

TOO SMART FOR ITS OWN GOOD: ADDRESSING THE PRIVACY AND SECURITY CHALLENGES OF THE INTERNET OF THINGS¹

By Jane Kirtley and Scott Memmel

I. INTRODUCTION

At a July 25, 2018 summit in Finland, Russian President Vladimir Putin gave President Donald Trump an Adidas “smart” soccer ball.² President Trump smiled, accepted the ball, and posed for several photographs holding the gift, before throwing it to an aide in the audience. Several observers, however, immediately raised security and privacy concerns related to the ball, arguing it could potentially be used in a cyberattack or to spy on the president or United States. U.S. Sen. Lindsey Graham (R-S.C.) tweeted, “[I]f it were me, I’d check the soccer ball for listening devices and never allow it in the White House.”³

Bloomberg reported on July 25 that the ball did, in fact, “contain[] a chip with a tiny antenna that transmits [information] to nearby [cell]phones.”

The chip, which is located under a logo on the ball reading “near-field communication tag,” is a common feature of the Adidas “AG” ball. It allows users to access videos, games, and other content by placing their mobile phone near the ball.⁴

Bloomberg reporter Vernon Silver suggested in his July 25 article that the chip could, potentially, “be programmed to initiate [a cyberattack] on a [mobile] phone,” citing a 2015 *Forbes* report that an engineer had used a similar chip to send a nearby Android phone a request to open a link that would install a malicious file that takes over the phone.⁵

Continued on page 19

TOO SMART FOR ITS OWN GOOD: ADDRESSING
THE PRIVACY AND SECURITY CHALLENGES OF
THE INTERNET OF THINGS 1

By Jane Kirtley and Scott Memmel

ONLINE CONTRACT FORMATION..... 3

A.J. Zottola, Christopher Kim, Allison Laubach, and Stephanie
Molyneaux



Wolters Kluwer

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.

Too Smart for Its Own Good *from page I*

Linus Neumann, a spokesman for German hacker collective Chaos Computer Club, however, told *Bloomberg* that “such a multi-stepped [cyber]attack [was] unlikely.”⁶ Silver also noted that it “couldn’t be determined from the photos [of the event and ball] whether the chip might have been removed, replaced with actual spy gear, or, even more remotely, whether the entire ball itself was fabricated for the event and only resembled the Adidas model in question.” *The Hill* noted on July 25 that the ball went through a security screening, a routine procedure for all gifts given to the president.⁷

Nevertheless, the Adidas soccer ball highlighted concerns often raised by numerous other “smart” or Internet-connected devices that are part of the Internet of Things (IoT). 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.”⁸ These devices or sensors are most commonly sold commercially to consumers but are also sold and used in “business-to-business contexts.”⁹ The IoT market is generally divided into nine segments, including Industrial IoT, Retail, Smart Utilities & Energy, Healthcare, Smart Cities, Connected Homes, Wearables, Connected Cars, and Personal Health.¹⁰

In the first half of 2018, experts predicted that the IoT would continue to grow rapidly.¹¹ IBM predicted that the number of IoT devices would grow to over 11 billion in 2018 and will increasingly incorporate Artificial Intelligence (AI), potentially making IoT devices “smarter” and “more productive,” according to *Forbes* on Jan. 4, 2018.¹² A July 2018 report from *GrowthEnabler* indicated that the IoT is expected to reach \$457.29 billion globally by 2020, up from \$157 billion in 2016.¹³ The study predicted that the number of IoT network connections will reach 27 billion by 2025, growing by 16 percent each year.¹⁴

A separate study by Gartner, a global research and advisory firm, predicted that by 2020, IoT technology will be found in 95 percent of electronics for new product designs.¹⁵ Juniper Research predicted that due to the continued proliferation of IoT devices, security spending worldwide on the IoT will increase to \$6 billion in 2023, an increase of 300 percent from 2018.¹⁶

Experts, however, warn that as the IoT continues to grow, so too do the privacy and security concerns involving IoT devices, with regulatory efforts by the federal government still lagging behind.¹⁷ Nevertheless, the FTC, the Food and Drug Administration (FDA), the National Institute of Standards and Technology (NIST), and U.S. Congress each took actions throughout 2017 and 2018 in an attempt to address some of these concerns.

This article first addresses the privacy and security concerns associated with the IoT, primarily related to “smart” TVs, “smart” cities, and medical devices, or the Internet of Medical Things (IoMT), as well as a new form of domestic abuse in which abusers use IoT devices to target or harass their current or former partners. Second, this article examines some of the regulatory actions contemplated by the federal government, including the FTC, FDA, NIST, and the House of Representatives. Finally, this article concludes by arguing that the federal government’s attempts to regulate the IoT raise more questions than they answer, including what is driving the regulation in the first place, as well as how regulatory efforts will be impacted by international frameworks and standards, such as the European Union’s (EU) General Data Protection Regulation (GDPR).

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

For several years, IoT observers and stakeholders have raised privacy and security concerns related to IoT devices.¹⁸ The primary privacy concern of IoT devices is that they directly collect sensitive information, including financial account numbers, health information, precise geolocation, and more.¹⁹ Experts have identified two particular types of “extremely sensitive” personal data, including health data and data collected from children’s toys.²⁰

The primary security concern of the IoT is the susceptibility of devices to cyberattacks, such as the May 2017 WannaCry attack²¹ and the October 2016 Distributed Denial of Service (DDoS) attacks²² that targeted the IoT.²³ A ransomware attack occurs when hackers infect a computer with a virus, allowing them to encrypt the computer’s data and make it inaccessible to the user(s).²⁴ The hackers then demand a

ransom to decrypt the data and delete the files if the user(s) fail to pay the ransom within a certain amount of time.²⁵ A DDoS attack “is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.”²⁶ The cybercriminal begins by exploiting the vulnerability of just one device, making it the “master,” which then identifies and targets other vulnerable devices, networks, and systems.²⁷

In 2018, new areas of security and privacy concerns, however, have arisen, including “smart” TVs and cities, as well as medical devices. Additionally, several observers noted that IoT devices were beginning to be used more frequently in a new form of domestic abuse in which abusers target and harass their partners or former partners by changing the settings of a smart thermostat, playing bursts of loud music through “virtual assistant” devices, and changing the lighting throughout their home, among other actions.

A. “SMART” TELEVISIONS

“Smart” TVs, which were owned by 45 percent of U.S. households in 2017,²⁸ are IoT devices raising particular privacy and security concerns. On July 5, 2018, *The New York Times* published an article by business reporter Sapna Maheshwari titled “How Smart TVs in Millions of U.S. Homes Track More Than What’s On Tonight.”²⁹ Maheshwari described how Internet and data companies “have harnessed new technology to immediately identify what people are watching on internet-connected TVs, then using that information to send targeted advertisements to other devices in their homes.” She wrote that marketers “have eagerly embraced such practices,” but that they have raised concerns and scrutiny from regulators and privacy advocates.³⁰

Maheshwari provided the example of Samba TV, one of the largest companies worldwide that tracks viewer information in order to personalize viewing recommendations. According to a spokesperson, the company “collected viewing data from 13.5 million smart TVs in the United States, and it has raised \$40 million in venture funding.”³¹ Samba TV does so through “Samba Interactive TV,” a service that provides special offers and recommends television shows after consumers select an “enable button.”³²

Maheshwari, however, noted that the button “does not detail how much information Samba TV collects to make those recommendations.”³³ She further asserted that consumers “couldn’t read [Samba TV’s terms of service and privacy policy] unless they went online or clicked through to another screen on the TV.” Maheshwari added, “The privacy policy, which provided more details about the information collected through the software, was more than 4,000 words, and the terms exceeded 6,500 words.”³⁴

The service collects “nearly everything that appears on the TV on a second-by-second basis, essentially reading pixels to identify network shows and ads,” and allows advertisers to base their targeting depending on whether a consumer watched conservative or liberal media outlets, for example. Additionally, the service identifies a consumer’s other IoT devices that share the same Internet connection as the smart TV.³⁵

