St. John's Law Review

Volume 93
Number 3 *Volume 93, 2019, Number 3*

Article 12

Protecting Consumers in the Age of the Internet of Things

Nicole Smith

PROTECTING CONSUMERS IN THE AGE OF THE INTERNET OF THINGS

NICOLE SMITH[†]

"Wake up, baby!"[1]

Imagine waking up in the middle of the night to the sound of a stranger speaking to your baby through the baby monitor. For one Texas couple, this horror story became reality when a man hacked their internet-connected monitors to watch and stalk their child.[2] In a similarly horrifying scenario, a hacker stalked Miss Teen USA, Cassidy Wolf, for a year via her webcam.[3] The stalker had 24/7 access to her webcam and also traced the keystrokes on her keyboard to learn her passwords for various web accounts.[4] Subsequently, the hacker used private information he learned about her from those accounts to blackmail her into doing whatever he wanted.[5] Unfortunately, as the amount of technology in use increases, frightening stories like these become more common. It is not difficult to envision a scenario in which hackers can gain access to financial information, medical records, and other critical private information. In light of ever increasing technological advances, Congress must respond by enacting legislation that addresses the specific security and privacy concerns that internet-connected technology presents.

[†] Articles Editor, *St. John's Law Review*; J.D. Candidate, 2020, St. John's University School of Law. The author would like to extend her gratitutude to the members and editors of the *St. John's Law Review* for their dedication and hard work throughout the publication process. She would also like to thank her soon-to-be husband and her family for their unwavering support and encouragement.

[1] *Home, Hacked Home: The Perils of Connected Devices*, ECONOMIST (July 10, 2014), https://www.economist.com/special-report/2014/07/12/home-hacked-home.

[2] *Id.*

[3] Cassidy Wolf, *Miss Teen USA Lived Through Your Worst Hacking Nightmare—Hear Her Frightening Story*, TEEN VOGUE (Nov. 8, 2013), https://www.teenvogue.com/story/cassidy-wolf-hacking.

[4] *Id.*

[5] *Id.*

I. AN OVERVIEW OF THE INTERNET OF THINGS

A. Definition and Scope of the Internet of Things

The term Internet of Things ("IoT"), also sometimes called the Internet of Everything, was first coined in 2005 and has since been defined in many ways.[6] The Federal Trade Commission ("FTC" or the "Commission") recently defined it as any device or sensor that can "connect, communicate or transmit information with or between each other through the Internet" excluding "computers, smartphones, or tablets."[7] A contributing writer for Forbes defined it more simply as "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)."[8] Further, Merriam-Webster places a higher emphasis on the devices' connectivity with each other, defining it as "the networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet."[9]

Regardless of the precise definition, the number of IoT devices is rapidly increasing, especially among consumers.[10] In 2017, Gartner, Inc. predicted that the number of IoT devices in use would rise from 8.4 billion to 20.4 billion by 2020.[11] Furthermore, Gartner claimed that devices used by consumers—as opposed to businesses—make up 63% of total devices used.[12] Additionally, Gartner estimated that consumers

---

[6] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 5 (2015).

[7] *Id.* at 6.

[8] Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#b55789b1d091.

[9] *Internet of Things*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/Internet%20of%20Things (last visited Sept. 20, 2019).

[10] Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n, Raising the Standard: Bringing Security and Transparency to the Internet of Things? (July 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf; *see also Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, GARTNER (Feb. 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 [hereinafter *Gartner*] (finding that consumer application represented 63% of IoT applications in 2017).

[11] *Gartner*, *supra* note 10.

[12] *Id.*

and businesses would spend $2 trillion on IoT devices in 2017,[13] and it predicts that number will rise to $3 trillion in 2020.[14] These data demonstrate how much we already rely on IoT devices, and they will only become a more integral part of our lives.

B. Examples of IoT Devices

Several different categories of devices make up the IoT. Common categories include health and fitness sensors, home appliances, automobile sensors, and employee sensors.[15] Each type of sensor will be discussed in turn.

1. Health and Fitness Sensors

Consumers and health care providers use health and fitness sensors to track behavior, changes in health, and other information such as vital signs. Categories of health and fitness sensors include:

> (1) countertop devices (such as a blood-pressure monitor or weight scale); (2) wearable sensors (such as an arm or wrist band); (3) intimate contact sensors (such as a patch or electronic tattoo); (4) ingestible sensors (such as an electronic pill); and (5) implantable sensors (such as a heart or blood health monitor).[16]

Wearable sensors and implantable sensors are discussed in more detail below.

Wearable devices are "devices that can be worn or mated with human skin to continuously and closely monitor an individual's activities, without interrupting or limiting the user's motions."[17] Popular examples of these devices include the Fitbit

---

[13] *Id.*

[14] *Id.*

[15] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98 (2014) (breaking down the internet of things into several categories, including health and fitness sensors, automobile sensors, home and electricity sensors, and employee sensors).

