies will be available in the event of systemic failures.

This article first addresses the security issues and concerns arising from the IoT, drawing particular attention to recent cyberattacks targeting computer systems and the IoT. This article next turns to the privacy issues related to IoT devices, especially those containing health data and data collected from children, which led to actions by Mattel, the FTC, and the FBI to mitigate some of the privacy concerns.

Third, this article examines regulatory actions in the United States by the federal government, including the FTC, National Telecommunications & Information Administration (NTIA), four U.S. Senators, and four U.S. Representatives, as well as by private companies within the IoT industry practicing self-regulation. As a means of comparison, this article next discusses

---

12. Louis Columbus, *Internet of Things Market to Reach $267B by 2020*, FORBES (Jan. 29, 2017, 12:30 PM), https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#7d16f853609b.

13. Press Release, Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016 (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917.

14. Press Release, IHS Markit, Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says (October 24, 2017), http://news.ihsmarkit.com/press-release/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says.

15. *Id.*

actions taken by the European Union, the Article 29 Working Party,[16] and European organizations to address security and privacy concerns related to the IoT. Whereas the United States takes a sectoral approach to privacy, with laws and regulations designed to address specific industries, the EU prefers an omnibus approach to privacy through implementation of an overarching, blanket law regulating privacy consistently across industries, providing certain rights to EU citizens regardless of context.[17] More specifically, this article addresses how two major EU regulations—the General Data Protection Regulation (GDPR) and the ePrivacy Regulation—implicate the IoT, especially guidelines aiming to mitigate concerns regarding the collection of EU individuals' personal data and the vulnerability of such data.

Finally, this article discusses who may be liable in the event of an IoT device malfunction or a cyberattack during which personal data stored on the device or a larger network is stolen. Although this remains an unanswered question in the courts, this article points to three areas of law and enforcement that suggest how liability may be determined and handled, including (1) enforcement actions by the FTC related to IoT devices, (2) End User License Agreements (EULAs) and product liability law, and (3) additional avenues, beyond product liability, that consumers may claim compensation for damages related to IoT devices, including some state data breach statutes.

## II. SECURITY AND PRIVACY ISSUES AND CONCERNS RAISED BY THE INTERNET OF THINGS

In order to understand the reasons behind regulation of the IoT, as well as potential liability, it is necessary to consider both the security and the privacy concerns associated with the devices. Experts warn that IoT devices will continue to be subject to cyberattacks in 2018, similar to the May 2017 WannaCry

16. *See infra* note 247.

17. Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/; *see also* Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. TIMES (Feb. 2, 2013), https://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html.

attack[18] and the October 2016 Distributed Denial of Service (DDoS) attacks[19] that targeted computer systems and the IoT, worldwide. These same experts argue that what constitutes reasonable security has not been clearly defined,[20] potentially leading to the "security crisis of 2018."[21]

Similarly, experts maintain that privacy concerns associated with the IoT will continue throughout 2018 because the industry lacks proper oversight regarding personal data collected by IoT devices.[22] Of particular concern, many IoT devices collect "extremely sensitive data," including health data and data collected from children's toys, despite efforts by the FTC and FBI to alert consumers to these potential privacy issues.[23]

### A. SECURITY ISSUES AND CONCERNS

In April 2017, the National Telecommunications and Information Administration (NTIA), an independent agency within the U.S. Department of Commerce, noted that the "[s]ecurity of [IoT] devices is increasingly important to the security and safety of consumers, businesses, and others."[24] The Electronic Privacy Information Center (EPIC) warns that the security issues associated with IoT devices arise because they are connected to the internet, making them vulnerable to

---

18. Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017, 12:29 PM), https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

19. *What Is a DDoS Attack?*, DIGITAL ATTACK MAP, https://www.digitalattackmap.com/understanding-ddos/ (last visited Feb. 14, 2018); *see also* Margaret Rouse, *Definition: Disrupted Denial of Service (DDoS) Attack*, TECHTARGET, http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

20. Jimmy H. Koo, *Dumb Devices Smarten Up, Widening Data Security Enforcement Net*, PRIVACY & SECURITY L. REP. (Bloomberg Law, New York, N.Y.) Jan. 8, 2018, at 1.

21. Nick Ismail, *The Internet of Things: The Security Crisis of 2018?*, INFO. AGE (Jan. 22, 2018), http://www.information-age.com/internet-things-security-crisis-123470475/.

22. Bree Fowler, *Gifts That Snoop? The Internet of Things Is Wrapped in Privacy Concerns*, CONSUMER REPS. (Dec. 13, 2017), https://www.consumerreports.org/internet-of-things/gifts-that-snoop-internet-of-things-privacy-concerns/.

23. *Id.*

24. NAT'L TELECOMM. & INFO. ADMIN., COMMUNICATING IOT DEVICE SECURITY UPDATE CAPABILITY TO IMPROVE TRANSPARENCY FOR CONSUMERS (2017).

cyberattacks that can be used to gain access to an entire network.[25] Complicating matters, most computer systems prevent against, or mitigate, cyberattacks through patches via regular updates.[26] However, many IoT devices have not been designed to use such patches in their software, leaving security issues unresolved.[27]

Furthermore, some IoT devices utilize cloud storage services that use remote servers to store data. Such "splitting control" over the device and the data leaves both prone to cyberattacks that may compromise the security of the devices and the data.[28] However, most IoT devices do not send collected data through networks to a centralized cloud server because of limited power, as well as limited connectivity and bandwidth.[29] Instead, most IoT devices utilize "fog computing," meaning the device itself or a nearby router are used to analyze and process the sensor data.[30] This decentralized IoT architecture, with data being stored and secured locally, prevents some of the security concerns associated with cloud storage;[31] however, it does not completely alleviate security issues, which are discussed below.

In November 2013, the FTC held a workshop, titled "The Internet of Things: Privacy and Security in a Connected World," during which panelists from government, industry, and consumer groups discussed a variety of issues related to IoT.[32] In a January 2015 report stemming from the workshop, the FTC detailed both the benefits and the risks of the IoT, including security concerns.[33] In particular, the FTC highlighted three potential threats to consumers.[34] First, IoT devices "enabl[e] unauthorized access and misuse of personal information" by

---

25. *Internet of Things (IoT)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/internet/iot/ (last visited Mar. 4, 2018).

26. *Id.*

27. *Id.*

28. *Id.*

29. Rhys Dipshan, *The IoT Ambiguity: Secure Architecture, Vulnerable Data*, LEGALTECH NEWS (Feb. 2, 2018), https://www.law.com/legaltechnews/sites/legaltechnews/2018/02/02/the-iot-ambiguity-secure-architecture-vulnerable-data/.

30. *Id.*

31. *Id.*

32. FED. TRADE COMM'N, *supra* note 8.

33. *Id.* at iii.

34. *Id.* at ii.

intruders and hackers gaining access to the data.[35] Second, IoT devices "facilitat[e] attacks on other systems," such as the network to which the IoT device is connected.[36] Finally, IoT devices may "create risks to physical safety in some cases."[37] For example, one participant at the FTC workshop declared that he had hacked insulin pumps, allowing him to change the settings remotely to stop the machines.[38] A different participant claimed that he could gain remote access to a car's internal computer network, allowing him to control the engine and braking systems.[39]

In the years since the report was published, IoT devices have been subject to ransomware and Distributed Denial of Service (DDoS) attacks, which many experts expect to continue, and increase, throughout 2018.[40] A ransomware attack occurs when hackers use a virus to infect a computer and to encrypt all of its data, making the data inaccessible.[41] The hackers then demand a ransom from the affected computer user to decrypt the data.[42] If the computer user fails to pay the ransom within a certain amount of time, the virus destroys the files.[43] In 2017, security company Symantec reported that ransomware attacks jumped to 483,800 incidents in 2016, an increase of more than one-third compared to 2015.[44] By contrast, a DDoS attack "is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources."[45] The cybercriminal begins a DDoS attack by exploiting the vulnerability of just one device,

---

35. *Id.*

36. *Id.*

37. *Id.* at 12.

38. *Id.*

39. *Id.*; *see also* Ben Dickson, *Why IoT Security Is So Critical*, TECHCRUNCH (Oct. 24, 2015), https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/ ("In another development, it was proven that Internet-connected cars can be compromised, as well, and hackers can carry out any number of malicious activities, including taking control of the entertainment system, unlocking the doors or even shutting down the car in motion.").

40. Ismail, *supra* note 21; *see also* Chris Preimesberger, *Predictions 2018: Internet of Things Will Expand as Threat Vector*, EWEEK (Dec. 28, 2017), http://www.eweek.com/security/predictions-2018-internet-of-things-will-expand-as-threat-vector.

41. Sherr, *supra* note 18.

42. *Id.*

43. *Id.*

44. *Id.*

45. *What Is a DDoS Attack?*, *supra* note 19; *see also* Rouse, *supra* note 19.

making it the DDoS "master," which then identifies other vulnerable devices, networks, and systems.[46]

One example of a large ransomware attack targeting internet and computer systems is the virus named WannaCry.[47] In May 2017, hackers targeted computers running the Microsoft Windows operating system by encrypting data and subsequently demanding ransom payments.[48] The WannaCry attack affected thousands of computers in more than 150 countries.[49] One of the more serious effects of the attack was the targeting of sixteen hospitals across the United Kingdom, leading to the cancellation of appointments and non-urgent operations at some locations.[50] The UK National Health Service stated that although the attack severely affected operations at the hospitals, particularly freezing computer operations running on an outdated Windows operating system, there was no indication that any patient data had been compromised.[51] The global financial and economic damage caused by WannaCry approached billions of dollars, making it one of the most damaging ransomware incidents in history.[52]

An example of a large-scale DDoS attack took place in October 2016 and directly targeted IoT devices. On October 26, 2016, *The Guardian*, among other media outlets, reported that the DDoS attack affected a large portion of the U.S. internet by

---

46. Rouse, *supra* note 19.

47. Jane E. Kirtley, *Global Privacy and Data Protection—2017*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 365, 440 (2017).

48. Timothy B. Lee, *The WannaCry Ransomware Attack Was Temporarily Halted. But It's Not Over Yet*, VOX (May 15, 2017, 4:20 PM), https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp.

49. Bill Chappell, *WannaCry Ransomware: What We Know Monday*, NAT'L PUB. RADIO (May 15, 2017, 2:31 PM), https://www.npr.org/sections/the two-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

50. Russell Brandom, *UK Hospitals Hit with Massive Ransomware Attack*, VERGE (May 12, 2017, 11:36 AM), https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin; *see also* Denis Campbell & Haroon Siddique, *Operations Cancelled as Hunt Accused of Ignoring Cyber-Attack Warnings*, GUARDIAN (May 15, 2017, 8:58 AM), https://www.theguardian.com/technology/2017/may/15/warning-of-nhs-cyber-attack-was-not-acted-on-cybersecurity ("Operations and hospital clinic appointments due to take place on Tuesday have been cancelled . . . .").

51. Brandom, *supra* note 50.

52. Jonathan Berr, *"WannaCry" Ransomware Attack Losses Could Reach $4 Billion*, CBS NEWS (May 16, 2017, 5:00 AM), https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

infecting a network of computers with Mirai, malware meant to bombard a server with so much traffic that it eventually collapses.[53] The servers belonged to Dyn, "a company that is a major provider of DNS services to other companies."[54] *The Guardian* reported that the attack affected the function of several websites "including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US."[55]

According to *WeLiveSecurity*, a publication of IT security company ESET, the DDoS attacks were "made possible by the large number of unsecured internet-connected digital devices, such as home routers and surveillance cameras."[56] The attacks infected thousands of IoT devices with the Mirai malware in order to find additional unsecured devices.[57] The result was the formation of a botnet, a group of hijacked Internet-connected private devices controlled remotely without the device's owner's consent or knowledge.[58] Experts also pointed to default passwords of IoT devices as another reason for the DDoS attack. *WeLiveSecurity* explained that "anyone placing [a smart] device on the internet without first changing the default password is, in effect, enabling attacks of the type witnessed on October 21."[59]

A 2017 report by Corero Network Security, which provides DDoS protection and mitigation for its clients, found that in Q3 of 2017, organizations faced an average of 237 DDoS attack attempts per month, marking a 35% increase from Q2, and a 91% increase from Q1.[60] Researchers have argued that one

---

53. Stephen Cobb, *10 Things to Know About the October 21 IoT DDoS Attacks*, WELIVESECURITY (Oct. 24, 2016, 7:16 PM), https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/; *see also* Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet (discussing the Mirai botnet and its role in the attack).

54. Cobb, *supra* note 53.

55. Woolf, *supra* note 53.

56. Cobb, *supra* note 53.

57. *Id.*

58. *Id.*; *see also Botnet DDoS Attacks*, INCAPSULA, https://www.incapsula.com/ddos/botnet-ddos.html (last visited Feb. 14, 2018) (defining botnet).

59. Cobb, *supra* note 53.

60. Alison DeNisco Rayome, *DDoS Attacks Increased 91% in 2017 Thanks to IoT*, TECHREPUBLIC (Nov. 20, 2017, 5:45 AM), https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/; *see also* CORERO & GTT, CORERO & GTT DDOS TRENDS REPORT: Q2–Q3 2017, 3 (2017),

reason for the increase is the growing implementation of IoT devices, many of which remain unsecured.[61]

More generally, in a 2017 survey, strategic consulting firm Altman Vilandrie & Company found that nearly half of U.S. companies using an IoT network were hit by a security breach.[62] The survey polled 400 IT executives across nineteen industries, with 48% reporting that they had experienced a breach.[63] Furthermore, experts predict that small businesses may become a preferred target of hackers throughout 2018.[64] Jason J. Hogg, CEO of Aon Cyber Solutions, anticipates that one of the largest targets for IoT hacking in 2018 will be small businesses that use this technology because hackers "[target] IoT [devices] as a pivot point to enter systems and take control of physical operations."[65] Successful attacks on small businesses can create a domino effect: damaging larger corporations that receive their services.[66]

However, despite all these security concerns, Bloomberg Intelligence analyst Jawahar Hingorani observes that companies are "often playing catch-up" to keep up with old and new security problems.[67] Bloomberg BNA adds that what constitutes reasonable security, whether defined by the FTC or private companies, "remains undefined."[68] In its "Information Age" blog, digital media company Vitesse Media predicts that IoT may be the "security crisis of 2018," especially if companies

---

https://www.gtt.net/wp-content/uploads/2017/12/Corero-Q2-Q3-Trend-Reports.pdf (establishing quoted statistics).