Samba TV claimed that it adheres to the Federal Trade Commission’s (FTC) privacy guidelines, arguing that it does not directly sell consumers’ data to third parties, but instead allows advertisers to pay to direct ads to other IoT devices in a consumer’s home.³⁶ Several observers, however, raised concerns about the company’s approach. In an interview with *The New York Times*, Justin Brookman, director of consumer privacy and technology policy at Consumers Union, an advocacy group, argued that smart TV companies should be more transparent for consumers.³⁷ “It’s still not intuitive that the box maker or the software embedded by the box maker is going to be doing this,” he said. “I’d like to see companies do a better job of making that clear and explaining the value proposition to consumers.”³⁸

On July 18, 2018, *Techdirt* called the smart TV industry “the poster child for dismal privacy, transparency[, and] security standards.”³⁹ Karl Bode wrote that smart TV vendors “have been among the laziest sectors around in terms of making sure private consumer data is adequately encrypted, and that consumers understand that their viewing habits and even some in-room conversations are being hoovered up and monetized, usually sloppily.”⁴⁰

Jonathan Mayer, an assistant professor of computer science and public affairs at Princeton University, said in an interview with Maheshwari that smart TV companies “aren’t subject to the stricter rules and regulations regarding viewing data that have traditionally

applied to cable companies,” leading to “this rise of weird ways to figure out what someone’s watching.”⁴¹ He added that “as long as [smart TV companies are] truthful to consumers, even if you make it really hard to exercise choices or don’t offer choices at all, you probably don’t have much of a legal issue” under FTC regulations.⁴²

In a Jan. 11, 2018 commentary, Ryan Barrett, the vice president of security and privacy at business cloud email provider Intermedia, argued that smart TVs also raise privacy and security concerns for small and mid-sized businesses.⁴³ “The potential risk is even greater for businesses that bring IoT devices into their companies. Consumers might get creeped out to think about their personal devices monitoring them and listening to their conversations, but businesses aren’t really thinking about the risks from this perspective,” he wrote. “[T]hese businesses are utilizing things such as smart TVs. Often smart TVs are connected to a Wi-Fi network to display analytics and statistics, but you’d be surprised at how often those TVs are connecting back to their manufacturers to gather advertising information and your usage statistics.” Barrett continued, “Some of the new TVs have webcams on them with incorporated microphones. And then there are cameras in the lobby. All this private business data about when and where people are coming and going and what they are doing is being recorded in the cloud, protected only by a password.”⁴⁴

On July 12, 2018, U.S. Sens. Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.) sent a letter to FTC Chairman Joseph Simons requesting that the agency “launch an investigation into the privacy policies and practices of smart TV manufacturers,” citing Maheshwari’s July 5 *New York Times* story.⁴⁵ The senators also cited Samba TV’s practices and wrote, “Regrettably, smart TV users may not be aware of the extent to which their televisions are collecting sensitive information about their viewing habits.” The letter continued, “Televisions have entered a new era, but that does not mean that users’ sensitive information no longer deserves protection. The content consumers watch is private, and it should not be assumed that customers want companies to track and use information on their viewing habits.”⁴⁶

Sens. Markey and Blumenthal provided recommendations for how smart TV companies should handle consumers’ data, including that “[a]ny entity

collecting and using sensitive information should comprehensively and concisely detail who will have access to that data, how that data will be used, and what steps will be taken to protect that information.” The letter added, “Users should be given the opportunity to affirmatively consent to the collection and use of their sensitive information, while still having access to the core functions of smart TV technology.” The senators concluded, “In light of the recent reports . . . we respectfully request that the FTC continue its efforts on smart TVs and launch an investigation into the privacy policies and practices of smart TV manufacturers.”⁴⁷

Maheshwari noted that Samba TV is not the only company within the smart TV industry to use controversial practices. On Feb. 6, 2017, smart TV manufacturer Vizio Inc., which owns its own data arm, Inscope, agreed to pay \$2.2 million to settle a case with the FTC and the New Jersey Attorney General’s Office.⁴⁸ In its February 2014 complaint, the FTC stated that Vizio’s smart TVs had a “Smart Interactivity” feature, which “enables program offers and suggestions.”⁴⁹ The FTC, however, contended that the company failed to inform consumers that the feature enabled the collection of their viewing data.⁵⁰

In December 2017, *The New York Times* reported that a start-up called Alphonso, another competitor of Samba TV that collects TV-viewing data for advertisers, had used gaming apps to gain access to smartphone microphones and listen for audio signals in TV ads and shows.⁵¹ The article stated that “these apps, once downloaded onto a smartphone, have the ability to keep tabs on the viewing habits of their users — some of whom may be children — even when the games aren’t being played.”⁵²

B. “SMART” CITIES

“Smart” cities have also raised security and privacy concerns. On Aug. 8, 2018, *The WorldPost*, a partnership between the Berggruen Institute and *The Washington Post*, reported that in October 2017, a Google-affiliated company called Sidewalk Labs (Sidewalk) announced its plans to build “the world’s first neighborhood ‘from the Internet up’ on 12 acres of the Toronto waterfront.”⁵³ The company’s stated goal was to “make urban life more streamlined, economical and green by infusing cities with sensors and

data analytics.” Sidewalk also planned, for example, to “build an ‘advanced microgrid’ to power electric cars, design ‘mixed-use’ spaces to bring down housing costs, employ ‘sensor-enabled waste separation’ to aid recycling and use data to improve public services.”⁵⁴

The WorldPost noted that technological innovation had already “far outpaced lawmakers’ ability to establish the rules of the road” including related to the IoT. “Smart” cities, however, take privacy and security concerns a step further.⁵⁵ The commentary read, “[S]o far, the virtual world has been something we opt into — giving up various rights in the terms of service agreements we hastily click closed — and can opt out of if we so choose. It’s one thing to willingly install Alexa in your home. It’s another when publicly owned infrastructure — streets, bridges, parks and plazas — is Alexa, so to speak. There’s no opting out of public space, or government services.” The commentary added, “Who will own the data streaming from sensors in every park bench, lamppost and dumpster in Quayside? No one at Sidewalk Labs, nor in local government, has given a straight answer to that question yet.”⁵⁶

In an Aug. 3, 2018, *Information Age* commentary, editor Nick Ismail contended that smart cities will present new “responsibilities to ensure critical components have the right failsafes, recovery and continuity plans so that specific components within a future smart city do not go down, affecting thousands of people at a time.”⁵⁷ Ismail cited a 2018 study by ISACA, a business technology professional association, which found that “only 15 [percent] of respondents consider cities to be most equipped to contend with smart infrastructure cyberattacks.”⁵⁸

C. MEDICAL DEVICES

In 2018, medical devices, or the Internet of Medical Things (IoMT), also continued to raise significant privacy and security concerns.⁵⁹ In a June 5, 2018, commentary, Seth Fortin, an associate in Seyfarth Shaw LLP’s Litigation Department, wrote that IoMT devices pose several security risks, including vulnerabilities in implanted devices — pacemakers, defibrillators, neurostimulators, and insulin pumps — which “pose the most obvious risk to patient safety.”⁶⁰ He argued that hackers may be able to “directly subvert the functions of the device[s].”⁶¹

Fortin, however, also wrote that there are less obvious risks associated with the IoMT, including that a hacker may steal “identities or credentials, especially as implanted devices that effectively act as personal identifiers become more common.” He added that in the near future, “it may even be possible to derive locational and activity data from implanted devices, just as it is presently possible to do so with wearable devices like fitness trackers.”⁶² A July 3, 2018 *Net News Ledger* commentary noted that cyberattacks are not the only potential risks to IoMT devices, but also accidents, natural disasters, device malfunctions, and disruptions of networks.⁶³

A Feb. 1, 2018 commentary by CSO, which provides “security decision-makers and users with the critical information [regarding] . . . criminal cyberattacks,” contended that IoMT devices are particularly vulnerable to security issues because they are “not designed with security in mind — either for the devices or the data they collect.”⁶⁴ The commentary further contended that “due to the critical nature of how they are used, IoMT devices can be difficult to patch and perform maintenance on.” The commentary explained that “[i]f a medical device is performing a life-saving function, there can be no downtime for IT teams to update the firmware or implement software patches, if those things are even possible. This means that IoMT devices often continue to operate with known vulnerabilities that can be exploited by cybercriminals as an entry point to the network.”

A Jan. 26, 2018 commentary by *Healthcare Business Today* provided additional reasons IoMT devices are particularly vulnerable to cyberattacks and other vulnerabilities, including that they “don’t always have simplified mechanisms to distribute or receive security-related updates and patches when a new vulnerability is discovered” and that they “are often programmed to access private and sensitive information stored on hospital networks. Unsecured endpoints and applications can act as an easy entry-way into the broader network when compromised.”⁶⁵ Additionally, the commentary noted that device manufacturers, unlike healthcare providers, “are not typically bound by [Health Insurance Portability and Accountability Act (HIPAA)] regulations that require features to secure the protected healthcare information (PHI) of patients.”⁶⁶

The CSO commentary therefore concluded that healthcare institutions “must focus on threat detection

as much as they do threat prevention” because cyberattacks of IoMT devices “are increasingly frequent and sophisticated.”⁶⁷ One proposed solution to IoMT vulnerabilities is network segmentation, meaning that when a threat is detected within a network, it is isolated to a single location, protecting other parts of the network.⁶⁸

Others suggest continued development of artificial intelligence (AI) and automation as a possible solution to IoMT cybersecurity concerns. CSO contended that the use of “[a]utomated response[s] based on actionable intelligence can minimize the interval between the detonation of malware and its mitigation — thereby successfully stopping a compromised IoMT device from accessing areas of the network where data is stored.”⁶⁹ *Healthcare Business Today* argued that “[s]ecurity needs to be able to operate at digital speeds, which means automating security responses and comprehensively applying intelligence combined with self-learning technologies so that networks can make effective and autonomous decisions.”⁷⁰

D. DOMESTIC ABUSE

In the first half of 2018, the IoT raised new security and privacy concerns after Internet-connected devices were used by abusers to target and harass their current or former partners.⁷¹ On June 23, 2018, *The New York Times* interviewed more than 30 domestic abuse survivors, their lawyers, shelter workers, and emergency responders, who described experiences in which “Internet-connected locks, speakers, thermostats, lights[,] and cameras that ha[d] been marketed as the newest conveniences [were] now also being used as a means for harassment, monitoring, revenge[,] and control.”⁷² Reporter Nellie Bowles, who wrote the article titled “Thermostats, Locks and Lights: Digital Tools of Domestic Abuse,” asserted that “[a]busers — using apps on their smartphones, which are connected to the internet-enabled devices — would remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power.” She continued, “Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse.”⁷³

According to Bowles, these experiences “were often aggravated by a lack of knowledge about how smart technology works, how much power the other

person had over the devices, how to legally deal with the behavior[,] and how to make it stop.”⁷⁴

In a July 1, 2018 opinion piece for *The Guardian*, John Naughton, a professor of the public understanding of technology at the Open University, described how abusers target their current or former partners using IoT devices.⁷⁵ “What has been less obvious until now is that it doesn’t have to be a hacker who can control ‘your’ home devices,” he wrote. “It could be a former partner, a jilted lover, a stalker, a former lodger or just someone you know who has a grievance. None of these will have to hack into your system, because they know the password — and in most cases you won’t have changed it after they left.” Naughton added, “The people who are particularly at risk are survivors of domestic abuse. . . . The perpetrators not only spy on their ex-partners, but can cause havoc with bursts of music, sudden changes in lighting or temperature and other attempts at intimidation,” citing Bowles’ article.⁷⁶

On July 6, 2018, *Gizmodo* reported that a research team at University College London had published a resource list for victims of such instances of domestic abuse.⁷⁷ The university’s Gender and Internet of Things (G-IoT) team, together with the London Violence Against Women and Girls (VAWG) Consortium, Privacy International, and the PETRAS IoT Research Hub, published the six-page document, which provided resources for “Internet of Things-Specific Advice.” One such resource was the blog “Technology Safety” managed by the National Network to End Domestic Violence (NNEDV), which “published dedicated information to assist in a better understanding of IoT in domestic violence cases.”⁷⁸ Another resource was Access Now, a digital rights non-profit with a 24/7 digital security hotline. The document also provided several resources concerning digital security for women and for children.⁷⁹

Accompanying the resource list was a guide describing “[h]ow internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse.”⁸⁰ The guide also outlined common IoT devices and their functionalities.⁸¹ *Gizmodo* wrote that the guide and resource list “[are] a crucial toolkit for those aiming to reestablish freedom from abusive partners, and the material included proves that a major step toward that liberation is digital literacy and secure and trustworthy support online.”⁸²

In a July 11, 2018 commentary for the “Malwarebytes Labs” blog, former director of research

at FaceTime Security Labs Christopher Boyd provided several potential ways in which domestic abuse survivors, experts, advocates, and others can “at least gain a foothold against domestic attackers.”⁸³ First, Boyd recommended that survivors “keep a record” of when the abuser targets them using IoT devices. “If you can build up a picture of every time the heating becomes unbearable, or the lights go into overdrive, or alarms start buzzing, this is valuable data for law enforcement,” he wrote.⁸⁴

Second, Boyd pointed out that IoT devices often “keep detailed statistics of use,” which survivors can use as additional evidence to match with their personal records. Third, Boyd suggested that advocacy groups “pop in and see if there’s anything you could do to help pass on useful information. . . . The more we share with each other, the more we can support abused partners to overcome their situations.”⁸⁵

Finally, Boyd provided several recommendations regarding the devices themselves, including “scrubbing” existing devices and changing passwords. Boyd also suggested that because “it’s impossible to say for sure that everything has been technologically exorcised,” individuals should consider “trash[ing] all pieces of tech” in the case of potential abuse.⁸⁶

In a July 2, 2018 *Engadget* article, senior editor Nicole Lee also provided some potential solutions, including that survivors can reset their IoT devices to factory settings, especially for devices that are “difficult to remove[,] like a connected doorbell or a smart thermostat.”⁸⁷ Ruth Patrick, the CEO of WomenSV, a Silicon Valley domestic violence program, told Lee that survivors should go “as low tech as possible,” such as “using a pad and paper to take notes, getting a flip phone instead of a smartphone[,] and checking their belongings for trackers like RFID tags and Bluetooth fobs.”⁸⁸

Lee, however, wrote that there is not an easy solution for domestic abuse through the IoT.⁸⁹ “On the surface, this seems like a relatively straightforward problem to solve: Just change your password or unplug the devices, right? Except the issue here is two-fold. Not only are the devices sometimes solely controlled by the abuser, but oftentimes making these changes will result in even worse abuse, especially if the couple is still living together,” she wrote. “Asking these victims to stop using the devices is like telling them to just leave their abuser; these situations are usually much more complex, and the victims could be putting their lives in danger by doing either.”⁹⁰

Boyd wrote that the problem is “a tough nut to crack” and there is “no quick fix” because “a lot of security pros are only just starting to understand this type of digitized assault, as well as the best ways to go about combatting it.” Thus, he argued that “we all need to up our game in technology circles and see what we can do to take this IoT-enabled horror show out of action before it spirals out of control.” He added, “As IoT continues to integrate itself into people’s day-to-day existence, in ways that can’t easily be ripped out afterwards, the potential for massive harm to the most vulnerable members of society is staring us in the face. We absolutely must rise to the challenge.”⁹¹

III. U.S. GOVERNMENT REGULATION OF THE INTERNET OF THINGS

Amidst the growing privacy and security concerns related to the IoT, the federal government, including the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), the National Institute of Standards and Technology (NIST), and the U.S. House of Representatives, took different actions regarding regulation and research of IoT devices.⁹²

A. FEDERAL TRADE COMMISSION

On June 15, 2018, the FTC’s Bureau of Consumer Protection (BCP) filed comments⁹³ with the U.S. Consumer Product Safety Commission (CPSC), which had published a notice of public hearing and request for written comments (notice) in the Federal Register regarding potential “Consumer Product Hazards” of IoT devices.⁹⁴ Observers noted that the FTC’s comments, which called on IoT companies to take reasonable steps to protect privacy, security, and safety of IoT devices, were consistent with the agency’s past approaches to privacy and security more generally.