61. Rayome, *supra* note 60.

62. Larry Karisny, *IoT Is Changing the Cybersecurity Industry*, GOV'T TECH. (Jan. 16, 2018), http://www.govtech.com/security/IoT-Is-Changing-the-Cybersecurity-Industry.html; *see also* Ken Briodagh, *New Survey Says Half of US Companies Using IoT Have Been Breached*, IOT EVOLUTION (June 1, 2017), http://www.iotevolutionworld.com/iot/articles/432498-new-survey-says-half-us-companies-using-iot.htm (discussing the 2017 survey).

63. Briodagh, *supra* note 62.

64. AON, 2018 CYBERSECURITY PREDICTIONS: A SHIFT TO MANAGING CYBER AS AN ENTERPRISE RISK 13 (2018), https://www.strozfriedberg.com/wp-content/uploads/2018/01/2018-Cybersecurity-Predictions-Report-Aon-Cyber-Solutions.pdf; *see also* Rob Starr, *Hackers Will Target Small Business Through the Internet of Things in 2018, New Report Says*, SMALL BUS. TRENDS (Jan. 16, 2018), https://smallbiztrends.com/2018/01/2018-cybersecurity-predictions.html (referencing the Aon report's finding that hackers will target small businesses that use IoT technology in 2018).

65. Starr, *supra* note 64.

66. *Id.*

67. Koo, *supra* note 20.

68. *Id.*

and organizations, as well as federal agencies, do not work to update security measures, policies, and potential solutions.[69]

### B. PRIVACY ISSUES AND CONCERNS

In its 2015 report, the FTC also addressed privacy concerns associated with IoT devices: that they directly collect sensitive information, including precise geolocation, financial account numbers, health information, and more.[70] Furthermore, the IoT involves large aggregations of data.[71] The FTC reported that approximately 10,000 households using a single company's IoT home automation product can collectively "generate 150 million discrete data points a day,"[72] or about "one data point every six seconds for each household."[73] The creation of "[s]uch a massive volume of granular data allows those with," or without, "access to the data to perform analyses . . . [impossible] with less rich data sets."[74] Another privacy concern raised by the FTC is that a manufacturer, cybercriminal, or even law enforcement, could remotely "eavesdrop" on an individual's home, a school, a hospital, or other private areas, leading to warrantless surveillance or illegal searches and recordings in violation of common law, privacy, and Fourth Amendment rights.[75]

Two types of "extremely sensitive" personal data have been highlighted as areas of particular concern moving forward: health data and data collected by children's toys. Regarding health data, Jimmy Koo in Bloomberg BNA observes that devices such as wearable fitness trackers that connect to the internet collect "extremely sensitive" health data about individuals' personal wellness.[76] The FTC contended in 2015 that such information could be used by insurance companies to decide whether to preemptively raise or lower individuals' insurance costs or deductible.[77]

*Med Device Online*, an online resource for manufacturers in medical device design, suggests that healthcare data, including

---

69. Ismail, *supra* note 21.
70. FED. TRADE COMM'N, *supra* note 8, at 14.
71. *Id.* at 14–15.
72. *Id.* at 14.
73. *Id.*
74. *Id.* at 15.
75. *Id.* at 17.
76. Koo, *supra* note 20.
77. FED. TRADE COMM'N, *supra* note 8, at 15–16.

medical records and results from hospital equipment such as MRI and X-ray machines, is also vulnerable as IoT medical devices become increasingly common in hospitals and the healthcare industry.[78] IBM's "2016 Cyber Security Intelligence Index" found that healthcare was the top industry cyberattacked in 2015,[79] including by the WannaCry attack. Studies from 2017 also suggest that the healthcare industry remains a major target, with organizations facing a new cyberattack every two weeks.[80]

The second area receiving particular attention is children's toys and personal data. CBS News contributor and *Wired* magazine editor-in-chief Nicholas Thompson asserts that there is "a real discrepancy between the privacy protections built into most internet-connected toys and the privacy protections that you want for your children" largely because it is hard to update children's toys.[81] Thompson drew particular attention to toys that have microphones and cameras, suggesting they can be used by hackers to eavesdrop, as has happened with baby monitors.[82] Children's toys that collect information such as names, email addresses, and home addresses are also vulnerable to hacking, especially if the information is stored in the cloud.[83]

---

78. Mildred Segura et al., *The Internet of Medical Things Raises Novel Compliance Challenges*, MED DEVICE ONLINE (Jan. 3, 2018), https://www.meddeviceonline.com/doc/the-internet-of-medical-things-raises-novel-compliance-challenges-0001.

79. Zlata Rodionova, *Healthcare Is Now Top Industry for Cyberattacks, Says IBM*, INDEPENDENT (Apr. 21, 2016), http://www.independent.co.uk/news/business/news/healthcare-is-now-top-industry-for-cyberattacks-says-ibm-a6994526.html.

80. Maia Hightower, *Industry Voices—Preserving Quality of Care in the Face of Cybersecurity Threats*, FIERCEHEALTHCARE (Dec. 6, 2017, 6:30 PM), https://www.fiercehealthcare.com/privacy-security/cybersecurity-medical-devices-internet-things-wannacry-patient-harm-quality.

81. *Why You Should Be "Wary" of Gifting an Internet-Connected Smart Toy*, CBS NEWS (Dec. 21, 2017), https://www.cbsnews.com/news/internet-connected-smart-toys-be-wary-of-gifting-privacy-security/.

82. *Id.*; *see also* Stuart Madnick, *Security Surprises Arising from the Internet of Things (IoT)*, FORBES TECH BLOG (May 8, 2017, 10:01 AM), https://www.forbes.com/sites/ciocentral/2017/05/08/security-surprises-arising-from-the-internet-of-things-iot/#7ef3a7fd2495 ("Baby monitors have been turned into eavesdropping devices . . . .").

83. *See Why You Should Be "Wary" of Gifting an Internet-Connected Smart Toy*, *supra* note 81 ("'We've had internet-connected toys that store information on the cloud like your child's voice that can then be hacked.' There have also been hacks that exposed personal data like names, email and home addresses.").

He added that children "don't have defenses against privacy invasions because they haven't learned these things."[84]

These privacy concerns prompted toy company Mattel, the FTC, and the FBI in 2017 to take precautionary actions related to children's IoT toys. First, on October 4, 2017, Mattel announced that it had canceled plans to sell "Aristotle," a smart device aimed at young children, amidst growing security and privacy concerns related to the device.[85] Mattel had introduced the device in January 2017, which combined a smart speaker with a digital assistant functionality and connected camera.[86] A May 2017 Campaign for a Commercial-Free Childhood (CCFC) petition pointed out that although the device was intended to soothe a crying baby with "nightlights, lullabies, and sleep sounds," it would also collect and store data about a child's activity.[87] Further, according to the petition, it would "connect[] to other apps and online retailers, which means that data may be shared with those partner corporations, which may use it to target the marketing of other products to young children and their parents."[88] In a statement, a spokeswoman for Mattel said that the decision not to sell Aristotle was prompted by Sven Gerjets, the company's new chief technology officer, who conducted a review of the Aristotle product and decided that it did not "fully align with Mattel's new technology strategy . . . ."[89]

---

84. *Id.*

85. James Vincent, *Mattel Cancels AI Babysitter After Privacy Complaints*, VERGE (Oct. 4, 2017), https://www.theverge.com/2017/10/5/16430822/mattel-aristotle-ai-child-monitor-canceled.

86. *Id.*

87. *Stop Mattel's Aristotle from Trading Children's Privacy for Profit*, CCFC https://org.salsalabs.com/o/621/p/dia/action4/common/public/?action_KEY=21718; *see also* Letter from Josh Golin & Michael O'Heaney, Executive Directors, Campaign for a Commercial-Free Childhood, to Margaret Georgiadis, CEO, Mattel, Inc. (Oct. 2, 2017), http://www.commercialfreechildhood.org/sites/default/files/Letter%20to%20Mattel.pdf.

88. *Stop Mattel's Aristotle from Trading Children's Privacy for Profit*, *supra* note 87.

89. Hayley Tsukayama, *Mattel Has Canceled Plans for a Kid-Focused AI Device that Drew Privacy Concerns*, WASH. POST (Oct. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/?utm_term=.75fb93da0d12.

Second, on June 21, 2017, the FTC published a press release, "FTC Updates COPPA Compliance Plan for Business,"[90] which described how the FTC updated its Six Step Compliance Plan for businesses regarding the Children's Online Privacy Protection Act of 1998 (COPPA).[91] Section 6502(a) of COPPA, titled "Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet," makes it "unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations" of the statute.[92]

The main revision of the FTC's compliance plan directed vendors to initially "Determine if Your Company is a Website or Online Service that Collects Personal Information from Kids Under 13," and the revision now included "connected toys or other Internet of Things devices" under the definition of "Website or online service."[93] Additionally, the FTC added two ways that companies could obtain parents' permission before collecting children's personal information: "asking knowledge-based authentication questions and using facial recognition to get a match with a verified photo ID."[94]

On July 17, 2017, the FBI published a public service announcement, which also addressed "privacy and contact concerns for children" in relation to IoT toys.[95] The FBI alert

---

90. Kristin Cohen & Peder Magee, *FTC Updates COPPA Compliance Plan for Business*, FED. TRADE COMM'N BUSINESS BLOG (June 21, 2017, 10:26 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business; *see also* 15 U.S.C. § 6502(a); Jane E. Kirtley, *FTC Takes Multiple Steps Towards Privacy and Security for IoT Consumers*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 393, 393–400 (2017) [hereinafter *FTC Takes Multiple Steps*].

91. *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2012).

92. 15 U.S.C. § 6502(a) (2012).

93. *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

94. Cohen & Magee, *supra* note 90.

95. FED. BUREAU OF INVESTIGATION, ALERT NO. I-071717 (REVISED)-PSA, CONSUMER NOTICE: INTERNET-CONNECTED TOYS COULD PRESENT PRIVACY

encouraged consumers to "consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes or trusted environments," citing the FTC's updated compliance plan.[96] According to the FBI, the toys "typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities—including speech recognition and GPS options" and can connect to the Internet, which means the toys "could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed."[97] The alert also provided recommendations for families regarding IoT toys, including "[c]arefully read disclosures and privacy policies" and "[c]losely monitor children's activity with the toys (such as conversations and voice recordings) through the toy's partner parent application," among other recommendations.[98]

Despite these actions by Mattel, the FTC, and the FBI, privacy concerns remain for children's toys as well as other IoT devices. Security and privacy experts warn that there is still "little oversight" of the data collected by the devices and how they are protected from hackers and cyberattacks.[99] Additionally, even if personal information is kept secure and private by IoT companies, former Assistant U.S. Attorney for the Northern District of California Hanley Chew notes that a law enforcement or government official needs only to obtain a subpoena to access IoT data because it can be interpreted as falling under "non-content" information as defined in the Electronic Communications Privacy Act of 1986.[100] Subpoenas do not require judicial approval, unlike search warrants, making it easier for the police or federal agencies to obtain information from IoT devices.[101] Thus, questions remain about what data law

---

AND CONTACT CONCERNS FOR CHILDREN (2017), https://www.ic3.gov/media/2017/170717.aspx; *see also FTC Takes Multiple Steps*, *supra* note 90, at 393.

96. FED. BUREAU OF INVESTIGATION, *supra* note 95.

97. *Id.*

98. *Id.*

99. Fowler, *supra* note 22; *see also* Kathy Kristof, *How to Tame Household Privacy Threats from Toys, TVs and More*, CBS MONEYWATCH (Jan. 10, 2018), https://www.cbsnews.com/news/how-to-tame-household-privacy-threats-internet-connected-toys/.

100. Dipshan, *supra* note 29.

101. *Id.*

enforcement or government agencies will be able to access, whether through a subpoena or a search warrant.[102]

## III. REGULATION OF THE INTERNET OF THINGS IN THE UNITED STATES

On January 4, 2018, Bloomberg Law contended that despite significant security and privacy concerns, IoT devices and data remain largely unregulated, with "no specific law or regulation governing how this data is used or collected."[103] However, the federal government, as well as private companies, have recently undertaken stronger measures to address the security and privacy issues related to IoT devices. Paul Rosenzweig, the founder of Red Branch Consulting PLLC, suggests that the "most significant regulatory push in the United States" will involve the IoT, with regulatory agencies imposing security and privacy requirements.[104]

### A. FEDERAL GOVERNMENT

In light of the security and privacy concerns associated with IoT devices, experts have called on the federal government, including federal agencies and Congress, to take a more active role in coordinating security standards.[105] Frost and Sullivan IoT research director Dilip Sarangan contends that because the responsibility of IoT privacy and security falls upon several actors in the IoT industry, including manufacturers, network providers, software developers, and others, it is difficult for the industry to develop industry-wide standards.[106] He further

---

102. *See id.*; Bruce Schneier, *Law Enforcement Access to IoT Data*, SCHNEIER ON SECURITY (Jan. 11, 2017, 6:22 AM), https://www.schneier.com/blog/archives/2017/01/law_enforcement_1.html; Jonathon Hauenschild, *Lawmakers Must Clarify Privacy Protections for the Internet of Things*, HILL (Jan. 6, 2017, 7:00 AM), http://thehill.com/blogs/pundits-blog/technology/312968-lawmakers-must-clarify-privacy-protections-for-the-internet-of.

103. Kirk Nahra, *The Top Ten Privacy and Data Security Developments to Watch in 2018*, BLOOMBERG L.: BIG L. BUS. (Jan. 5, 2018), https://biglawbusiness.com/the-top-ten-privacy-and-data-security-developments-to-watch-in-2018/.

104. Paul Rosenzweig, *Cybersecurity Predictions for 2018*, LAWFARE (Jan. 2, 2018, 8:00 AM), https://www.lawfareblog.com/cybersecurity-predictions-2018.

105. Jon Gold, *IoT Security Needs a White Knight*, NETWORKWORLD (Jan. 15, 2018, 4:30 AM), https://www.networkworld.com/article/3247774/internet-of-things/iot-security-needs-a-white-knight.html.