In 2013, the FTC held a workshop, titled “The Internet of Things: Privacy and Security in a Connected World,” during which panelists from the federal government, industry, and consumer groups discussed several issues related to IoT.⁹⁵ In January 2015, the FTC filed a report based on the discussions at the workshop, detailing both the benefits and risks

of the IoT.⁹⁶ The FTC called the IoT a “priority” and provided several best practices for businesses to protect consumers’ privacy and security.⁹⁷

Since the publication of the report, the FTC has taken several actions related to the IoT. In January 2017, the agency launched a contest “seeking tools to help consumers protect the security of their [IoT] devices.”⁹⁸ In 2016 and 2017, the FTC 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.⁹⁹

On March 27, 2018, the CPSC published a notice of public hearing and request for written comments (notice) regarding the IoT and “Consumer Product Hazards.”¹⁰⁰ The notice first announced that the CPSC was holding a public hearing on May 16, 2018, in order to “receive information from all interested parties about potential safety issues and hazards associated with internet-connected consumer products. The information received from the public hearing will be used to inform future Commission risk management work.”¹⁰¹

Second, the notice discussed why the hearing was necessary, including that although the IoT “holds the promise of many benefits to consumers[,] . . . internet connectivity is also capable of introducing a potential for harm (a hazard) where none existed before the connection was established.” The CPSC primarily focused on hazards including “[f]ire, burn, shock, tripping or falling, laceration, contusion, and chemical exposure,” but acknowledged that there were also “personal data security and privacy concerns.”¹⁰²

Finally, the CPSC listed several questions for which it was seeking comment, including “How can CPSC educate consumers on the proper use of IoT-connected devices?” and “Are there ways CPSC can collaborate with other federal agencies to address potential safety hazards related to IoT?”¹⁰³

On May 16, the CPSC held the public hearing, which included 13 diverse stakeholders, including from consumer and trade organizations representatives, a university professor, researchers, and others.¹⁰⁴ A May 23, 2018 “All About Advertising Law” blog post reported that the participants discussed the privacy issues related to the IoT, as well as current regulations, legal ramifications, and liability issues associated with the IoT.¹⁰⁵ The consumer activists described the hazards related to the IoT as “urgent”

and called on the CPSC to “provide a certification process for IoT devices and stronger mandatory regulations for manufacturers that incorporate software technologies into their products,” emphasizing an “industry-led approach.”¹⁰⁶

On June 15, 2018, in response to the CPSC’s notice, the BCP filed comments with the Commission.¹⁰⁷ First, the Bureau agreed with the CPSC that the IoT “offers enormous benefits to consumers — including many products that offer safety benefits,” such as medical devices that track health data in order to inform patients’ treatment.¹⁰⁸ The BCP also recognized that “IoT devices themselves are a hazard,” including the potential to cause fires, burns, shocks, chemical exposure, and other hazards.¹⁰⁹

Second, the BCP stated that although it acknowledged that the CPSC was not focused on “personal data security or privacy implications of IoT devices,” the “security risks associated with IoT devices may implicate broader safety concerns, not just privacy.”¹¹⁰ The Bureau provided the example of a criminal, who, by hacking a connected-home network, could “not only collect information about consumers who live in the house, but also could activate or deactivate home security devices, potentially causing threats to personal safety.”

The BCP further contended that the IoT causes several technology and data-related hazards, including “loss of a critical safety function, loss of connectivity, or degradation of data integrity.” The agency provided the example of a car’s braking system failing when it is infected with malware.¹¹¹ The agency also cited the Mirai botnet in 2016, which was “composed of IoT devices, such as IP cameras and routers, infected with malicious software . . . to engage in a distributed denial of service (‘DDoS’) attack of unprotected residential building management systems in Finland.”¹¹² Thus, the BCP concluded that a “company setting up a program to address security risks on its IoT device should take measures to secure that device from hackers, for both privacy *and* safety issues.”¹¹³

Third, the BCP argued that “[r]equiring IoT devices to have perfect security would deter the development of devices that provide consumers with the safety and other benefits” and acknowledged that it “does not expect perfect security.”¹¹⁴ Instead, the Bureau proposed requiring IoT companies to take “reasonable steps to secure them from unauthorized access.”¹¹⁵

Finally, the BCP specifically addressed several of the CPSC's questions, including "What is the appropriate role of government in promoting IoT safety?" The BCP stated that although its staff "does not take a position on whether or not the CPSC should implement regulations relating to IoT device hazards," it recommended that the Commission be "technology-neutral and sufficiently flexible so that [the CPSC's approach] does not become obsolete as technology changes."¹¹⁶ The agency also contended that there is "no onsize fits all" approach to securing IoT devices.

The BCP further commented that the CPSC "should . . . improve transparency and provide consumers with information to better evaluate the safety and security of their IoT products." Such an approach create "an enforcement backstop" by allowing the FTC "to use its authority . . . to take action against companies that misrepresent their security practices in their certifications."¹¹⁷

In a June 22, 2018 *National Law Review* article, Keller and Heckman LLP partner Sheila A. Millar argued that the FTC's comment was consistent with its past approach in its 2015 guidance and report.¹¹⁸ Millar also emphasized the need for government agencies to work together, including the FTC and CPSC, contending that "[because] the FTC and other agencies have years of expertise and jurisdiction over privacy and data security, it will be important for agencies to coordinate and collaborate, focusing on their respective areas of expertise. The FTC is the lead agency on information security."¹¹⁹

Wiley Rein LLP associate Kathleen E. Scott and partner Megan L. Brown agreed in a June 15, 2018 commentary.¹²⁰ "With so much activity focused on the nascent IoT market, regulators need to work to coordinate their efforts and avoid chilling innovation through unnecessary work and duplication of efforts," they wrote. Scott and Brown noted that Wiley Rein had filed comments to the CPSC on behalf of the U.S. Chamber of Commerce's Technology Engagement Center and its Institute for Legal Reform, which urged the Commission to "coordinate with other agencies — including the FTC, [National Institute of Standards and Technology (NIST),] and [National Telecommunications and Information Administration (NTIA)] — to address IoT concerns with a light-touch approach that enables innovation and creativity."¹²¹

B. FOOD AND DRUG ADMINISTRATION

On Aug. 29, 2017, the FDA announced that it had approved a firmware¹²² update for implantable cardiac pacemakers manufactured by St. Jude Medical, Inc., which was acquired by pharmaceutical company Abbott Laboratories in 2017.¹²³ The devices, which provide pacing for slow or irregular heart rhythms, had "cybersecurity vulnerabilities," creating "the risk of patient harm" if exploited.

The FDA found that the vulnerabilities potentially allowed an unauthorized user to access a patient's device using commercially available equipment. The individual could then "modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or administration of inappropriate pacing."¹²⁴

Although there were "no known reports of patient harm related to the cybersecurity vulnerabilities in the 465,000 (US) implanted devices impacted," St. Jude Medical developed a firmware update as a "corrective action (recall) for all of [the affected] devices." The update required any device attempting to communicate with the pacemaker first provide authorization.¹²⁵

The FDA stated that the growth of IoMT has meant that "[m]any medical devices — including [the] implantable cardiac pacemakers — contain configurable embedded computer systems that can be vulnerable to cybersecurity intrusions and exploits."¹²⁶ The administration continued, "As medical devices become increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates."¹²⁷ The FDA concluded by stating that it would "continue its work with manufacturers and health care delivery organizations — as well as security researchers and other government agencies — to develop and implement solutions to address cybersecurity issues throughout a device's total product lifecycle."

C. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce, also took steps

in 2018 to address security and privacy concerns related to the IoT.¹²⁸ In February 2018, an “Internet of Things (IoT) Task Group” (Task Group) created by NIST’s Interagency International Cybersecurity Standardization Working Group (Working Group) released a draft report on IoT cybersecurity standards, titled “Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)” (report).¹²⁹ The 187-page document, in order to inform IoT stakeholders about security standards of IoT devices, provided a definition of the IoT, as well as listed and described areas in which IoT technology has been applied and utilized; core areas and standards of cybersecurity; and cybersecurity objectives, risks, and threats related to IoT devices and networks.¹³⁰

The purpose of the Working Group, which was established in December 2015, was to “coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization.”¹³¹ The Working Group determined that there must be “coordinat[ion] across the U.S. government and working with the . . . private sector” in order to have effective U.S. government participation in international efforts to regulate the IoT. As a result, on April 25, 2017, the Working Group established the IoT Task Group “to determine the current state of international cybersecurity standards development for IoT,” which led to the February 2018 report.¹³²

The report stated that “IoT security and resiliency are critical” to “reap the substantial benefits and to minimize the potentially significant risks.” Second, the Task Group noted that the report’s intended audience was both the government and the public with the purpose of “inform[ing] and enabl[ing] policymakers, managers, and standards participants as they seek timely development of and use of such standards in IoT components, systems, and services.”¹³³

Third, the report acknowledged that “[t]here can be confusion around the meaning of the term ‘Internet of Things’ for a variety of reasons,” including that the technology is rapidly changing and that there are multiple stakeholders connected to the IoT. Thus, the report brought together “common elements” of several “high-level definitions and descriptions of IoT,” and concluded that the IoT consists of two fundamental concepts:

- IoT components are connected by a network providing the potential for a many-to-many relationship between components (this network capability may or may not be TCP/IP based)
- [S]ome of the IoT components have sensors and actuators that allow the components to interact with the physical world.¹³⁴

Fourth, the report described five areas in which IoT technology has been applied and utilized, including (1) connected vehicles,¹³⁵ (2) consumer IoT,¹³⁶ (3) health IoT and medical devices,¹³⁷ (4) smart buildings,¹³⁸ and (5) smart manufacturing.¹³⁹ The Task Group asserted that each area raised separate security concerns, including consumer IoT where “proper implementation of security within consumer IoT software, firmware, and hardware is often a neglected and overlooked priority.”¹⁴⁰

For example, the report stated that consumers “may not be aware of the far-reaching security vulnerabilities introduced by something as innocuous as connecting a smart LED bulb to the[ir] home network.” If consumer IoT device, however, were to become compromised, it could “be[come] a gateway into the broader network. IoT threats could spread through networks and the Internet. By infecting a device and infiltrating one network, the threat can spread to an entirely separate network just by being in wireless range of another IoT device.” Thus, the Task Group recommended that “the increased popularity and acceptance by the consumer must be weighed against the security risks inherent to every device attached to a network.”¹⁴¹

Fifth, the report described 11 cybersecurity core areas, providing several examples of relevant standards for each. One such area was “cryptographic techniques,” such as encryption, which are meant to provide confidentiality, trust-worthy data platforms, and more. Another area was network security, which provides “security requirements and guidelines on processes and methods for the secure management, operation[,] and use of information, information networks, and their inter-connections.”¹⁴²

Sixth, the report described three cybersecurity objectives related to the IoT:

- Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;

- Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and
- Availability: Ensuring timely and reliable access to and use of information.¹⁴³

The report provided risks¹⁴⁴ and threats¹⁴⁵ for each of the five IoT technology application areas, using the three objectives as a framework.

Finally, the report applied the cybersecurity core areas as possible solutions for IoT security, looking at the impacts, benefits, and limitations of each. The report also analyzed the status of cybersecurity standards worldwide, including discussing several “possible gaps,” such as network security standards that “may require updates and/or new standards will be needed to address IoT networks that have the potential for spontaneous connections.”¹⁴⁶ The report concluded that “[g]iven how the pace of IT innovation is magnitudes faster than the pace of development of supporting standards, it is critical to be forward thinking about cybersecurity needs in the future operational environment,” including the cybersecurity core areas and objectives discussed throughout the report.¹⁴⁷

D. U.S. HOUSE OF REPRESENTATIVES

In June 2018, two bills were introduced in the U.S. House of Representatives related to the IoT.¹⁴⁸ On June 7, 2018, Rep. Robert E. Latta (R-Ohio) introduced H.R. 6032, the “State of Modern Application, Research, and Trends of IoT Act” or “SMART IoT Act,” which requires the Secretary of Commerce to “conduct a study on the state of the [U.S. IoT] industry.”¹⁴⁹ On June 26, Rep. Barbara Comstock (R-Va.) introduced H.R. 6229, titled “National Institute of Standards and Technology Reauthorization Act of 2018,” which included two sections expanding IoT research conducted by the National Institute of Standards and Technology (NIST), including to address questions related to security and privacy concerns.¹⁵⁰

The SMART IoT Act requires that the Secretary of Commerce “conduct a study on the state of the internet-connected devices industry . . . in the United States” and submit a report to Congress.¹⁵¹ The bill first states that the Department of Commerce shall

“develop and conduct a survey of the internet-connected devices industry through outreach to participating entities.” The results of the survey would include a “list of the industry sectors that develop internet-connected devices” and a “list of public-private partnerships focused on promoting the adoption and use of internet-connected devices, as well as industry-based bodies, including international bodies, which have developed, or are developing, mandatory or voluntary standards for internet-connected devices.” The survey results would also include “the status of the industry-based mandatory or voluntary standards,” as well as a “description of the ways entities or industry sectors develop, use, or promote the use of internet-connected devices.”¹⁵²

Second, H.R. 6032 requires that the Department of Commerce “develop a comprehensive list of Federal agencies with jurisdiction over the entities and industry sectors” found in the survey. Additionally, the Department would need to “identify all inter-agency activities that are taking place among the Federal agencies” and describe their “jurisdiction and expertise.”¹⁵³

Finally, the bill requires the Department of Commerce’s study to “identify all regulations, guidelines, mandatory standards, voluntary standards, and other policies implemented by each of the Federal agencies . . . as well as all guidelines, mandatory standards, voluntary standards, and other policies implemented by industry-based bodies.”¹⁵⁴

Rep. Latta called H.R. 6032 “an important first step and foundation for future policy on IoT issues” during the mark-up session for the bill.¹⁵⁵ He added, “We have heard from many stakeholders working on these important issues that because IoT is increasingly becoming ubiquitous, it is very difficult to know who is doing what — both in the federal government and in the private sector. . . . A lack of collaboration and dialogue presents the problem of creating unnecessary barriers to innovation — something we cannot afford to do if we want to unleash the power of IoT in the United States.”¹⁵⁶

Latta also described several potential benefits of the bill. “At the federal level, this will help promote interagency discussions and help avoid conflicting or duplicative obligations or requirements that may slow innovation and progress,” he said. “At the industry level, this will help innovators and businesses know how entities are developing, using and promoting use of IoT solutions. It will also highlight industry-based

efforts to self-regulate and provide industry with a one-stop-shop for a compilation of industry-based standards — both ones already in effect and those currently being developed.”¹⁵⁷ Latta added, “The SMART IoT Act is a critical first step to future IoT policy efforts.”¹⁵⁸

In a May 23, 2018 commentary, Wiley Rein LLP law clerk Paul Coyle and partners Megan L. Brown and Shawn H. Chang wrote that the SMART IoT Act has “broad bipartisan support within the Subcommittee on Digital Commerce and Consumer Protection” and that “House Leadership may look to pass this bill as a refreshing bipartisan achievement.”¹⁵⁹ They also called the legislation a “thoughtful step[] toward a comprehensive federal IoT strategy that will promote the growing IoT sector.”¹⁶⁰

On June 26, 2018, Rep. Comstock introduced H.R. 6229, which authorizes the U.S. Secretary of Commerce to provide \$1,198,500,000 for the NIST for the fiscal year 2018.¹⁶¹ Additionally, the bill requires that the Department of Commerce “enhance and expand the [NIST’s] guidance and assistance to Federal agencies . . . by providing technical guidance and education and training of . . . agency staff responsible for cybersecurity, consultative services, and other assistance at such agencies.”¹⁶²

Section 4(c) of H.R. 6229 particularly applies to the IoT. It proposes “expand[ing] the fundamental and applied research carried out by [NIST] to address key questions relating [to] the measurement of privacy, security, and vulnerability of software tools and communications networks, including through . . . investment in programs to prepare the United States with strong cybersecurity and encryption technologies to apply to emerging technologies such as . . . the internet of things.”¹⁶³

Section 7 is titled “Internet of Things” and provides that the Secretary of Commerce “shall continue to conduct research with respect to and support the expanded connectivity, interoperability, and security of interconnected systems and other aspects of the internet of things” in four ways.¹⁶⁴ First, the NIST would research the “development of . . . new tools and methodologies for cybersecurity of the [IoT].” Second, the Institute would continue conducting research related to the “development of technologies to address network congestion and device interference, such as . . . internet of things protocols.” Third, the NIST would be required to “conven[e] experts in the public and private sectors to develop recommendations for

accelerating the adoption of sound interoperability standards, guidelines, and best practices for the [IoT].” Finally, the NIST would research the “development and publication of new cybersecurity tools, encryption methods, and best practices for internet of things security.”