106. *Id.*

explains that IoT implementation has several moving parts that may be administered by multiple different organizations and third parties.[107]

From 2016 through January 2018, the FTC, National Telecommunications & Information Administration (NTIA), four U.S. Senators, and four U.S. Representatives, in association with the Food and Drug Administration (FDA) and the National Institute of Standards and Technology (NIST), took steps to address IoT privacy and security concerns. First, the FTC was involved in several legal disputes connected to the IoT and security.[108] As discussed in Section II.B, the FTC also updated its compliance plan regarding COPPA to include IoT devices, with the FBI sending an alert related to similar concerns.[109]

Second, in a July 18, 2017 meeting, a public-private sector working group ("Working Group") convened by the NTIA, finalized a guidance document drafted in April 2017 addressing how manufacturers should communicate information to consumers about security updates for IoT devices.[110]

Third, on August 1, 2017, four U.S. Senators introduced a bipartisan bill aiming to improve the cybersecurity of IoT devices supplied by vendors to the U.S. government.[111] The legislation contained several provisions, including requirements that vendors "ensure [the] devices are patchable, rely on industry standard protocols, do not use hard-coded passwords, and do not contain any known security vulnerabilities."[112]

Finally, on October 5, 2017, Rep. David Trott (R-Mich.) introduced the "Internet of Medical Things Resilience Partnership Act of 2017."[113] The legislation aimed to "establish a working group of public and private entities led by the Food

---

107. *Id.*

108. *See FTC Takes Multiple Steps*, *supra* note 90, at 394–95.

109. *Id.* at 393; *see also* Cohen & Magee, *supra* note 90.

110. NAT'L TELECOMM. & INFO. ADMIN., *supra* note 24, at 1.

111. Press Release, U.S. Senator for Virginia Mark R. Warner, Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices (Aug. 1, 2017), https://www.warner.senate.gov/public/index.cfm/pressreleases?id=06A5E941-FBC3-4A63-B9B4-523E18DADB36; *see also* Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (2017).

112. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111.

113. Internet of Medical Things Resilience Partnership Act of 2017, H.R. 3985, 115th Cong. (2017); *see also* Segura et al., *supra* note 78.

and Drug Administration to recommend voluntary frameworks and guidelines to increase the security and resilience of Internet of Medical Things devices, and for other purposes."[114]

1. Federal Trade Commission Enforcement Actions

Since convening the Working Group in 2013, the FTC has viewed IoT security as a priority.[115] In addition to explaining the benefits and risks of the IoT in its 2015 report, the FTC provided several recommendations for best practices businesses can implement in order to protect consumers' privacy and security, including that manufacturers adopt a "security by design approach" by building security into an IoT device.[116] The FTC supported not only providing notice to consumers about what data is being collected, but also giving them a choice of how their data is collected and shared.[117] The FTC also explained how it aimed to ensure that IoT manufacturers considered security and privacy.[118] Finally, the report emphasized the need to develop self-regulatory programs to encourage the adoption of privacy- and security-sensitive practices.[119]

Another action by the FTC regarding IoT privacy and security was a contest launched in January 2017 "seeking tools to help consumers protect the security of their [IoT] devices."[120] On July 26, 2017, the agency announced that a mobile app developed by Steve Castle, a New Hampshire software

---

114. H.R. 3985.

115. *Id.*; *see also* Francoise Gilbert, *Securing the Internet of Things Is an FTC Priority*, LAW360 (Feb. 3, 2017), https://www.law360.com/articles/886166/securing-the-internet-of-things-is-an-ftc-priority.

116. Press Release, Fed. Trade Comm'n, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices; *see also FTC Takes Multiple Steps*, *supra* note 90, 393–400 (2017).

117. FED. TRADE COMM'N, *supra* note 8; *see also* Jane E. Kirtley, *FTC Releases Report on the Internet of Things; Global Privacy and Data Protection*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2015, at 655, 674 (2015).

118. FED. TRADE COMM'N, *supra* note 8.

119. *Id.*

120. Press Release, Fed. Trade Comm'n, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security; *see also FTC Takes Multiple Steps*, *supra* note 90, 393–400 (2017).

developer, had won the $25,000 top prize.[121] According to a press release by the FTC, the app is intended to

> help users manage the IoT devices in their home. It would enable users with limited technical expertise to scan their home Wi-Fi and Bluetooth networks to identify and inventory connected devices. It would flag devices with out-of-date software and other common vulnerabilities and provide instructions on how to update each device's software and fix other vulnerabilities.[122]

Apart from the report and contest, the FTC has also reached settlements with several companies in IoT related cases, including ASUSTeK Computer Inc. (ASUS), D-Link Systems, Inc. (D-Link), Lenovo Group Ltd. (Lenovo), Vizio Inc. (Vizio), and VTech.[123]

a. ASUSTeK Computer Inc.

On February 23, 2016, the FTC announced that it had reached a settlement with Taiwan-based computer hardware maker ASUS after the agency contended that security flaws in its routers put the home networks of hundreds of thousands of consumers at risk.[124] According to the FTC's complaint, ASUS introduced a feature known as AiCloud on its routers in August 2012, labeling it as a "private personal cloud for selective file sharing" allowing "indefinite storage and increased privacy."[125] The FTC alleged that AiCloud had "multiple vulnerabilities that would allow attackers to gain unauthorized access to consumers' files and router login credentials."[126] The FTC further alleged that ASUS failed to provide notice to consumers that the

---

121. Press Release, Fed. Trade Comm'n, FTC Announces Winner of its Internet of Things Home Device Security Contest (July 26, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

122. *Id.*

123. Press Release, Fed. Trade Comm'n, ASUS Settles FTC Charges that Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Risk (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put; *see* Jimmy Koo, *FTC Reports on 2017 Privacy, Data Security Enforcement*, BLOOMBERG BNA PRIVACY & DATA SEC. BLOG (Jan. 24, 2018), https://www.bna.com/ftc-reports-2017-b73014474565/; *see also* Daniel R. Stoller, *Lenovo Settles FTC, State Ad Software Security, Privacy Claims*, BLOOMBERG BNA: NEWS (Sept. 5, 2017), https://www.bna.com/lenovo-settles-ftc-n73014464166/.

124. Press Release, Fed. Trade Comm'n, *supra* note 123.

125. Complaint, ASUSTeK Comput., Inc., No. C-4587, File No. 142–3156, at *2 (F.T.C. July 8, 2016).

126. *Id.*

vulnerabilities existed, nor had it advised consumers how to disable AiCloud features that would mitigate the vulnerabilities.[127]

ASUS also introduced another cloud storage feature called AiDisk, which enabled individuals to remotely access files on a USB storage device attached to the router.[128] Regarding this feature, the FTC alleged that it had an "insecure design" because default settings provided "anyone on the internet with unauthenticated access to all of the files saved on the consumer's USB storage device."[129] ASUS again failed to notify consumers about the security concerns for nearly a year.[130] The complaint added several additional vulnerabilities of ASUS products.[131]

In July 2016, the FTC finalized the settlement, which required ASUS to establish and maintain a comprehensive security program subject to independent audits for the next 20 years, as well as to notify consumers about software updates or other steps to protect themselves from security flaws.[132] The agency called the settlement part of an "ongoing effort to ensure that companies secure the software and devices that they provide to consumers."[133]

b. D-Link Systems, Inc.

On January 5, 2017, the FTC filed a complaint seeking a permanent injunction and other equitable relief against D-Link Corporation and D-Link Systems, Inc. (collectively "D-Link") in the U.S. District Court for the Northern District of California, San Francisco Division, alleging that D-Link's internet cameras and routers contained inadequate security measures.[134]

---

127. *Id.* at *3.
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.* at *5.
132. Press Release, Fed. Trade Comm'n, FTC Approves Final Order in ASUS Privacy Case (July 28, 2016), https://www.ftc.gov/news-events/press-releases/2016/07/ftc-approves-final-order-asus-privacy-case.
133. Press Release, Fed. Trade Comm'n., *supra* note 123.
134. Melissa Daniels, *D-Link Sued by FTC Over Security Flaws in Routers, Cameras*, LAW360 (Jan. 5, 2017), https://www.law360.com/articles/877899; *see also* Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. D-Link Corp., No. 17-CV-00039 (N.D. Cal. filed Jan. 5, 2017), https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf; *FTC Takes Multiple Steps*, *supra* note 90, 393–400 (2017).

According to the FTC's complaint, Taiwan-based D-Link Corporation "directed its activities to the United States by designing, developing, marketing, and manufacturing routers, Internet-protocol ('IP') cameras, and related software and services, intended for use by consumers throughout the United States."[135] D-Link Systems, Inc., the corporation's U.S. subsidiary, "advertised, marketed, distributed, or sold routers, IP cameras, and related software and services, intended for use by consumers throughout the United States." [136]

The FTC alleged that D-Link engaged "in unfair or deceptive acts or practices"[137] because the company "[failed] to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers."[138] Furthermore, the FTC argued that D-Link "failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access[.]"[139] Consequently, the FTC contended that these failures led to "thousands" of routers and cameras being vulnerable to cyberattacks, putting consumers' personal information and local networks at risk,[140] and requested injunctive relief, though the agency did not allege that any personal data had been exposed.[141]

However, on September 25, 2017, Bloomberg BNA reported that the FTC would have to refile some of its claims related to security vulnerabilities and misleading advertising after a federal judge dismissed three of the six unfairness claims

---

135. Complaint, *supra* note 134, at 2; *see also* Allison Grande, *Taiwan Co. Escapes US Court in FTC Data Security Case*, LAW360 (May 11, 2017, 10:09 PM), https://www.law360.com/articles/922914; Joint Stipulation and Order Dismissing D-Link Corporation Without Prejudice, Fed. Trade Comm'n v. D-Link Corp., No. 17-CV-00039 (N.D. Cal. filed May 15, 2017), https://www.ftc.gov/system/files/documents/cases/2017.05.15_d.e._75_order_dismissing_dlc_wo_prej._and_req_disc.pdf (stating that on May 11, 2017, the FTC agreed to drop D-Link Corporation from the lawsuit).

136. Complaint, *supra* note 134, at 3.

137. 15 U.S.C. § 45(a).

138. Complaint, *supra* note 134, at 2.

139. *Id.* at 5.

140. *Id.* at 5–7.

141. *Id.* at 13; *see also* Nicole Ewart & Reed Freeman, *Federal Trade Commission Issues Privacy and Data Security Report for 2017*, WILMERHALE: PRIVACY AND CYBERSECURITY L. BLOG (Jan. 22, 2018), https://www.wilmerhale.com/blog/privacy-and-cybersecurity/post/?id=17179886720.

stemming from the company's alleged lax router security. [142] On September 20, 2017, *Consumerist* reported that the dismissal stemmed from the FTC's lack of proof to substantiate half of its claims.[143] U.S. District Court for the Northern District of California Judge James Donato wrote:

> The FTC does not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Instead, the FTC relies solely on the likelihood that DLS put consumers at "risk" . . . .[144] That is effectively the sum total of the harm allegations, and they make out a mere possibility of injury at best. The FTC does not identify a single incident where a consumer's financial, medical or other sensitive personal information has been accessed, exposed or misused in any way . . . . The absence of any concrete facts makes it just as possible that [the] devices are not likely to substantially harm consumers, and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor.[145]

Bloomberg BNA reported on January 24, 2018 that the FTC had not refiled the dismissed claims, but the litigation over the remaining charges remained ongoing.[146]

c. Lenovo Group Ltd.

On September 5, 2017, Lenovo agreed to no-fault settlements with the FTC and 32 states amidst allegations by the FTC that the ad software it installed had compromised users' web security and invaded their privacy.[147] The case arose in 2014 when Lenovo began selling laptops to U.S. consumers that came with a preinstalled software program called VisualDiscovery.[148]

---

142. Daniel R. Stoller, *D-Link Ducks Some FTC Internet of Things Data Security Claims*, BLOOMBERG LAW: PRIVACY AND DATA SECURITY (Sept. 25, 2017), https://www.bna.com/dlink-ducks-ftc-n57982088313/.

143. Laura Northrup, *Judge Gives D-Link Partial Win in FTC Case over Vulnerable Devices*, CONSUMERIST (Sept. 20, 2017, 4:28 PM), https://consumerist.com/2017/09/20/judge-dismisses-ftc-case-accusing-d-link-of-selling-vulnerable-devices/.

144. Fed. Trade Comm'n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, 2017 WL 4150873 at *5 (N.D. Cal. Sept. 19, 2017); *see also* Paul Roberts, *Court Balks at FTC's D-Link Complaint, Wants Proof of Harm*, SECURITY LEDGER (Sept. 21, 2017, 6:21 PM), https://securityledger.com/2017/09/court-balks-ftcs-d-link-complaint-wants-proof-harm/.

145. Fed. Trade Comm'n v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, slip op. at *5 (N.D. Cal. Sept. 19, 2017).

146. Koo, *supra* note 123.

147. Stoller, *supra* note 123.

148. Press Release, Fed. Trade Comm'n, Lenovo Settles FTC Charges It Harmed Consumers with Preinstalled Software on Its Laptops that

The FTC alleged that the software "interfered with how a user's browser interacted with websites and created serious security vulnerabilities" because it had access to "all of a consumer's sensitive personal information transmitted over the Internet, including login credentials, Social Security numbers, medical information, and financial and payment information."[149] Furthermore, problems with the software meant consumers' browsers could not warn users when they visited malicious websites with invalid digital certificates, according to the FTC complaint.[150]

As part of the FTC settlement, Lenovo agreed not to misrepresent any feature of installed software and to get affirmative user consent before installing such software, as well as provide an opt-out mechanism before loading similar software. The company was also required to implement and maintain a comprehensive data security software program for any software it installs.[151] Under the separate state agreement, Lenovo agreed to pay 32 State Attorney Generals $3.5 million.[152]

d. Vizio Inc.

On February 6, 2017, Vizio agreed to pay $2.2 million to settle a case with the FTC and the New Jersey attorney general's office.[153] According to the FTC's February 2014 complaint, Vizio manufactured smart TVs that had a "Smart Interactivity"

---

Compromised Online Security (Sept. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled; *see also* Complaint, In the Matter of Lenovo Inc., Docket No. C-4636 (Filed Dec. 20, 2017), https://www.ftc.gov/system/files/documents/cases/152_3134_c4636_lenovo_united_states_decision_and_order.pdf.