In a statement, Rep. Comstock described why H.R. 6229 was necessary, including the portions related to the IoT. “These investments in research and development will address the growing cybersecurity threats that harm our federal agencies and infrastructure and help reduce the cyber risks that are growing more frequent by the day,” she wrote.¹⁶⁵

IV. CONCLUSION

Throughout 2017 and 2018, the federal government, including the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), the National Institute of Standards and Technology (NIST), and U.S. Congress, considered several regulatory actions related to the IoT. Although these efforts were intended to address security and privacy concerns related to IoT devices, they raised new questions regarding the regulation of “smart” technology.

First, the federal government’s actions came as private sector companies began taking their own self-regulatory actions related to the IoT¹⁶⁶ in order to address consumers’ concerns and expectations, as well as to increase trust and accountability between brands and consumers.¹⁶⁷ As some experts have pointed out, consumers, however, seem increasingly willing to trade data privacy and security for convenience,¹⁶⁸ raising questions about whether pressure from consumers to regulate the IoT even exists. If not, what is driving the federal government’s push for increased regulation? Is it for political reasons with the November 2018 midterm elections approaching? Is it potential Fourth Amendment concerns arising from the IoT, specifically government or law enforcement surveillance?

The second major question is whether new standards will conflict with international frameworks related to data privacy, including the European Union’s (EU) General Data Protection Regulation (GDPR).¹⁶⁹ The EU formally adopted the GDPR on April 27, 2016, creating new responsibilities and obligations for data controllers and processors to protect

EU citizens' personal data and expand their privacy rights.¹⁷⁰ The framework, which took effect on May 25, 2018,¹⁷¹ has a broad territorial scope, applying to U.S.-based companies, even if they do not have offices or employees in the EU.¹⁷² As a result, even if a company attempts to comply with the U.S. federal government's new regulatory measures, it may not meet the criteria of the GDPR, leading to potential fines and reputational damage for the company.¹⁷³ If the U.S. government intends to continue its sectoral approach to data privacy and security,¹⁷⁴ it will conflict with the EU's omnibus approach to privacy,¹⁷⁵ potentially raising more questions and concerns than its regulatory efforts solve.

NOTES

- 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 2018 conference held on Nov. 8–9, 2018. 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 2018, retaining the right to republish the contents elsewhere. Jeffrey P. Cunard et al., Practising L. Inst., Communications Law in the Digital Age 2018 (2018).
- Vernon Silver, *Putin's Soccer Ball for Trump Had Transmitter Chip, Logo Indicates*, Bloomberg (Jul. 25, 2018), <https://www.bloomberg.com/news/articles/2018-07-25/putin-soccer-ball-for-trump-had-transmitter-chip-logo-indicates>.
- Id.*
- Id.*
- Id.* See also Thomas Fox-Brewster, *Hacker Implants NFC Chip In His Hand To Bypass Security Scans And Exploit Android Phones*, Forbes (Apr. 27, 2015), <https://www.forbes.com/sites/thomasbrewster/2015/04/27/implant-android-attack/#331160f61d23>.
- Silver, *supra* note 2.
- Jacqueline Thomsen, *Soccer ball Putin gave Trump contains transmitter chip — but for Adidas: report*, Hill (Jul. 25, 2018), <http://thehill.com/homenews/administration/398799-soccer-ball-putin-gave-trump-contains-transmitter-chip-but-for-adidas>.
- Fed. Trade Comm'n Staff Report, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015), available at <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iorpt.pdf>; Jane E. Kirtley, *FTC Releases Report on the Internet of Things: Global Privacy and Data Protection*, in Communications Law In The Digital Age 2015, at 674 (2015).
- Id.*
- Internet of Things Investments are Expected to Grow Globally*, PRNewswire (Jul. 17, 2018), <https://up ticknews wire.com/internet-of-things-investments-are-expected-to-grow-globally/>.
- Jane E. Kirtley, *Internet of Things Continues to Raise Security and Privacy Concerns, Prompts Actions by Federal Agencies and U.S. Congress* in Communications Law in the Digital Age 2018, at §§ I.F. (2018).
- Bernard Marr, *The Internet Of Things (IOT) Will Be Massive In 2018: Here Are The 4 Predictions From IBM*, Forbes (Jan. 4, 2018), <https://www.forbes.com/sites/bernardmarr/2018/01/04/the-internet-of-things-iot-will-be-massive-in-2018-here-are-the-4-predictions-from-ibm/#3dd6082bedd3>.
- Internet of Things Investments are Expected to Grow Globally*, *supra* note 10.
- Id.*
- Press Release, Gartner, *Gartner Reveals Top Predictions for IT Organizations and Users in 2018 and Beyond* (Oct. 3, 2017), <https://www.gartner.com/newsroom/id/3811367>.
- Sooraj Shah, *IoT security spend to increase 300% by 2023 — Juniper Research*, Vinelake (Jul. 18, 2018), <https://internetofbusiness.com/security-spend-jupiter/>.
- Aaron Tan, *Global IoT security standard remains elusive*, Computer Weekly (Jun. 27, 2018), <https://www.computerweekly.com/news/252443777/Global-IoT-security-standard-remains-elusive>; Derek B. Johnson, *Why is no one raising a hand to regulate the internet of things?* FCW (Mar. 16, 2018), <https://fcw.com/articles/2018/03/16/iot-regulation-is-pab-johnson.aspx>.
- Evan Wolff et al., *Regulatory Rules Of The Road For IoT Manufacturers*, Law360 (Jul. 28, 2017), <https://www.law360.com/articles/946940/regulatory-rules-of-the-road-for-iot-manufacturers>; NTIA Communicative Upgradability and Improving Transparency Working Group, *Communicating IoT Device Security Update Capability to Improve Transparency for Consumers* (Apr. 25, 2017), https://www.ntia.doc.gov/files/ntia/publications/draft-communicating-iot-security-update_0426.pdf. See also Jane E. Kirtley, *Federal Trade Commission, National Telecommunications & Information Administration, and U.S. Senators Address "Internet of Things" Security and Privacy in Communications Law in the Digital Age 2017*, at §§ I.C. (2017); Kirtley, *supra* note 11.
- Kirtley & Memmel, *infra* note 23.
- 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.
- Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017, 12:29 PM), <https://www.cnet.com/news/wannacrywannacrypt-uwix-ransomware-everything-you-need-to-know/>.
- What Is a DDoS Attack?, Digital Attack Map, <https://www.digital-attackmap.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/distributeddenial-of-service-attack>.
- Jane Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 Minn. J.L. Sci. & Tech. 455 (2018) available at <https://scholarship.law.umn.edu/mjlst/vol19/iss2/5>.
- Sherr, *supra* note 21.
- Id.*
- What Is a DDoS Attack? *supra* note 22; see also Rouse, *supra* note 22.
- Id.*
- TV Sets Intelligence Service, HIS Markit, last accessed Jul. 23, 2018, <https://technology.ihs.com/Services/530848/tv-sets-intelligence-service>; Kirtley, *supra* note 11.
- Sapna Maheshwari, *How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight*, N.Y. Times (Jul. 5, 2018), <https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html?nytmobile=0>.
- Id.*
- Id.*
- Id.*
- Id.*
- Id.*
- Id.*
- Id.*
- Id.*