149. Press Release, Fed. Trade Comm'n, Lenovo Settles FTC Charges It Harmed Consumers with Preinstalled Software on Its Laptops that Compromised Online Security (Sept. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

150. *Id.*

151. *Id.*

152. *Id.*

153. Hayley Tsukayama, *Vizio Agrees to Pay $2.2 Million to Settle FTC's Television-Spying Case*, WASH. POST (Feb. 6, 2017), https://www.washingtonpost.com/business/economy/vizio-agrees-to-pay-22-million-to-settles-ftcs-television-spying-case/2017/02/06/3d4d4b16-ec8f-11e6-9662-6eedf1627882_story.html.

feature, which "enables program offers and suggestions."[154] However, the FTC alleged that Vizio failed to inform consumers that the feature also enabled the collection of their viewing data.[155] The complaint further alleged that Vizio had appended specific demographic information to the viewing data, such as sex, age, income, marital status, household size, education level, home ownership, and household value, before selling the data to third parties.[156] The FTC called Vizio's data tracking unfair and deceptive, because it was done without users' consent.[157]

Following the settlement, an order by U.S. District Court for the Central District of California Judge Josephine Staton required Vizio to "prominently disclose and obtain affirmative express consent for its data collection and sharing practices."[158] The order also required Vizio to delete data collected before March 1, 2016, and to implement a comprehensive data privacy program and biennial assessments of that program.[159]

e. VTech

On January 8, 2018, the FTC also reached a settlement in a case regarding children's toys and COPPA.[160] The agency

---

154. Complaint ¶ 22, FTC v. Vizio Inc., NO. 17-CV-00758 (D.N.J. filed Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf; *see also FTC Takes Multiple Steps*, *supra* note 90, 393–400 (2017).

155. Complaint, *supra* note 154, ¶ 38.

156. *Id.* ¶ 17; *see also* Press Release, Fed. Trade Comm'n, Vizio to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without User's Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

157. Press Release, Fed. Trade Comm'n, *supra* note 156.

158. Stipulated Order for Permanent Injunction and Monetary Judgment at § II.A., Fed. Trade Comm'n v. Vizio Inc. NO. 17-CV-00758 (D.N.J. filed Feb. 6, 2017).

159. *Id.* §§ III, IV.

160. Press Release, Fed. Trade Comm'n, Electronic Toy Maker VTech Settles FTC Allegations that It Violated Children's Privacy Law and the FTC Act (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated; *see also* Alan Friel and Carolina Alonso, *Toying with Children's Data: Lessons from the FTC's First Connected Toys Settlement Action*, DATA PRIV. MONITOR (Jan. 17, 2017), https://www.dataprivacymonitor.com/coppa/toying-with-childrens-data-lessons-from-the-ftcs-first-connected-toys-settlement-action/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

reached a $650,000 settlement with VTech, which "develop[s] a number of products and services for children," including portable devices known as "electronic learning products" or "ELPs."[161] The FTC contended in its complaint that VTech is therefore subject to COPPA, which applies to any operator of a commercial website or online service directed to children that collects, uses, and/or discloses their personal information.[162] COPPA requires that such companies follow steps to ensure children's information is protected, which includes disclosing to parents how the data is used.[163]

The main action of the litigation concerned Kid Connect, a mobile application that allows children to communicate with other children after parents or other adults download and register the app.[164] The FTC alleged that VTech failed to take several steps required by COPPA, including failing to provide a link to their privacy policy in each area where the app collected personal information.[165] VTech also failed to "develop, implement, or maintain a comprehensive information security program" and "implement adequate safeguards and security measures," among several other allegations.[166]

The complaint also claimed that VTech learned in November 2015 that a hacker had gained remote access to the company's computer network through "commonly known and reasonably foreseeable vulnerabilities," and withdrew personal information from several IoT devices and apps, including Kid Connect.[167] Although VTech stored passwords and children's photos and audio files in an encrypted format, the hacker gained access to a database that contained the decryption keys, which would have allowed the cybercriminal to access the information. It was not until a journalist approached the company that it learned about the hack.[168] Furthermore, the FTC alleged that although VTech continued to assert in its privacy policy that

---

161. Complaint ¶ 10, U.S. v. Vtech, No. 1:18-cv-114 (N.D. Ill. filed Jan. 8, 2018) (hereinafter VTech Complaint).
162. *Id.* ¶¶ 17–21.
163. *Id.*
164. *Id.* ¶¶ 22–38.
165. *Id.*
166. *Id.* ¶ 25.
167. *Id.* ¶ 27.
168. *Id.* ¶ 28.

most personal information was encrypted, in fact, none of it was actually encrypted.[169]

As part of its settlement with the FTC, VTech was "permanently prohibited from violating COPPA in the future and from misrepresenting its security and privacy practices."[170] The company was also required to implement a comprehensive data security program subject to independent audits for 20 years.[171] The litigation against VTech was one of over 20 COPPA cases brought by the FTC since 2000 and provided an additional example of how federal agencies, including the FTC and FBI, have addressed security and privacy of children's IoT devices under COPPA.[172]

### 2. National Telecommunications and Information Administration

On April 25, 2017, the National Telecommunications and Information Administration (NTIA), an independent agency within the U.S. Department of Commerce, released a report titled "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers."[173] Drafted by a public-private sector working group ("Working Group") convened by the NTIA, the document addressed how IoT companies, particularly manufacturers, should communicate security updates for IoT devices. In a July 18 meeting, the NTIA Working Group

---

169. *Id.* ¶ 12.

170. Press Release, Fed. Trade Comm'n, *supra* note 160.

171. *Id.*

172. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017, at 7 (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

173. Brian Kennedy, *The FTC and Industry Propose Best Practices for IoT Security Updates*, HOGAN LOVELLS (July 28, 2017), http://www.hldataprotection.com/2017/07/articles/cybersecurity-data-breaches/the-ftc-and-industry-propose-best-practices-for-iot-security-updates/#page=1; *see also* Jane E. Kirtley, *NTIA Finalizes Document Regarding Communication of IoT Security Update Information Following Comments from the FTC and Others*, in PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 400 (2017); NAT'L TELECOMM. & INFO. ADMIN., *supra* note 24; Evan Wolff et al., *Regulatory Rules Of The Road For IoT Manufacturers*, LAW360 (July 28, 2017), https://www.law360.com/articles/946940/regulatory-rules-of-the-road-for-iot-manufacturers (noting that the document synthesized guidance materials from various IoT stakeholders and regulators who had responded to a January 2017 NTIA green paper titled "Fostering the Advancement of the Internet of Things.").

published the final version of its guidance document after reaching a consensus.[174]

The first version of the document stated that security updates to IoT devices "are a key way to protect IoT devices when vulnerabilities are discovered and attacks evolve, though the method and capability of IoT devices to receive security updates varies across devices, services, and deployments."[175] Additionally, the document explained that IoT consumers "may desire basic information about their devices' security capabilities, particularly with regard to whether and how devices receive security updates."[176] The report added, "[t]here is also interest on the part of many policymakers and technologists for promoting transparency for consumers about the security needs and capabilities of internet-enabled devices."[177]

Next, the NTIA document outlined information "that manufacturers can communicate to better inform consumers and the marketplace about IoT devices' capability to receive security updates . . . ."[178] The information was divided into two categories: "key elements" and "additional considerations."[179] The first key element recommended that businesses describe "whether the [IoT] device is capable of receiving security updates."[180] Second, the report recommended that IoT companies provide a "[s]ummary of how the device receives security updates," including whether the device can receive automatic updates and, if not, "[w]hat user action is required to ensure the device is updated correctly and in a timely fashion?"[181] The final key element urged manufacturers to "[d]escribe the anticipated timeline for the end of security update support" because "routine security updates typically [end] as a device or software reaches the end of its lifecycle."[182] Thus, it "may be helpful to describe how long . . . consumers

174. NAT'L TELECOMM. & INFO. ADMIN, *supra* note 24.
175. *Id*. at 1.
176. *Id*.
177. *Id*.
178. NAT'L TELECOMM. & INFO. ADMIN, *supra* note 24.
179. *Id*. at 2.
180. *Id*.
181. *Id*. at 3.
182. *Id*.

[can] expect, at a minimum, the device to receive security updates."[183]

Turning to "additional considerations," the NTIA first recommended that IoT companies "[d]escribe how the user is notified about security updates," through a notification appearing on the IoT device or through an email.[184] Second, the document suggested that companies make clear "what happens when the device no longer receives security update support."[185] Finally, the Working Group suggested that IoT manufacturers describe how they ensure that security updates themselves are secure.[186]

On June 19, 2017, the FTC provided public comments for the NTIA recommendations.[187] The FTC emphasized the importance of consumers being provided "clear information about whether, how, for how long, and at what cost their IoT devices will receive security support," in light of the growing importance of "[ensuring IoT] devices are reasonably secure."[188] In so doing, the FTC argued, IoT companies "can benefit consumers, foster competition, and promote innovation in security."[189] The FTC also provided a series of recommendations regarding the "key elements" and the "additional elements" discussed by the Working Group.[190]

In a virtual meeting held on July 18, 2017, the NTIA Working Group finalized its IoT document.[191] The completed

---

183. *Id.*

184. NAT'L TELECOMM. & INFO. ADMIN, *supra* note 24.

185. *Id.*

186. *Id.* at 4.

187. FED. TRADE COMM'N, FEDERAL TRADE COMMISSION PUBLIC COMMENT ON "COMMUNICATION IOT DEVICE SECURITY UPDATE CAPABILITY TO IMPROVE TRANSPARENCY FOR CONSUMERS" (June 19, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf; *see also* Kirtley, *supra* note 173; Wolff et al., *supra* note 173 (noting that the NTIA also received over 130 responses from IoT manufacturers, solution providers, security experts, and consumer advocates, among other stakeholders).

188. FED. TRADE COMM'N, *supra* note 187, at 2.

189. *Id.*

190. *Id.* at 6.

191. Joshua Higgins, *NTIA Approves Finalized Guide on Communicating IoT Security to Consumers*, INSIDE CYBERSECURITY (July 21, 2017), https://insidecybersecurity.com/daily-news/ntia-approves-finalized-guide-communicating-iot-security-consumers; *see* John J. Heitmann & Jameson

document noted that it "reflects input and comments on earlier draft versions that were received from various stakeholders participating in the NTIA's multistakeholder process, including comments provided by the Federal Trade Commission."[192] One particular change was the addition of the phrase "for when support begins or ends (e.g. Jan. 1, 2025, or one year after date of registration)" regarding the "anticipated timeline" provided by IoT manufacturers.[193] Second, the final document updated the recommendation that manufacturers describe "how the user is notified about security updates" to include an "optional subscription service offering affirmative notifications" and "the timing of updates, such as if updates are available on a regular schedule."[194] The Working Group emphasized that the guidelines "[were] not meant to supersede regulation or serve as a legal standard" but instead "to identify and consolidate critical points it recommends manufacturers weigh as they develop IoT devices."[195]

3. U.S. Senate Bill

On August 1, 2017, four U.S. Senators introduced a bipartisan bill, which aimed to improve the security of IoT devices by "establishing minimum security requirements for federal procurements of connected devices."[196] U.S. Sens. Mark

---

Dempsey, *NTIA Holds Virtual Meeting of Multistakeholder Process on Internet of Things Security Upgradability and Patching*, COMMLAW MONITOR (July 28, 2017), http://www.commlawmonitor.com/2017/07/articles/federal-state-regulatory/ntia-holds-virtual-meeting-of-multistakeholder-process-on-internet-of-things-security-upgradability-and-patching/; *see also* Kirtley, *supra* note 173.

192. NAT'L TELECOMM. & INFO. ADMIN, *supra* note 24.

193. *Id.* at 3 (The section now reads: "[s]upport for routine security updates typically ends as a device or software reaches the end of its lifecycle. If [sic] may be helpful to describe how long can consumers expect, at a minimum, the device to receive security update support. A specific date for when support begins or ends (e.g. Jan. 1, 2025) may be preferable to a general time period, though companies may describe their product lifecycles differently. If the device will be supported indefinitely without foreseeable end, or if the duration update support is unknown, manufacturers might indicate this.").

194. NAT'L TELECOMM. & INFO. ADMIN, *supra* note 24.

195. John J. Heitmann & Jameson J. Dempsey, *NTIA Holds Virtual Meeting of Multistakeholder Process on Internet of Things Security Upgradability and Patching*, LEXOLOGY (July 28, 2017), https://www.lexology.com/library/detail.aspx?g=83a1cc1d-7a8a-4b28-b136-2adde1398188.

196. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111; *see also* Jane E. Kirtley, *U.S. Senators Introduce Bill Seeking to Improve*

R. Warner (D-Va.) and Cory Gardner (R-Colo.), co-chairs of the Senate Cybersecurity Caucus, as well as Sens. Ron Wyden (D-Or.) and Steve Daines (R-Mont.), introduced the "Internet of Things (IoT) Cybersecurity Improvement Act of 2017," which aimed to require that IoT "devices purchased by the U.S. government meet certain minimum security requirements."[197] "Inter-connected device" is defined as "a physical object that (a) is capable of connecting to and is in regular connection with the Internet; and (b) has computer processing capabilities that can collect, send, or receive data."[198]

The legislation outlines several requirements for IoT vendors, including that their IoT devices are "patchable" in order "to fix or remove a vulnerability or defect in the software or firmware component in a properly authenticated and secure manner."[199] Second, the bill requires vendors to ensure that their products do not contain "known vulnerabilities,"[200] meaning "any attribute of hardware, firmware, software, process, or procedure or combination of 2 or more of these factors that could enable or facilitate the defeat or compromise of the confidentiality, integrity, or availability of an information system or its information or physical devices to which it is connected."[201] Third, the bill requires that vendors ensure their IoT devices "rely on standard protocols," such as "standard ports for network traffic," encryption, or "interconnection with other

---

*Security of IoT Devices*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 405–09 (2017).

197. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111.

198. Internet of Things Cybersecurity Improvement Act of 2017, *supra* note 111; *see also* Sarah Wronsky & Lawrence Block, *Proposed Internet of Things Cybersecurity Bill May Create Hurdles for Government Contractors*, GLOBAL REG. ENFORCEMENT LAW BLOG (Aug. 11, 2017), https://www.lexology.com/library/detail.aspx?g=c0da944b-4c46-4812-8bbf-dbf2540db87f.

199. *See* Internet of Things Cybersecurity Improvement Act of 2017, *supra* note 111; Sen. Mark Warner et al., *Fact Sheet, Internet of Things Cybersecurity Improvement Act of 2017*, MARK R. WARNER, U.S. SENATOR FROM COMMONWEALTH VA., https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act—-fact-sheet.pdf (last visited Mar. 1, 2018).

200. Internet of Things Cybersecurity Improvement Act of 2017, *supra* note 111; *see also* Mark Warner et al., *supra* note 199.

201. Internet of Things Cybersecurity Improvement Act of 2017, *supra* note 111.

devices."[202] Finally, IoT devices cannot "include any fixed or hard-coded credentials used for remote administration, the delivery of updates, or communication."[203]

The legislation next outlines ways IoT vendors can help manage risks stemming from insecure devices. More specifically, if a governmental agency "reasonably believes that procurement of an [IoT] device [compliant with the legislation] would be unfeasible or economically impractical," it may petition the Office of Management and Budget (OMB) for permission "to purchase a non-compliant [IoT] device."[204] The OMB is required to develop "alternative network-level security requirements for devices with limited data processing and software functionality."[205] Each governmental agency is also required to maintain an inventory of their use of IoT devices.[206] Finally, the bill directs the Department of Homeland Security National Protection and Programs Directorate (NDDP) to

> [w]ork with industry to develop coordinated disclosure guidelines for vendors selling IoT to the US government, which vendors would then adopt, allowing researchers to uncover vulnerabilities in those products and responsibly share them with the vendor, without fear of liability under the Digital Millennium Copyright Act (DMCA) or Computer Fraud and Abuse Act (CFAA).[207]

In an August 1, 2017 statement, Sen. Warner explained why the legislation is needed.[208] "While I'm tremendously excited about the innovation and productivity that Internet-of-Things devices will unleash, I have long been concerned that too many Internet-connected devices are being sold without appropriate safeguards and protections in place," said Sen. Warner. "This legislation would establish thorough, yet flexible, guidelines for Federal Government procurements of connected devices. My hope is that this legislation will remedy the obvious market

---

202. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111; *see also* Mark Warner et al., *supra* note 199.

203. Internet of Things Cybersecurity Improvement Act of 2017, *supra* note 111.

204. *Id.*

205. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111.

206. *Id.*

207. Mark Warner et al., *supra* note 199.

208. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111; *see also* Kirtley, *supra* note 196.

failure that has occurred and encourage device manufacturers to compete on the security of their products."[209]

Sen. Gardner agreed, saying,

> The Internet of Things (IoT) landscape continues to expand, with most experts expecting tens of billions of devices operating on our networks within the next several years[.]As these devices continue to transform our society and add countless new entry points into our networks, we need to make sure they are secure from malicious cyber-attacks. This bipartisan, commonsense legislation will ensure the federal government leads by example and purchases devices that meet basic requirements to prevent hackers from penetrating our government systems without halting the life-changing innovations that continue to develop in the IoT space.[210]

An August 2, 2017 *Business Insider* commentary noted that the legislation is "limited" because "[i]t only applies to vendors supplying the US federal government."[211] However, the article also cited Ray O'Farrell, chief technology officer at cloud computing firm VMware, who contended that the bill "includes 'reasonable security recommendations' that would be important to improve protection of federal government networks."[212] Reed Smith LLP associate Sarah Wronsky and partner Lawrence Block also noted that despite the bill being limited in its scope, it still represents an important step to address IoT security.[213] "Although the bill does not apply to consumer devices, industry experts anticipate the proposed legislation is a stepping stone to broader regulation of security and privacy in all IoT devices," Wronsky and Block wrote in an August 11 commentary for the *Global Regulatory Enforcement Law Blog*.[214] "Despite its rapid increase in procurement of IoT devices, the government has yet to adequately address critical issues, including risk and uncertainty about privacy and security of the devices."[215] As of

---

209. Press Release, U.S. Senator for Virginia Mark R. Warner, *supra* note 111.

210. *Id.*

211. Rob Price, *US Lawmakers Are Trying to Fix the Security Nightmare That Is the 'Internet of Things'*, BUS. INSIDER (Aug. 2, 2017), http://www.businessinsider.com/r-us-senators-to-introduce-bill-to-secure-internet-of-things-2017-8.

212. *Id.*

213. Wronsky & Block, *supra* note 198.

214. *Id.*

215. *Id.*

February 2018, the Senate bill remained in committee, with a companion bill promised in the House of Representatives.[216]

4. U.S. House of Representatives Bill

In October 2017, several U.S. Representatives also took aim at regulating IoT devices, though in this case specifically targeting medical devices, or Internet of Medical Things (IoMT). Rep. David Trott (R-Mich.) introduced H.R. 3985, the "Internet of Medical Things Resilience Partnership Act of 2017," which was first co-sponsored by Rep. Susan Brooks (R-Ind.) then by Rep. Erik Paulsen (R-Minn.) and Rep. Daniel Donovan (R-N.Y.).[217] Referred to the Subcommittee on Health, the bill's purpose is to "establish a working group of public and private entities led by the Food and Drug Administration to recommend voluntary frameworks and guidelines to increase the security and resilience of Internet of Medical Things devices, and for other purposes."[218]

The bill requires the Commissioner of the FDA, in consultation with the NIST, to establish the working group, which will help create a report to be submitted to Congress. The report would be required to include:

> (1) an identification of existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to mitigate vulnerabilities in the devices described in subsection (a); (2) an identification of existing and developing international and domestic cybersecurity standards, guidelines, frameworks, and best practices that mitigate vulnerabilities in such devices; (3) a specification of high-priority gaps for which new or revised standards are needed; and (4) potential action plans by which such gaps can be addressed.[219]

The NIST, an agency under the U.S. Department of Commerce, has previously drafted numerous documents, models, and more providing guidance related to cybersecurity

---

216. Shaun Waterman, *How Congress Could Handle Cybersecurity-Focused Bills in 2018*, CYBERSCOOP (Jan. 8, 2018), https://www.cyberscoop.com/congress-2018-cybersecurity-outlook/.

217. Internet of Medical Things Resilience Partnership Act of 2017, H.R. 3985, 115th Cong. (2017); *see also H.R. 3985—Internet of Medical Things Resilience Partnership Act of 2017*, CONGRESS.GOV, https://www.congress.gov/bill/115th-congress/house-bill/3985/cosponsors (last visited Mar. 14, 2018).

218. H.R. 3985; *see also* Segura et al., *supra* note 78.

219. H.R. 3985, § 2(c).

and IoT, all of which are available on their website.[220] If H.R. 3985 is eventually passed, or perhaps even if it is not, the NIST, as well as the FDA, will continue to be involved in drafting policies, recommendations, reports, and more related to IoT devices, including IoMT.

### B. PRIVATE SECTOR COMPANIES SELF-REGULATION

Although some experts have demanded that the federal government address and regulate the IoT, others have called on private companies to engage in self-regulation. Larry Karisny, the director of ProjectSafety.org, an organization that finds, tests, and deploys solutions for cyber security,[221] argues that it would be more advantageous for the IoT industry to self-regulate given that IoT suppliers and venture capitalist startups are "clearly aware" that they have to address the security and privacy issues of IoT devices or risk losing customers, spending money on regulatory issues, or facing legal action.[222] He also contends that the IoT industry is already the one "moving cybersecurity forward."[223]

On October 23, 2017, *Engadget* reported that Google, Sprint, and other companies were backing UK mobile chip designer ARM's new security framework called Platform Security Architecture (PSA).[224] The goal of the project is to create a common industry framework and security foundation for every IoT device.[225] According to ARM, 100 billion IoT devices already use its designs, with another 100 billion expected by 2021.[226] PSA is comprised of "threat models, security analyses, hardware and firmware architecture specifications, and an open source firmware reference implementation," which, collectively, "provide[] a recipe" for security to be consistently designed into

---

220. *NIST Initiatives in IoT*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot (last visited Feb. 2, 2018).

221. *About*, PROJECT SAFETY, https://www.projectsafety.org/about (last visited Feb. 2, 2018).

222. Karisny, *supra* note 62.

223. *Id.*

224. Steve Dent, *Google and Others Back Internet of Things Security Push*, ENGADGET (Oct. 23, 2017), https://www.engadget.com/2017/10/23/google-arm-internet-of-things-security/.

225. *See id.*

226. *Id.*

IoT devices at the hardware and firmware levels.[227] The framework therefore applies to the entire IoT industry and to all IoT devices, according to ARM.[228]

In an October 23, 2017 "SiliconANGLE" blog post, senior staff writer Mike Wheatley explained that ARM's proposal would address three problems associated with the IoT: first, that IoT devices "cannot easily be updated with new software to patch known vulnerabilities."[229] Second, PSA could address the problem that IoT devices come with default security credentials and generic usernames and passwords, which most consumers neglect to change or do not know that they need to change.[230] Finally, the initiative could address that most IoT devices store and send private data in plain-text format, which makes it easier to obtain if a device is compromised.[231]

Wheatley also contended that industry analysts, in addition to several large corporations, supported ARM's proposal.[232] He quoted Patrick Moorhead, president and principal analyst at research firm Moor Insights & Strategy, who said:

> [b]road-based IoT deployment will require a fundamental rethinking on security and I think ARM's industry proposal has a lot of merit . . . . Securing a trillion end points make security mandatory, not optional, and ARM's proposal contemplates many of the most aggressive surface attack points and also provides a way to update the silicon in the future for new kinds of attacks.[233]

On January 17, 2018, *Business Wire* reported that another company was seeking to improve security of the IoT.[234] VDOO, a cybersecurity company, which says that it aims to become the

---

227. *Platform Security Architecture*, ARM, https://developer.arm.com/products/architecture/platform-security-architecture (last visited Feb. 2, 2018).

228. *Id.*

229. Mike Wheatley, *Arm Unveils Plan to Secure the "Internet of Things" Inside the Chip*, SILICONANGLE (Oct. 23, 2017), https://siliconangle.com/blog/2017/10/23/arm-unveils-platform-security-architecture-secure-internet-things/.

230. *Id.*

231. *Id.*

232. *Id.*

233. *Id.*

234. Matt Burke, *With $13M in Initial Funding, VDOO Aims to Secure the Internet of Things (IoT)*, BUS. WIRE (Jan. 17, 2018), https://www.businesswire.com/news/home/20180117005711/en/13M-Initial-Funding-VDOO-Aims-Secure-Internet; *see also Solutions*, VDOO, https://www.vdoo.com/solutions.html (last visited Feb. 2, 2018).

"Security Authority of IoT devices,"[235] announced it had raised $13 million in initial funding to develop the company's IoT security platform.[236] The platform is intended to provide an automated process that analyzes gaps in devices' security and subsequently delivers the approximate security requirements and implementation guidance based on the analysis.[237] The platform would also provide security certification for nearly all IoT devices.[238] Netanel Davidi, Co-CEO and founder of VDOO, claims that:

> [t]he problem is that there are no actionable processes or standards to guide IoT makers in the implementation of the proper security for each specific device. VDOO helps IoT makers protect their customers, by enabling them to set and implement the right security for each of their devices, in a quick and balanced manner.[239]

In a January 31, 2018 post on her blog, Stacey Higginbotham, the former Senior Editor of *Fortune,* states that she "like[s] VDOO's idea of trying to protect devices before they head out in the field in a scalable way."[240] She also notes, however, that VDOO faces several challenges, including that it is a "tall order" to ensure that "once a vulnerability is found, the [IoT] device gets updated and all devices in the field get patched."[241]

Higginbotham also notes that another startup, Armis, is attempting to improve IoT security from the "end-user perspective" by offering a subscription-based software that monitors the devices in a corporate or factory network.[242] If a device demonstrates security vulnerabilities or other problems,

---

235. *About VDOO*, VDOO, https://www.vdoo.com/about.html (last visited Mar. 3, 2018).

236. Burke, *supra* note 234.

237. *Id.*; *see also* Lindsey O'Donnell, *IoT Security Startup VDOO Nabs $13M in Funding, with Former Palo Alto Networks Channel Exec Heading Up Partner Program Strategy*, CRN (Jan. 18, 2018), http://www.crn.com/news/internet-of-things/300098141/iot-security-startup-vdoo-nabs-13m-in-funding-with-former-palo-alto-networks-channel-exec-heading-up-partner-program-strategy.htm.

238. Burke, *supra* note 234.

239. *Id.*

240. Stacey Higginbotham, *Two Startups and Two Approaches to IoT Security*, STACEY ON IOT (Jan. 31, 2018), https://staceyoniot.com/two-startups-and-two-approaches-to-iot-security/.

241. *Id.*

242. *Id.*; *see also Armis Launches from Stealth to Eliminate IoT Security Blind Spot for Enterprises*, PR NEWSWIRE (June 6, 2017), https://www.prnewswire.com/news-releases/armis-launches-from-stealth-to-eliminate-iot-security-blind-spot-for-enterprises-300469178.html.

Armis' software sends information to other security programs used by the company or it attempts to shut down the problematic equipment.[243]

## IV. REGULATION OF THE INTERNET OF THINGS IN THE EUROPEAN UNION

Meanwhile, the European Union and the Article 29 Working Party have also taken action directly and indirectly affecting the IoT, including issuing position papers and an opinion,[244] as well as passing the General Data Protection Regulation (GDPR) and ePrivacy Regulation,[245] though questions remain about how the new regulations will affect the IoT. These regulations demonstrate the different approaches taken by the EU and the United States. The EU uses an omnibus approach, providing Europeans with certain rights of privacy across all platforms and sectors. The United States has a "patchwork quilt" of privacy laws applying to different industries.[246] Moreover, under the First Amendment, United States law typically balances privacy rights and interests against freedom of expression, whereas the EU contends that privacy is a fundamental right, and the use of personal data by third parties should be subject to regulation, controls, and transparency, requiring government oversight.

### A. ARTICLE 29 WORKING PARTY PUBLISHES INTERNET OF THINGS OPINION; EUROPEAN UNION PUBLISHES POSITION PAPERS

In September 2014, the Article 29 Data Protection Working Party, which provides independent advice on data protection matters to the European Commission and helps develop data protection policies in the EU Member States, published "Opinion

243. *Id.*

244. *See generally Article 29 Working Party*, EUR. COMM'N, http://ec.europa.eu/newsroom/article29/news-overview.cfm.