36. *Id.*
37. *Id.*
38. *Id.*
39. Karl Bode, 'Smart' TVs Remain The Poster Child For Dismal Privacy, Transparency & Security Standards, *Techdirt* (Jul. 11, 2018), <https://www.techdirt.com/articles/20180711/07314740215/smart-tvs-remain-poster-child-dismal-privacy-transparency-security-standards.shtml>.
40. Maheshwari, *supra* note 29.
41. *Id.*
42. *Id.*
43. Ryan Barrett, *Privacy: The Dark Side of the Internet of Things*, Dark Reading (Jan. 11, 2018), <https://www.darkreading.com/endpoint/privacy-the-dark-side-of-the-internet-of-things/aId-id/1330772>.
44. *Id.*
45. Letter from U.S. Sens. Edward J. Markey & Richard Blumenthal to the Honorable Joseph Simons, Fed. Trade. Comm'n Chairman (Jul. 12, 2018), available at <https://www.markey.senate.gov/imo/media/doc/FTC%20smart%20TV%20letter%20.pdf>. See also Sapna Maheshwari, Two Senators Call for Investigation of Smart TV Industry, *N.Y. Times* (Jul. 12, 2018), <https://www.nytimes.com/2018/07/12/business/media/senators-smart-tv-investigation.html>; AJ Dellinger, Some Senators Want to Know if Smart TVs Are Spying on Us, *Gizmodo* (Jul. 13, 2018), <https://gizmodo.com/some-senators-want-to-know-if-smart-tvs-are-spying-on-u-1827593298>.
46. Letter, *supra* note 45.
47. *Id.*
48. 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-settle-ftcs-television-spying-case/2017/02/06/3d4d4b16-ec8f-11e6-9662-6eedf1627882_story.html. See also Kirtley & Memmel, *supra* note 23.
49. Complaint, *FTC v. Vizio Inc.*, No. 17-CV-00758 (D.N.J. filed Feb. 6, 2017), available at https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017_02.06_complaint.pdf.
50. *Id.*
51. See Sapna Maheshwari, *That Game on Your Phone May Be Tracking What You're Watching on TV*, *N.Y. Times* (Dec. 28, 2017), <https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html>.
52. *Id.*
53. Brian Barth, *The fight against Google's smart city*, *Wash. Post* (Aug. 8, 2018), https://www.washingtonpost.com/news/theworldpost/wp/2018/08/08/sidewalk-labs/?noredirect=on&utm_term=.7915df062744.
54. *Id.*
55. *Id.*
56. *Id.*
57. Nick Ismail, *The future smart city and the impact on risk, availability, security and privacy*, *Info. Age* (Aug. 3, 2018), <https://www.information-age.com/future-smart-city-123473926/>.
58. *Id.*
59. Kirtley, *supra* note 11.
60. Seth Fortin, *The Internet of Things + Medical Devices = Liability (Part 1)*, *Future Employer Blog* (Jun. 15, 2018), <https://www.futureemployer.com/blog/2018/6/15/the-internet-of-things-medical-devices-liability-part-1>.
61. *Id.*
62. *Id.*
63. Abel Anderson, *Will IoT Open Healthcare to Even More Attacks?* *Net News Ledger* (Jul. 3, 2018), <http://www.netnewsledger.com/2018/07/03/will-iot-open-healthcare-to-even-more>.
64. Jonathan Nguyen-Duy, *Healthcare's Secret Weapon for Securing the IoMT*, *CSO* (Feb. 1, 2018), <https://www.csoonline.com/article/3252150/security/healthcare-s-secret-weapon-for-securing-the-iomt.html>.
65. Derek Manky, *How Automation and AI Improve Healthcare Cybersecurity*, *Healthcare Bus. Today* (Jan. 26, 2018), <https://www.healthcarebusinesstoday.com/how-automation-and-ai-improve-healthcare-cybersecurity/>.
66. *Id.*
67. *Id.*
68. Nguyen-Duy, *supra* note 64. See also Rajoo Nagar, *Using Internal Segmentation to Secure the IoMT*, *Fortinet* (Dec. 28, 2017), <https://www.fortinet.com/blog/industry-trends/using-internal-segmentation-to-secure-the-iomt.html>; *Network Segmentation: A Key Measure for IoT Security*, *Arctic Wolf Blog* (Mar. 21, 2018), <https://arcticwolf.com/blog/network-segmentation-a-key-measure-for-iot-security/>.
69. Nguyen-Duy, *supra* note 64.
70. Manky, *supra* note 65; Megan Williams, *IoMT cyber risk management starts with smart endpoint security*, *Tektonika* (Jul. 12, 2018), <https://www.tektonikamag.com/index.php/2018/07/12/iomt-cyber-risk-management-starts-with-smart-endpoint-security/>.
71. Kirtley, *supra* note 11.
72. Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, *N.Y. Times* (Jun. 23, 2018), <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>.
73. *Id.*
74. *Id.*
75. John Naughton, *The internet of things has opened up a new frontier of domestic abuse*, *Guardian* (Jul. 1, 2018), <https://www.theguardian.com/commentisfree/2018/jul/01/smart-home-devices-internet-of-things-domestic-abuse>.
76. *Id.*
77. Melanie Ehrenkranz, *There's a New Resource List for Domestic Abuse Victims Targeted Through the Internet of Things*, *Gizmodo* (Jul. 6, 2018), <https://gizmodo.com/theres-a-new-resource-list-for-domestic-abuse-victims-t-1827402761>.
78. Leonie Tanczer, Trupti Patel, Simon Parkin, & George Danezis, *Gender and IoT (G-IoT) Resource List*, *UCL* (Jul. 2018), <https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/g-iot-resource-list>.
79. *Id.*
80. *Id.*
81. *Id.*
82. Ehrenkranz, *supra* note 77.
83. Christopher Boyd, *IoT domestic abuse: What can we do to stop it?* *Malwarebytes Lab* (Jul. 11, 2018), <https://blog.malwarebytes.com/cybercrime/2018/07/iot-domestic-abuse-can-stop/>.
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. Nicole Lee, *For victims of smart home abuse, there's no easy out*, *Engadget* (Jul. 2, 2018), <https://www.engadget.com/2018/07/02/smart-home-abuse-no-easy-out/>.
90. *Id.*
91. *Id.*
92. See Kirtley, *supra* note 11.
93. Fed. Trade Comm'n, *Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, In the Matter of The Internet of Things and Consumer Product Hazards* (Jun. 15,

- 2018), available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf.
94. The Internet of Things and Consumer Product Hazards, U.S. Consumer Product Safety Comm'n (83 FR 13122) (Mar. 27, 2018), available at <https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards>.
 95. Jane E. Kirtley, *FTC Releases Report on the Internet of Things; Global Privacy and Data Protection*, in *Communications Law In The Digital Age 2015*, at 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>.
 96. Fed. Trade Comm'n, *Staff Report On The Internet Of Things: Privacy & Security In A Connected World*, *supra* note 95.
 97. *Id.*
 98. 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>.
 99. 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/>; 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-settle-ftcs-television-spying-case/2017/02/06/3d4d4b16-ec8f-11e6-9662-6eedf1627882_story.html; 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>; Complaint, *U.S. v. VTech No. 1:18-cv-114* (N.D. Ill. filed Jan. 8, 2018).
 100. The Internet of Things and Consumer Product Hazards, *supra* note 94; Kirtley, *supra* note 11.
 101. *Id.*
 102. *Id.*
 103. *Id.*
 104. *Public Hearing on the "Internet of Things and Consumer Product Hazards" Part 1*, CPSC (May 16, 2018), available at <https://www.cpsc.gov/Newsroom/Video/public-hearing-on-the-internet-of-things-and-consumer-product-hazards-part-1>; *Public Hearing on the "Internet of Things and Consumer Product Hazards" Part 2*, CPSC (May 16, 2018), available at <https://www.cpsc.gov/Newsroom/Video/public-hearing-on-the-internet-of-things-and-consumer-product-hazards-part-2>. See also Heather Bramble and Thomasina Poirot, *The Internet of Things, Product Safety, and Product Liability: A Risky Combination*, All About Advertising L. Blog (May 23, 2018), <https://www.allaboutadvertisinglaw.com/2018/05/the-internet-of-things-product-safety-and-product-liability-a-risky-combination.html>.
 105. *Id.*
 106. Bramble & Poirot, *supra* note 104.
 107. Fed. Trade Comm'n, *Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, In the Matter of The Internet of Things and Consumer Product Hazards* (Jun. 15, 2018), available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf.
 108. *Id.*
 109. *Id.*
 110. *Id.*
 111. *Id.*
 112. *Id.* See also Richard Chirgwin, *Finns Chilling as DDoS Knocks Out Building Control System*, Register (Nov. 9, 2016), https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/; Kirtley, *supra* note 18.
 113. *Id.* (emphasis in original).
 114. *Id.*
 115. *Id.* (emphasis in original).
 116. Fed. Trade Comm'n, *supra* note 107.
 117. *Id.*
 118. Sheila A. Millar, *FTC Staff Submits Comment to CPSC on Potential IoT Safety Hazards*, Nat'l L. Rev. (Jun. 22, 2018), <https://www.natlawreview.com/article/ftc-staff-submits-comment-to-cpsc-potential-iot-safety-hazards>. See also Fed. Trade Comm'n Staff Report, *Internet of Things: Privacy and Security in a Connected World*, *supra* note 8.
 119. Millar, *supra* note 119.
 120. Kathleen Scott & Megan L. Brown, *FTC and Chamber Weigh in on IoT at CPSC*, Wiley Rein (Jun. 15, 2018), <https://www.wileyconnect.com/home/2018/6/15/ftc-and-chamber-weigh-in-on-iot-at-cpsc>.
 121. *Id.* See also U.S. Chamber of Commerce, *Comments Of Chamber Technology Engagement Center & U.S. Chamber Institute for Legal Reform* (Jun. 15, 2018), available at <https://static1.squarespace.com/static/579264f644024387a8bacc7f1/5b241ee80e2e726797f609c9/1529093865359/Comments+of+the+U.S.+Chamber+of+Commerce.pdf>.
 122. Safety Communication, Food & Drug Admin., *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication* (Aug. 29, 2017), available at <https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm> ("'Firmware' is a specific type of software embedded in the hardware of a medical device (e.g. a component in the pacemaker).").
 123. *Id.*
 124. *Id.*
 125. *Id.*
 126. *Id.*
 127. *Id.*
 128. Kirtley, *supra* note 11.
 129. Nat'l Inst. of Standards & Tech., *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)* (2018). See also Susan Miller, *NIST maps out IoT security standards*, GCN (Feb. 15, 2018), <https://gcn.com/articles/2018/02/15/nist-iot-standards.aspx>; Johnson, *supra* note 17.
 130. Nat'l Inst. of Standards & Tech., *supra* note 131.
 131. *Id.*
 132. *Id.*
 133. *Id.*
 134. *Id.*
 135. *Id.* ("Connected vehicle (CV) technology is expected to enable vehicles, roads, and other 470 infrastructure to communicate and share vital transportation information.").
 136. *Id.* ("The consumer IoT includes all IoT applications for consumer products. In the residence, connected objects might include: thermostats, alarm systems, smoke detectors, doorbells, smart appliances (e.g., washers, dryers, refrigerators, ovens,