245. *See IoT Regulation: IoT, GDPR, ePrivacy Regulation and More Regulations*, I-SCOOP (Mar. 10, 2017), https://www.i-scoop.eu/internet-of-things-guide/iot-regulation/; *Proposal for an ePrivacy Regulation*, EUR. COMM'N (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation; Jane E. Kirtley, *EU Proposes ePrivacy Regulation*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 576–79 (2017); *EU ePrivacy Regulation*, INT'L ASSOC. PRIVACY PROF. (2017), https://iapp.org/resources/topics/eu-eprivacy-regulation/.

246. Singer, *supra* note 17.

8/2014 on the Recent Developments on the IoT."[247] In particular, the Working Party raised six particular concerns related to IoT devices, including "lack of control and information asymmetry,"[248] "low-quality consent,"[249] "extrapolation of inferences from data and repurposing of original processing,"[250] "intrusive identification of behaviour [sic] patterns and user profiling,"[251] "limitations on the possibility of remaining anonymous whilst using services,"[252] and "security risks,"[253] such as cyberattacks.[254] The opinion also addressed how different EU laws would apply to the processing of personal data by IoT devices and the different parties within the IoT

---

247. European Commission, Opinion 8/2014 on the on [sic] Recent Developments on the Internet of Things, 14/EN WP 223 (Sept. 16, 2014), www.dataprotection.ro/servlet/ViewDocument?id=1088 (stating that new proposals will strengthen individual rights and tackle the challenges of globalization and new technologies); *see also The Internet of Things and Privacy in Europe and the USA*, TAYLOR WESSING (Mar. 2015), https://united-kingdom.taylorwessing.com/globaldatahub/article_wp29_iot.html (stating that Opinion 8/2014 will provide data protection through its discussion and analysis on a variety of subjects: wearable technology, quantified self, and home automation (domotics), information asymmetry, low-quality consent, data repurposing, intrusive identification of behavior patterns and user profiling, and security risks).

248. *Internet of Things and Privacy in Europe and the USA*, *supra* note 247 (stating that "lack of control and information asymmetry" is "the communication between individuals, devices and backend systems resulting in the generation, storage and sharing of certain IoT-pushed data over which the end user has no control").

249. *Id.* ("Many IoT devices do not contain an obvious point at which the end user can give consent and, even more difficult, many IoT-related services do not give any alternatives to the end user's personal data being created, stored or shared. In these situations, there must be new ways of obtaining a valid consent from the end user (e.g. privacy proxies or 'sticky policies' which stay with the data regardless of which party has access to it).").

250. *Id.* (stating that "extrapolation of inferences from data and repurposing of original processing" is the disclosure of raw data to third-parties and the "regeneration of data for new purposes can easily go beyond the purposes for which the data was originally collected").

251. *Id.* (defining "intrusive identification of behaviour [sic] patterns and user profiling" as certain private behaviors and habits becoming unwantedly identifiable through the use of the IoT).

252. *Id.* ("Wearing IoT objects that are close to the data subjects results in a range of identifiers being available (e.g. MAC addresses) with re-identification of anonymi[z]ed data also an issue.").

253. *Id.* (stating a "security risk" can make the date vulnerable to being attacked at various points, including at the communication link and storage infrastructure levels).

254. European Commission, *supra* note 247.

industry.[255] Finally, the Working Party addressed the obligations imposed on IoT stakeholders, as well as the rights of data subjects.[256] Ultimately, the Working Party concluded that although the IoT presents several benefits for users and IoT companies, the privacy and security challenges must also be followed closely, requiring IoT devices to have "legal and technical compliance."[257] The Working Party also intended the opinion to "contribute to the uniform application of the legal data protection framework in the IoT as well as to the development of a high level of protection with regard to the protection of personal data in the EU."[258]

In December 2016, the European Union Agency for Network and Information Security (ENISA) led an initiative resulting in the issuance of position papers on IoT security.[259] Joined by semiconductor manufacturing companies Infineon Technologies, NXP Semiconductors, and STMicroelectronics, ENISA cited concerns that a European market failure for cybersecurity and privacy "creates a severe risk that the European economy is falling behind in its ability to tap into the promising emerging IoT markets."[260] The papers concluded that there is "no basic level, no level zero defined for the security and privacy of connected and smart devices," nor are there any legal guidelines.[261] Thus, the agency contended that it is necessary to define the European Baseline Requirements for Security and Privacy in a way that "minimizes risk, is neutral in technological terms, and remains open to innovation."[262]

The top priorities outlined in the papers were related to the development of baseline requirements for IoT security and privacy.[263] ENISA and the manufacturers agreed that any existing and new EU regulation should take standards

---

255. *Id.*
256. *Id.*
257. *Id.*
258. *Id.*
259. Ofer Amitai, *Growing Regulation of IoT Security*, IOT J. (2017), http://www.iotjournal.com/articles/view?17024/2; *see also Common Position on Cybersecurity*, ENISA (Dec. 2016), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity/view.
260. *Common Position on Cybersecurity*, ENISA, *supra* note 259, at 1.
261. *Id.*
262. *Id.*
263. *See generally id.*

developed and supported by EU stakeholders into account.[264] As the following sections will suggest, the GDPR and ePrivacy Regulation may have implications for the IoT.[265] The papers also emphasized the need for EU Member States' existing security processes and services to be evaluated and adapted to IoT devices, eventually leading to certification of the processes.[266] In addition to analyzing and developing standard IoT requirements, the papers also called for greater awareness of EU citizens, organizations, and companies regarding security and privacy of the IoT.[267]

ENISA further advocates that baseline requirements of IoT security and privacy must be effective in all areas of the IoT industry, from components to complex systems.[268] The papers also called for appropriate training in schools, universities, and industry, a "level playing field" for all stakeholders, risk management practices, and more.[269]

Since the publication of the Working Party's opinion and ENISA's process papers in 2016, an EU organization, a European organization, and a European initiative have been developed to address the security and privacy concerns stemming from the IoT. The Alliance for Internet of Things Innovation (AIOTI) was initiated as a result of the European and global IoT technology and market developments.[270] According to its website, AIOTI "aims to create and master sustainable innovative European IoT ecosystems in the global context to

---

264. *Id.* at 1–2.

265. *See IoT Regulation: IoT, GDPR, ePrivacy Regulation and More Regulations*, I-SCOOP, (Mar. 10, 2017), https://www.i-scoop.eu/internet-of-things-guide/iot-regulation/.

266. *Common Position on Cybersecurity*, ENISA, *supra* note 259, at 3 (stating that current processes should be built on defined baseline security requirements and existing internationally recognized certification schemes. If the European Commission defined a policy framework for ensuring minimal security requirement for connected devices, the development of security standards would become more efficient and adapt to new circumstances related to IoT).

267. *Id.* ("There is a lack of awareness when it comes to security and privacy in IoT. Industry, especially SME, needs to be provided with information about existing security features such as encryption, appropriate key storage, strong authentication, privacy and identity management systems.").

268. *Id.* at 1.

269. *Id.* at 4.

270. *More About AIOTI*, ALLIANCE FOR INTERNET OF THINGS INNOVATION, https://aioti.eu/learn-more-about-aioti/ (last visited Feb. 2, 2018).

address the challenges of IoT technology and applications deployment including standardisation [sic], interoperability and policy issues."[271] The European Research Cluster on the Internet of Things (IERC) is a separate organization that aims to "address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities."[272] The group aims to foster communication and coordination between different IoT projects throughout Europe.[273]

A third European organization seeking to promote the IoT is the IoT-European Platforms Initiative (IoT-EPI), a collection of seven research and innovation projects related to the IoT.[274] The initiative, which has total funding of 50 M€ and a partner network of 120 established companies, is intended to develop innovative platform technologies and foster technology adoption.[275] The organization also holds special events meant to foster networking amongst IoT companies and other organizations.[276]

### B. GENERAL DATA PROTECTION REGULATION IMPLICATIONS

As alluded to above, experts contend that the GDPR may have implications for the IoT, though questions remain about how the provisions of these regulations will apply to IoT devices in practice. On April 27, 2016, the European Union (EU) formally adopted the General Data Protection Regulation (GDPR)[277] to replace the Data Protection Directive.[278] The GDPR, which becomes effective on May 25, 2018, creates new responsibilities and obligations for data controllers and processors, while seeking to provide a clearer legal environment in which EU companies can operate.[279] The EU estimated that this will save businesses a collective €2.3 billion ($2.7 billion) a

---

271. *Id.*

272. *About IERC*, EUR. RESEARCH CLUSTER ON THE INTERNET OF THINGS, http://www.internet-of-things-research.eu/ (last visited Feb. 2, 2018).

273. *Id.*

274. *About IoT-EPI*, IOT-EUROPEAN PLATFORMS INITIATIVE, http://iot-epi.eu/about/ (last visited Feb. 2, 2018).

275. *Id.*

276. *Id.*

277. 2016 O.J. (L 119).

278. 1995 O.J. (L 281); *see also* Jane E. Kirtley, *EU Continues Implementation Process for General Data Protection Regulation*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 567–72 (2017).

279. 2016 O.J. (L 119), art. 14.

year.[280] The regulation also aims to expand the privacy rights of EU citizens, providing them more control over their personal data.[281]

The GDPR applies to both "controllers" and "processors" of data.[282] A data controller is the person, organization, or business that determines how and why personal data is processed, whereas a data processor is the person or entity that processes personal data on behalf of the data controller.[283] The GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization [etc.]"[284] The GDPR applies to a company if it has a branch, office, subsidiary, or other establishment or partnership in the EU that collects, receives, transmits, uses, stores or otherwise processes personal data.[285] The GDPR will also apply both when a company offers goods or services to individuals in the EU and when a company collects any information that is considered personal identifiable information.[286] Controllers are responsible for ensuring that their processors abide by data protection laws.[287]

Experts agree that there are several requirements in the GDPR that may have implications on the IoT industry. For example, the GDPR requires companies or organizations to conduct Data Protection Impact Assessments (DPIAs) when data processing "'is likely to result in a high risk to the rights and freedoms of natural persons.'"[288] Given the high security and

---

280. European Commission Press Release Memo/17/1441, Questions and Answers – Data Protection Reform Package (May 24, 2017).

281. 2016 O.J. (L 119), art. 14.

282. *Id.*; *see also* Jane E. Kirtley, *EU Continues Implementation Process for General Data Protection Regulation*, *in* PRACTISING L. INST., COMMUNICATIONS LAW IN THE DIGITAL AGE 2017, at 567–72 (2017).

283. *Am I a 'Data Controller' or a 'Data Processor', and Why Is It Important Anyway?*, OSBORNE CLARKE (May 31, 2016), http://www.osborneclarke.com/insights/am-i-a-data-controller-or-a-data-processor-and-why-is-it-important-anyway/.

284. 2016 O.J. (L 119), art. 4(2).

285. *Id.* at art. 4(7).

286. *Id.*

287. *Id.*

288. *Data Protection Impact Assessments Under the GDPR*, IT GOVERNANCE, https://www.itgovernance.co.uk/data-protection-impact-assessment-dpia (last visited Feb. 2, 2018); *see also IoT Regulation: IoT, GDPR,*

privacy risks associated with the IoT, this requirement of the GDPR is likely to apply to IoT companies.

Second, the GDPR requires that data breaches be reported if personal data is involved, such as in DDoS and ransomware cyberattacks. Companies dealing with personal data must be able to identify and deal with security breaches, in addition to creating a mandatory notification system in the event of any breaches of personal data.[289]

Third, the GDPR outlines several requirements for how personal data is stored, either in the cloud or in-house hardware, and requires IoT companies to follow these provisions.[290]

A fourth area arises for the IoT in GDPR requirements that an individual's consent be obtained to process their personal data. Under the GDPR, silence or inactivity do not constitute valid consent; the data subject must agree to the data processing through an affirmative act.[291] Additionally, the GDPR states that children under age 13 cannot give consent, and children between 13 and 15 are subject to EU Member States' particular laws.[292] As a result, IoT companies who create and/or market IoT devices for children have additional mandatory considerations regarding consent.

Finally, the GDPR stipulates that data subjects have a right, at any time, to be informed about how their personal data is used and to whom it is disclosed.[293] IoT devices present additional technologies that can lead a data controller to potentially lose track of the information.[294]

### C. EPRIVACY REGULATION IMPLICATIONS

An additional framework that experts generally agree will have implications for the IoT is the ePrivacy Regulation, though

---

*ePrivacy Regulation and More Regulations*, I-SCOOP (Mar. 10, 2017), https://www.i-scoop.eu/internet-of-things-guide/iot-regulation/.

289. *Internet of Things Privacy: What GDPR Means for IoT Data*, LANNER (Oct. 24, 2017), https://www.lanner-america.com/knowledgebase/iot/internet-things-privacy-gdpr-iot-data-protection/.

290. *Id.*

291. Laura Vegh, *The Internet of Things in the Era of the GDPR*, EU GDPR COMPLIANT (Oct. 24, 2017), https://eugdprcompliant.com/internet-of-things-era-of-gdpr/.

292. *Id.*; *see also Internet of Things Privacy: What GDPR Means for IoT Data*, *supra* note 289.

293. Vegh, *supra* note 291.

294. *Id.*

the full effects have yet to be seen. On January 10, 2017, the European Commission adopted the ePrivacy Regulation, which is meant to complement the existing ePrivacy Directive.[295] The directive, adopted in 2002 to address issues raised by the 1995 Data Protection Directive—a framework that governed the collection, processing, and use of personal data—was intended to protect EU citizens' privacy and confidentiality rights as they used electronic communication services, as well as to regulate how telecommunications companies could use EU individuals' data.[296] The proposed ePrivacy Regulation extends coverage from telecommunication companies and internet service providers (ISPs) to include any company processing personal data.[297]

Additionally, the ePrivacy Regulation is intended to consolidate EU Member States' implementation of the law's protections and align it with the GDPR.[298] The move marks an additional step in the European Commission's attempts to harmonize data protection across the EU because regulations have binding legal force throughout every EU member state.[299] Conversely, EU directives require member states to adopt their own laws that implement the desired specific outcomes of the directive, which often results in variations across EU member states.[300]

Several experts point out that the ePrivacy Regulation "clearly" or "explicitly" mentions the IoT, specifically Recital 1, which states "the principle of confidentiality should apply to current and future means of communication,"[301] and Recital 12, which reads, "Connected devices and machines increasingly

---

295. *Proposal for an ePrivacy Regulation*, EUR. COMM'N (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation; *see also EU Proposes ePrivacy Regulation*, *supra* note 245.

296. *See generally* 2002 O.J. (L 201).

297. Rohan Massey, *European Union: Thoughts On EU's Draft E-Privacy Regulation*, LAW360 (Apr. 18, 2017), https://www.law360.com/articles/910235/thoughts-on-eu-s-draft-e-privacy-regulation.

298. *EU ePrivacy Regulation*, INT'L ASSOC. PRIVACY PROF. (2017), https://iapp.org/resources/topics/eu-eprivacy-regulation/.

299. *Id.*

300. *Difference Between a Regulation, Directive, and Decision*, USDA (Dec. 21, 2016), http://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision/.

301. *IoT Regulation: IoT, GDPR, ePrivacy Regulation and More Regulations*, *supra* note 245.

communicate with each other by using electronic communications networks. . . . In order to ensure full protection of the rights to privacy and confidentiality of communications . . . it is necessary to clarify that this Regulation should apply to the transmission of machine-to-machine communications."[302] Additionally, provisions regarding the processing of communications data and consent requirements could also apply to IoT devices, though experts remain unsure about how great of an effect the regulation will have and what the implications will be.[303]

## V. LIABILITY

According to a Mason Hayes & Curran May 2016 blog post, there are two main areas where liability can arise with IoT devices: a device malfunction and cyberattacks or hacks that lead to theft of personal data stored on the device or a larger network.[304] The question arises in each of these cases: who is liable?[305] So far, experts agree that this is largely unanswered.[306] However, several existing legal and regulatory concepts suggest how liability might be determined and handled with the IoT, including (1) enforcement actions by the FTC related to IoT devices, including those mentioned earlier section in this article, (2) End User License Agreements (EULAs) and product liability law, and (3) additional avenues, beyond product liability, that consumers may use to claim compensation for damages related to IoT devices.

---

302. EUR. PARL. DOC. (COM A8–0324/2017), http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324&language=EN; *see also Study on the Impact of the Proposed ePrivacy Regulation*, HÄRTING (Oct. 19, 2017), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf.

303. David Meyer, *Why the IoT Industry Needs to Pay Attention to ePrivacy Regulation*, INTERNET OF BUS. (Oct. 23, 2017), https://internetofbusiness.com/iot-industry-needs-pay-attention-eprivacy-regulation/; *see also Study on the Impact of the Proposed ePrivacy Regulation*, *supra* note 302.

304. *Untangling the Web of Liability in the Internet of Things*, MASON HAYES AND CURRAN TECH LAW BLOG (May 19, 2016), https://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things.

305. *Id.*; Michael Kassner, *IoT and Liability: Who Pays When Things Go Wrong?*, TECHREPUBLIC (Aug. 1, 2016), https://www.techrepublic.com/article/iot-and-liability-who-pays-when-things-go-wrong/.

306. *E.g., Untangling the Web of Liability in the Internet of Things*, *supra* note 305.

### A. EXTRAPOLATING FROM FTC ENFORCEMENT ACTIONS

FTC enforcement actions related to IoT devices may predict potential liability considerations for the IoT. In its complaints against ASUS, D-Link, Lenovo, Vizio, and VTech, the FTC made several claims under Section 5(a) of the Federal Trade Commission Act (FTC Act), which makes "unfair and deceptive acts or practices in or affecting commerce" unlawful.[307]

According to the Federal Reserve's Consumer Compliance Handbook, Section 5(a), acts or practices are considered deceptive where "(1) a representation, omission, or practice misleads or is likely to mislead the consumer; (2) a consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and (3) the misleading representation, omission, or practice is material."[308] Acts or practices are considered unfair if they "cause[] or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[309]

One particular claim raised by the FTC in its enforcement actions was that an IoT company practiced "misrepresentation" when it failed to take "reasonable steps to ensure security." For example, in its complaint against D-Link, the FTC alleged that the company "[failed] to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers."[310] In its complaint against VTech, the FTC alleged that the company maintained in its privacy policy that most personal information was encrypted, when, in fact, it was not.[311] Similarly, the FTC claimed in several enforcement actions that IoT devices had

---

307. 15 U.S.C. § 45(a).

308. FED. RES., FTCA § 5 UNFAIR OR DECEPTIVE ACTS OR PRACTICES, at 1 (2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf; *see also* 15 U.S.C. § 45.

309. 15 U.S.C. § 45(n).

310. D-Link Complaint, *supra* note 134, ¶ 1.

311. VTech Complaint, *supra* note 161, ¶ 12.

"vulnerabilities,"[312] inadequate security measures,[313] and insecure designs.[314]

Second, the FTC also alleged in several of these cases that consumers were not notified of security breaches or of updates or patches that became available to improve security of IoT devices. For example, in its complaint against Vizio, the FTC alleged that the company "failed to adequately disclose that the 'Smart Interactivity' feature comprehensively collected and shared consumers' television viewing activity."[315]

Third, the FTC emphasized the security risks associated with users' personal data, such as in the case against Lenovo in which the FTC alleged that the company "created two significant security vulnerabilities" because the users' internet browser had access to "all of a consumer's sensitive personal information that was transmitted on the Internet, such as login credentials, Social Security numbers, financial account information, medical information, and web-based email communications."[316] In the case against VTech, the FTC alleged that the company had violated COPPA, which protects children's personal data.[317] Because the Commission enforces a variety of specific consumer protection statutes, it is possible it will attempt to make IoT companies liable for laws beyond COPPA, such as HIPAA, among others.

Finally, the FTC alleged in each of its enforcement actions listed above that consumers had been injured or harmed as a result of the unfair practices by the technology companies. The FTC alleged that ASUS "subjected consumers to substantial injury"[318] and that Lenovo's practice of collection and sharing of sensitive data without consumers' consent has "caused or is likely to cause substantial injury to consumers."[319]

However, although the FTC alleged in its complaint against D-Link that the company's practices "caused, or are likely to

312. ASUSTek Complaint, *supra* note 125, ¶ 3; Lenovo Complaint, *supra* note 148, ¶ 11.
313. VTech Complaint, *supra* note 161.
314. ASUSTek Complaint, *supra* note 125, ¶ 15.
315. Vizio Complaint, *supra* note 154, ¶ 38.
316. Lenovo Complaint, *supra* note 148, at ¶ 6 and 11.
317. VTech Complaint, *supra* note 161, at ¶ 17.
318. ASUSTek Complaint, *supra* note 125, at ¶ 35.
319. Lenovo Complaint, *supra* note 148, at ¶ 37.

cause, substantial injury to consumers in the United States,"[320] Judge Donato rejected this claim, ruling that the FTC needed to be more specific in tying its claims about a company's misrepresentations of IoT product security to evidence of concrete harm to consumers.[321]

Experts contended throughout 2017 that the FTC may, in fact, be shifting towards a "concrete harms" approach in its data security enforcement actions. While serving as acting Chairwoman of the FTC, Maureen K. Ohlhausen was one of two commissioners who were critical of the FTC's decisions to bring enforcement actions alleging unfair data security practices against companies in situations when consumer harm was not clearly apparent.[322] In January 2017, Ohlhausen dissented from the agency's filing of a complaint against D-Link, contending that the focus of FTC action should be a showing of tangible harm prior to taking enforcement action and that part of "regulatory humility" is to foster both business innovation and privacy innovation.[323]

In a February 2017 speech before the American Bar Association, Ohlhausen contended that her leadership of the FTC would focus on enforcement actions in which concrete harms could be alleged.[324] "The FTC should focus enforcement on matters where consumers are harmed or where companies don't keep their promises," Ohlhausen said during the speech. "The agency should focus on cases with properly and objectively determined concrete harms such as diminished or disrupted

---

320. D-Link Complaint, *supra* note 134, at ¶ 29.

321. *See* Fed. Trade Comm'n v. D-Link Sys., Inc., 2017 WL 4150873, at *5 (N.D. Calif. 2017).

322. *See* Glenn G. Lammi, *FTC Must Refocus on Harm to Consumers and Competition*, FORBES (Mar. 8, 2017, 2:03 PM), https://www.forbes.com/sites/wlf/2017/03/08/ftc-must-refocus-on-harm-to-consumers-and-competition/#6ad3376a5c11 (the other being former Commissioner Joshua Wright).

323. Allison Grande, *New FTC Chair to Shift Data Security Focus to Actual Harm*, LAW360 (Jan. 26, 2017, 9:28 PM), https://www.law360.com/articles/885212/new-ftc-chair-to-shift-data-security-focus-to-actual-harm.

324. Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Opening Keynote at ABA 2017 Consumer Protection Coference (Feb. 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf; s*ee also* James R. Hood, *Trump Appointee Sees Overreach in Earlier FTC Actions*, CONSUMER AFFAIRS (Feb. 8, 2017), https://www.consumeraffairs.com/news/ftcs-new-head-eyes-harms-based-approach-to-privacy-protection-020817.html.

competition, monetary injury, and unwarranted health and safety risks."[325]

By focusing on concrete harms, Ohlhausen promised "to deepen the FTC's understanding of the economics of privacy . . . includ[ing] studying consumer preferences and the relationship between access to consumer information and innovation."[326] She contended that concentrating on consumer injury will allow the FTC to be more selective and better allocate its limited resources. During her February 2017 speech, Ohlhausen said, "for every consumer protection case the FTC brings, we must ensure that we seek and obtain for consumers relief that is tied to consumer injury."[327]

Ohlhausen drew a distinction between a "notice-and-choice approach" to privacy protection and a "harms-based approach."[328] The "notice-and-choice" approach, generally favored by the FTC under President Barack Obama, gave consumers the choice to "opt out" of sharing certain types of information, such as Personal Identifiable Information (PII). The "harms-based" approach, on the other hand, seeks to protect consumers only from privacy breaches that are harmful.[329]

On April 4, 2017 *Consumer Affairs* reported that Electronic Frontier Foundation (EFF) staff attorney Sophia Cope claimed the harms-based approach "is exactly what companies have been hoping for."[330] "It removes consumer choice and control over their privacy," Cope wrote in an email to *Consumer Affairs*,[331]

> Now bureaucrats get to decide that certain data practices are not harmful, even if they include collecting highly sensitive information about people and what they do online, engaging in non-stop online surveillance, monetizing that information for commercial gain, and sharing that information with numerous unknown parties. Consumers deserve better from the FTC.[332]

---

325. Orson Swindle, *Why President Trump Should Choose Maureen Ohlhausen to Lead the FTC*, HILL (Feb. 2, 2017, 1:20 PM), http://origin-nyi.thehill.com/blogs/pundits-blog/the-administration/320468-why-president-trump-should-choose-maureen-ohlhausen-to.

326. Ohlhausen, *supra* note 324.

327. *Id.*

328. Hood, *supra* note 324.

329. Swindle, *supra* note 325.

330. Hood, *supra* note 324.

331. *Id.*

332. *Id.*

In October 2017, President Donald Trump announced that he would nominate Joseph Simons to replace Ohlhausen as the new head of the FTC, as well as naming three additional nominees to the agency.[333] Simons previously served as a co-chair of the antitrust practice at the law firm Paul Weiss, where his clients included Microsoft and Sony, among other technology companies.[334] Simons also served as the FTC's competition bureau under President George W. Bush.

According to *The Washington Post* on October 19, 2017, some policy analysts, including Berin Szoka, president of the think tank TechFreedom, argued that Simons' first task should be to clarify how the FTC communicates its expectations to companies involved in data security. In response to a question posed by the U.S. Senate Committee on Commerce, Science, and Transportation asking what he felt to be the top three challenges facing the FTC, Simons stated that one such challenge was that "[r]apid changes in technology and cyber threats provide a significant challenge to the Agency's ability to fulfill its consumer protection mission and provide meaningful guidance to the business community."[335] Simons argued that the FTC must continue to protect consumers despite these challenges, which would likely include IoT devices. He said, "It is critical, despite these challenges, that the FTC protect consumers without unduly burdening them or interfering with the ability of firms (especially small firms and new entrants) to use data to enhance competition."[336] Thus, although he did not explicitly

---

333. Brian Fung, *Trump's Pick for a Top Consumer Watchdog Once Represented Microsoft and MasterCard*, WASH. POST (Oct. 19, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/19/trumps-pick-for-a-top-consumer-watchdog-once-represented-microsoft-and-mastercard/?utm_term=.7f6effad8fd8; *see also* Ashley Gold, et al., *Trump Will Nominate Joseph Simons for FTC Chair*, POLITICO (Oct. 19, 2017), https://www.politico.com/story/2017/10/19/trump-simons-federal-trade-commission-243931.

334. Brian Fung, *supra* note 333.

335. JOSEPH SIMONS, STATEMENT ON BIOGRAPHICAL AND FINANCIAL INFORMATION FOR THE SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, https://www.commerce.senate.gov/public/_cache/files/6c4149af-3023-4825-90f1-3c38e279fd0d/6A0CCF409AF89DC8D5C0A84CE8730012.confidential—-simons—-committee-questionnaire-redacted.pdf; *see also* Li Zhou, *FTC Confirmation Hearing Soon?*, POLITICO (Feb. 6, 2018), https://www.politico.com/newsletters/morning-tech/2018/02/06/ftc-confirmation-hearing-soon-094789.

336. JOSEPH SIMONS, *supra* note 335.

discuss the IoT, Simons' answer suggested that the FTC will continue enforcement actions to protect consumers in the face of cyber threats.