- televisions), door locks, door openers, and smart lightbulbs. Wearables for consumer use, such as smart wristwear and smart fabrics, as well as implants, for applications such as consumer health or identification, are also part of the consumer IoT. Smart phones are often serving as the human user interface for these components, as are smart home assistants.”).
137. *Id.* (“In the healthcare sector, health IoT gathers, transmits and analyzes data derived from sources such as electronic health records (EHR) containing personally identifiable information (PII), personal health records (PHR), patient generated health data, and other machine-generated healthcare data. Health IoT will support services like such as real-time monitoring, medication compliance, and imaging.”).
 138. *Id.* (“[S]mart building technologies . . . help its occupants work comfortably, while improving energy efficiency and achieving various sustainability goals as mandated by the government. The various technology components, as implemented, form an integrated automated environment[.]”).
 139. *Id.* (“Smart manufacturing environments will leverage enterprise-wide integration of data, technology, advanced manufacturing capabilities, and cloud and other services with new business models . . . However, strategies are still needed to comprehensively address security challenges brought about by this new industrial revolution, as these opportunities are revolutionizing attack capabilities as well.”).
 140. *Id.*
 141. *Id.*
 142. *Id.*
 143. *Id.*
 144. *Id.* (“For the purposes of this Report, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts (both inherent and residual) that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.”).
 145. *Id.* (“A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.”).
 146. *Id.*
 147. *Id.*
 148. See Kirtley, *supra* note 11.
 149. State of Modern Application, Research, and Trends of IoT Act, H.R. 6032, 115th Cong. (2018).
 150. National Institute of Standards and Technology Reauthorization Act of 2018, H.R. 6229, 115th Cong. (2018).
 151. State of Modern Application, Research, and Trends of IoT Act, *supra* note 150.
 152. *Id.*
 153. *Id.*
 154. *Id.*
 155. Kelly Hill, *Energy & Commerce Committee to consider Smart IOT Act*, RCR Wireless News (June 20, 2018), <https://www.rcrwireless.com/20180619/policy/commerce-committee-to-consider-smart-iot-act-tag6>.
 156. *Id.*
 157. *Id.*
 158. *Id.*
 159. Paul Coyle, Megan Brown, & Shawn Chang, *Kicking the Smart Tires on IoT Legislation*, Wiley Rein (May 23, 2018), <https://www.wileyconnect.com/home/2018/5/23/kicking-the-smart-tires-on-iot-legislation>.
 160. *Id.*
 161. National Institute of Standards and Technology Reauthorization Act of 2018, *supra* note 151.
 162. *Id.*
 163. *Id.*
 164. *Id.*
 165. Tim Starks, *Another committee jumps into cyber deterrence debate*, Politico (Jun. 28, 2018), <https://www.politico.com/newsletters/morning-cybersecurity/2018/06/28/another-committee-jumps-into-cyber-deterrence-debate-266706>.
 166. Kirtley & Memmel, *supra* note 23.
 167. Matthew E.S. Coleman, *Can Self-Regulation Meet Privacy Challenges of IoT?* TrustArc (Jun. 23, 2015), <https://www.trustarc.com/blog/2015/06/23/can-self-regulation-meet-privacy-challenges-iot/>.
 168. Lisa Lacy, *Why Consumers Are Increasingly Willing to Trade Privacy for Convenience*, Adweek (Mar. 12, 2018), <https://www.adweek.com/digital/why-consumers-are-increasingly-willing-to-trade-privacy-for-convenience/>; May Wong, *Pizza Over Privacy? A Paradox of the Digital Age*, Stanford Bus. (Aug. 3, 2017), <https://www.gsb.stanford.edu/insights/pizza-over-privacy-paradox-digital-age>; Hayley Tsukayama, *People care more about convenience than privacy online*, Wash. Post (Oct. 7, 2014), <https://www.washingtonpost.com/news/the-switch/wp/2014/10/07/people-care-more-about-convenience-than-privacy-online/>.
 169. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119). See also Jane E. Kirtley, *GDPR Takes Effect, Creates Implications for U.S. Companies in Communications Law in the Digital Age 2018*, at §§ VI.A. (2018).
 170. See Jane E. Kirtley, *EU Continues Implementation Process for General Data Protection Regulation in Communications Law in the Digital Age 2017*, at §§ VI.C. (2017).
 171. Danny Palmer, *What is GDPR? Everything you need to know about the new general data protection regulations*, ZDNet (May 23, 2018), <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/>.
 172. *Does GDPR Apply to You?*, Womble Carlyle (Jul. 25, 2017), <http://www.wcsr.com/Insights/Alerts/2017/July/Does-GDPR-Apply-to-You>; Aaron W. Spiceworks, *Don't ignore the compliance rule that could cost US companies millions in 2018*, Spiceworks (Apr. 25, 2017), <https://community.spiceworks.com/topic/1985896-don-t-ignore-the-compliance-rule-that-could-cost-us-companies-millions-in-2018>; Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business*, Forbes (Dec. 4, 2017), <https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/#3ee808396ff2>; GDPR for US Companies, Compliance Junction (Apr. 2018), <https://www.compliancejunction.com/gdpr-for-us-companies/>; Lorcan Malone, *How Europe's Data Privacy Regulations Will Affect U.S. Businesses*, Business.com (Feb. 14, 2018), <https://www.business.com/articles/how-gdpr-will-affect-us-businesses/>.
 173. Kirtley, *supra* note 179.
 174. 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/> (The United States takes a sectoral approach to privacy, with laws and regulations designed to address specific industries.).
 175. Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. Times (Feb. 2, 2013), <https://www.nytimes.com/2013/02/03/technology/consumer-data-protectionlaws-an-ocean-apart.html> (The EU implements blanket laws regulating privacy consistently across industries.).

Copyright of Journal of Internet Law is the property of Aspen Publishers Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.