Ultimately, questions remain about whether the FTC will continue enforcement actions against IoT companies if they cannot prove concrete harm. Even if the agency does not take this approach, Judge Donato's decision in the D-Link case problematizes the ability of the FTC to hold companies liable for harms caused to consumers without concrete evidence. It is also worth noting that the FTC actions described in this article are not binding court verdicts, though they still represent, potentially, the beginning of a standard for security in the IoT.[337]

### B. PRODUCT LIABILITY LAW AND END USER LICENSE AGREEMENTS

Providing additional insight into liability related to the IoT, product liability is an area of law in which manufacturers and retailers are held responsible for damages caused by their products' failures.[338] Liability claims fall into three categories: negligence, strict liability, and breach of warranty.[339] Negligence refers to liability where the product manufacturer's conduct is called into question, such as whether the company acted with a lesser standard of care than someone in similar circumstances would have exercised.[340] Strict liability holds a manufacturer responsible for the damages caused by its product, such as if it was defective, whether related to design, manufacturing, or packaging. A product may also be defective if the company failed to provide an adequate warning to consumers.[341] Finally, breach-of-warranty cases arise when a manufacturer violates the warranties it makes for a product.[342]

---

337. Lucas Amodio, *Is the Internet of Things Ripe for Product Liability Law?*, LINKEDIN (Feb. 3, 2016), https://www.linkedin.com/pulse/internet-things-ripe-product-liability-law-lucas-amodio-c-eh/.

338. Denis W. Stearns, *An Introduction to Product Liability Law*, MARLER CLARK (2001), https://marlerclark.com/pdfs/intro-product-liability-law.pdf.

339. *Products Liability: A Litigation Overview*, SMITH, GAMBRELL & RUSSELL (2013), http://www.sgrlaw.com/ttl-articles/2015/.

340. *Negligence*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/negligence (last visited Mar. 6, 2018).

341. *Products Liability: A Litigation Overview*, *supra* note 339.

342. *Id.*

For traditional devices, consumers can generally receive compensation from manufacturers, suppliers, or sellers provided they can demonstrate personal injury or property damage from a defective product, such as a traditional refrigerator causing a fire that burned down an individual's home.[343] However, this is not the case for most IoT devices, largely due to EULAs, which are contracts signed or accepted by consumers in order to use their IoT products.[344] Although IoT devices have the potential to cause or lead to a range of harm, such as from a hacker controlling a thermostat and turning off a homeowner's heat in the winter, causing pipes to freeze,[345] EULAs "allow manufacturers to disclaim most, if not all, liability for damages incurred by the usage of IoT products."[346] Thus, EULAs and software licenses make it very difficult, if not impossible, for consumers to claim compensations when products fail or when these types of damages occur.[347]

The challenge for consumers is that in order to gain full access to all the functionalities of most IoT devices, they must sign the software agreement or EULA, which is rarely negotiable.[348] Nest, a smart appliances vendor, for example, employs a restrictive EULA that disclaims all liabilities for its product's failures, but requires users to sign the agreement in

---

343. Eireann Leverett, *Time to Decide on Internet of Things Liability*, MEDIUM (Feb. 1, 2017), https://medium.com/privacy-international/time-to-decide-on-internet-of-things-liability-c39cee0142ff.

344. *Id.*; *see also* Leta Gorman, *The Era of the Internet of Things: Can Product Liability Laws Keep Up?*, DEF. COUNS. J., July 2017, 4, https://www.iadclaw.org/securedocument.aspx?file=DCJArticles/The_Era_of_the_Internet_of_Things.pdf (suggesting that consumers may be "compelled to sign a standard form agreement that automatically waived claims in order to use the software that accompanied the product").

345. Amodio, *supra* note 337.

346. Bao Kham Chau et al., Liability for Home IoT 2 (Dec. 2015) (unpublished final paper, MIT), https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall15-papers/Liability%20for%20hone%20IoT.pdf; *see also* Annalee Newitz, Dangerous Terms: A User's Guide to EULAs, ELECTRONIC FRONTIER FOUND. (Feb. 17, 2005), https://www.eff.org/wp/dangerous-terms-users-guide-eulas.

347. *See* Chau et al., *supra* note 346.

348. *See* Seth Stevenson, *By Clicking on this Article, You Agree to . . .* , SLATE (Nov. 17, 2014, 7:00 AM), http://www.slate.com/articles/technology/technology/2014/11/end_user_license_agreements_does_it_matter_that_we_don_t_read_the_fine_print.html.

order to use their smart thermostats.[349] Consequently, the users have entered into a contract with Nest in which they relinquish the right to sue for damages caused by the thermostat.

Perhaps the only viable way for consumers to hold manufacturers and others liable for damages caused by an IoT device is by demonstrating that the contract was "unconscionable."[350] In order for a contract to be deemed as such, the user must show both procedural unfairness ("procedural unconscionability") and unfairness in substantive terms ("substantive unconscionability"), "on a kind of sliding scale, where a showing of greater unfairness on one means that less unfairness need be shown on the other."[351] Generally, procedural unconscionability relates to the process of making a contract and includes unequal bargaining power or surprises in the contract process, such as obscure language hidden in small print.[352] Conversely, substantive unconscionability relates to the actual terms of the contract being one-sided or overly harsh.[353] However, there is to date no clear framework, nor court decision, related to unconscionability of EULAs tied to IoT devices.[354]

Additional aspects of IoT devices further complicate product liability.[355] First, the complexity of IoT devices' interconnectivity "makes it much harder to establish who is liable under traditional laws and regulations when something goes wrong."[356] Second, as Lucas Amodio, an intellectual property attorney at Armstrong Teasdale LLP, contends, where data is compromised by hacks, it is often hard to quantify the damage caused as opposed to physical damages.[357] The Mason Hayes & Curran 2016 blog post questions whether the aggrieved IoT user is required to prove they have suffered damage or harm stemming

---

349. *See* End User License Agreement, NEST, https://nest.com/legal/eula/ (last visited Feb. 16, 2018).

350. Chau et al., *supra* note 346.

351. BRIAN H. BIX, CONTRACT LAW RULES, THEORY, AND CONTEXT 90–91 (2012).

352. MERRIAM-WEBSTER'S DICTIONARY OF LAW 383 (Linda Picard Wood ed., 2016).

353. *Id.* at 474.

354. *See* Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 842 (2016).

355. Kassner, *supra* note 305; Amodio, *supra* note 337.

356. *Untangling the Web of Liability in the Internet of Things*, *supra* note 304.

357. Amodio, *supra* note 337; Gorman, *supra* note 344.

from an IoT company's actions.[358] One final consideration is whether liability related to IoT devices should be criminal, civil or both. The Mason Hayes & Curran post argues that the answer depends on the severity of the harm.[359]

### C. OTHER METHODS CONSUMERS CAN USE TO CLAIM COMPENSATION FOR DAMAGES

Product liability lawsuits are not the only way consumers can fight back when they suffer damages. Collective consumer backlash could deter companies from creating faulty products in the first place or discourage other consumers from buying the products.[360] Additionally, federal agencies, especially the FTC, may undertake enforcement actions against companies who do not adequately protect consumers' security and privacy, leading to settlements or other enforcement actions.[361] The Mason Hayes & Curran post also argues that an alternate approach to product litigation would be for courts and legislators to consider assigning liability between each actor in the IoT product and network chain, regardless of their culpability.[362] However, the authors of the post concede that this not as simple as it sounds because a court would be required to determine whether the liability lies with the IoT companies or the actual hacker.[363]

For example, on October 21, 2015, the Subcommittee on Commerce, Manufacturing, and Trade held a hearing on "Examining Ways to Improve Vehicle and Roadway Safety."[364] The Subcommittee considered a legislative staff discussion draft document that included multiple proposals intended to improve motor vehicle safety processes and privacy practices among auto manufacturers, and prepare the National Highway Traffic Safety Administration (NHTSA) for the next generation of

---

358. *Untangling the Web of Liability in the Internet of Things*, *supra* note 304.

359. *Id.*; *see also* Kassner, supra note 305.

360. Chau et al., *supra* note 346, at 9.

361. *Id.*

362. *Untangling the Web of Liability in the Internet of Things*, *supra* note 304.

363. *Id.*

364. MAJORITY STAFF OF H.R. COMM. ON ENERGY AND COMMERCE, 114TH CONG., MEMO FOR HEARING ON EXAMINING WAYS TO IMPROVE VEHICLE AND ROADWAY SAFETY (Oct. 2015), http://docs.house.gov/meetings/IF/IF17/20151021/104070/HHRG-114-IF17-20151021-SD002.pdf.

vehicles and innovation in the auto industry.[365] One draft measure proposed that car manufacturers be fined $5,000 a day if they did not submit a detailed privacy policy to the Department of Transportation.[366] Under the draft legislation, car manufacturers could be held liable if they violate any part of their own privacy policies or if they fail to file a privacy policy in the first place.[367] However, "the maximum penalty automakers face would be limited to $1 million, and they would be shielded from Federal Trade Commission scrutiny for 'unfair' or 'deceptive' acts related to privacy as long as their privacy policies meet all the legislation's requirements," thus creating a safe harbor for manufacturers.[368]

One final recourse for consumers could be through state law, specifically data disposal laws, security breach notification laws, and general data security laws pertaining to the private sector.[369] According to the National Conference of State Legislatures (NCSL), data disposal laws, passed by at least 32 states, require entities to destroy, dispose of, or otherwise make unreadable personal information.[370]

Conversely, security breach notification laws, enacted by 48 states and Washington, D.C., require private or governmental entities to notify individuals of security breaches in which personally identifiable information is implicated or compromised.[371] According to the NCSL, security breach laws

---

365. *Id.* (explaining the purpose of the memo in the introduction).

366. H.R. COMM. ON ENERGY AND COMMERCE, 114TH CONG., DISCUSSION DRAFT OF A BILL FOR HEARING ON EXAMINING WAYS TO IMPROVE VEHICLE AND ROADWAY SAFETY 22 (Oct. 2015), http://docs.house.gov/meetings/IF/IF17/20151021/104070/BILLS-114pih-DiscussionDraftonVehicleandRoadwaySafety.pdf.

367. Brian Fung, *Lawmakers Want to Fine Carmakers $5,000 a Day for Not Having a Privacy Policy*, WASH. POST: SWITCH (Oct. 19, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/10/19/lawmakers-want-to-fine-carmakers-5000-a-day-for-not-having-a-privacy-policy/.

368. *Id.*

369. Amy Talbott, Privacy Laws: How the US, EU and Others Protect IoT Data (or Don't), ZDNet (Mar. 7, 2016), http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/.

370. *Data Disposal Laws*, NAT'L CONF. OF STATE LEGISLATURES (Dec. 1, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

371. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

generally have provisions regarding "who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); definitions of 'personal information' (e.g., name combined with SSN, [driver's] license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information)."[372]

Thirteen states also have more general data security laws that address other aspects of security, generally taking a more preemptive or preventative approach.[373] Most contain requirements that businesses that own, license, or maintain personal data must implement and maintain reasonable security procedures, as well as protect personal information from unauthorized access, destruction, use, modification, or disclosure.[374] Massachusetts Regulation 201 CMR 17.00 provides an example of preemptive action in that it includes an extensive list of protocols companies must implement into their security architecture if they handle personal information.[375]

In a March 2016 special feature titled "Internet of Things: The Security Challenge," *ZDNet* contributor and *TechRepublic* associate editor Amy Talbott noted that at least one state has a law specifically addressing IoT devices—in this case, smart TVs.[376] She noted that California, which has comparably strong data privacy laws, has a statute related to the security of IoT televisions. Business & Professions Code sections 22948.20–22948.25 prohibit a "person or entity [from] provid[ing] the operation of a voice recognition feature within this state without prominently informing, during the initial setup or installation of a connected television, either the user or the person designated by the user to perform the initial setup or installation of the

372. *Id.*

373. *Data Security Laws—Private Sector,* NAT'L CONF. OF STATE LEGISLATURES (Dec. 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx; *see also* Ieuan Jolly, *Data Protection in the United States: Overview*, PRACTICAL LAW (July 1, 2017), https://content.next.westlaw.com/6-502-0467?transitionType=Default&firstPage=true&bhcp=1&contextData=(sc.Default).

374. *Id.*

375. *Id.*; *see also* 201 MASS. CODE REGS. 17.00 (2010).

376. Talbott, *supra* note 369.

connected television."[377] The law also limits how recordings collected by the remote can be used or distributed.[378]

Talbott also contended that these state privacy laws, although most do not specifically mention the IoT, are generally applicable to IoT devices because they frequently collect users' personal data.[379] However, a May 2017 article by FCW, which provides federal technology executives with information, ideas, and strategies, argues that its policymakers still must determine whether new laws at the federal and state level are needed to help ensure the security of IoT devices.[380] He quotes Naomi Lefkowitz, a senior privacy policy advisor at the NIST, who said that "there will be no perfect privacy," but that the IoT "require[s] additional legislative solutions."[381]

## VI. CONCLUSION

In the concluding pages of E.M. Forster's novella, *The Machine Stops*,[382] the human inhabitants of a dystopian subterranean world discover that "the Machine," the omnipotent mechanical being upon which they depend for food, shelter, communication, travel, and other elements necessary for life, is breaking down. Although initially the Machine had been merely a tool, subservient to its human masters, over time, "Humanity, in its desire for comfort . . . [q]uietly and complacently, [] was sinking into decadence, and progress had come to mean the progress of the Machine." Gradually, "all, save a few retrogrades, worship[ped] it as divine," relying on the Book of the Machine, a vast technological manual "with instructions against any possible contingency" to guide their lives. Complaints about malfunctions were channeled to a Committee on the Mending Apparatus, which in turn forwarded them to an anonymous Central Committee, which might or might not respond – or might retaliate with punishment. But as the original inventors of the Machine die off, fewer people understand how the Machine functions. The Mending Apparatus breaks down, and

377. CAL. BUS. & PROF. CODE § 22948.20–25.

378. *Id.*

379. Talbott, *supra* note 369.

380. Chase Gunter, *What Does the Internet of Things Mean for Data Breaches?*, FCW (May 11, 2017), https://fcw.com/articles/2017/05/11/iot-security-data-gunter.aspx.

381. *Id.*

382. Forster, *supra* note 1.

eventually, the Machine itself malfunctions and, without warning, stops, dooming humankind. Yet one of the characters observes, "Oh, tomorrow – some fool will start the Machine again, tomorrow!"

Forster's cautionary tale is obviously an allegory. It warns of the loss of privacy and humanity that can occur when human beings are too dependent on technology to fulfill their needs, and of the risks to fundamental values when that technology is poorly understood. His prescient novella encourages us to remember that we must be the ones to control "the Machine."

As the Internet of Things becomes more and more pervasive, it is tempting, and some might say inevitable, to simply cede individual sovereignty to those who develop and operate the technology. But through law, regulations, litigation, and consumer activism, we have the capacity to rewrite "The Book of the Machine." And we must.

***