[16] *Id.* at 98–99.

[17] Mostafa Haghi et al., *Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices*, 23 HEALTHCARE INFORMATICS RES. 4, 4–5 (2017).

and the Apple Watch.[18] Generally, users wear these devices on their wrists to track several health indicators such as footsteps, heart rate, sleeping patterns, calories burned, and more.[19] The devices can also analyze these data and provide advice to users on ways to improve their health.[20] In the past decade, wearable devices have become increasingly popular.[21] In fact, a 2016 study showed that 17% of Americans over the age of 65 and 20% of Americans under the age of 65 used wearable devices.[22]

Additionally, implantable sensors are an integral part of our health care system. One example of an important internet-connected medical device is the pacemaker.[23] The implantable pacemaker monitors and assesses the performance of a person's heart and automatically transmits that data to a doctor for review.[24] Another example is the cardioverter defibrillator, which detects abnormalities in a patient's heartbeat and automatically sends an electric shock to restart the heart if needed.[25] Like the pacemaker, the cardioverter defibrillator also stores and transmits important heart-health data for a doctor's review.[26] The importance of implantable connected devices that

---

[18] FITBIT, https://www.fitbit.com/home (last visited Sept. 20, 2019); *Apple Watch Series 4*, APPLE, https://www.apple.com/apple-watch-series-4/ (last visited Aug. 15, 2019).

[19] *Our Technology*, FITBIT, https://www.fitbit.com/technology (last visited Sept. 20, 2019); *Apple Watch Series 4 – Health & ECG*, APPLE, https://www.apple.com/apple-watch-series-4/health/ (last visited Aug. 15, 2019).

[20] *Our Technology*, *supra* note 19; *Apple Watch Series 4 – Health & ECG*, *supra* note 19.

[21] *See* Haghi et al., *supra* note 17, at 4.

[22] Bruce Japsen, *Wearable Fitness Devices Attract More Than the Young and Healthy*, FORBES (July 11, 2016), https://www.forbes.com/sites/brucejapsen/2016/07/11/wearable-fitness-devices-attract-more-than-young-healthy/#244b67e957df.

[23] Molika Ashford, *First Internet-Connected Pacemaker Successfully Implanted*, POPULAR SCI. (Aug. 11, 2009), https://www.popsci.com/scitech/article/2009-08/first-patient-implanted-pacemaker-communicates-wirelessly-her-doctor. The first internet-connected pacemaker was implanted in 2009. *Id.* The device communicates with the doctor, so the doctor will be aware of any irregularities and will be able to act quickly to remedy them. *Id.*

[24] *Id.*

[25] *Implantable Cardioverter Defibrillator*, AM. HEART ASS'N, http://www.heart.org/en/health-topics/arrhythmia/prevention--treatment-of-arrhythmia/implantable-cardioverter-defibrillator-icd (last visited Sept. 20, 2019).

[26] *Id.*

collect health data will only continue to grow.[27] As this technology becomes more commonplace, it will be crucial to protect the sensitive data that these devices collect.

2. Home Appliances

Internet-connected home appliances are also constantly expanding in number. Amazon Web Services has divided internet-connected home devices into three categories: home automation, home security and monitoring, and home networking.[28] The most popular examples of home appliance devices in use today include Amazon's Alexa, Samsung's Family Hub smart refrigerator, and the Nest Thermostat. Alexa, an example of a home automation device, assists users by answering questions, reporting the news, and playing music.[29] Most impressively, Alexa can control other appliances in the home via internet connection, such as lightbulbs.[30] Further, Samsung's smart refrigerator is also a home automation device.[31] Through an application, users can view the inside of the refrigerator on the go to take note of its contents.[32] The refrigerator can also create shopping lists and display recipes.[33] Next, the Nest Learning Thermostat is a multifaceted device that uses self-programming technology to monitor and change the temperature of the home.[34] It also acts as a home security system by sending the consumer digital alerts if it detects smoke, carbon monoxide, or extremely low temperatures that could

---

[27] Cadie Thompson, *The Future of Medicine Means Part Human, Part Computer*, CNBC (Dec. 24, 2013, 8:30 AM), https://www.cnbc.com/2013/12/23/the-future-of-medicine-means-part-human-part-computer.html (reporting that a top health technology researcher expects that in a decade "one-third of the population will have either a temporary device or another more permanent connected device in their body").

[28] *Connected Home – Internet of Things*, AMAZON WEB SERVS., https://aws.amazon.com/iot/solutions/connected-home/ (last visited Sept. 20, 2019).

[29] *See All Things Alexa: Alexa Features*, AMAZON, https://www.amazon.com/b/ref=gbpp_itr_m-2_5fb2_16067214?node=16067214011&ie=UTF8 (last visited Oct. 14, 2018).

[30] *Alexa Features: Using Multiple Devices with Alexa*, AMAZON, https://www.amazon.com/b/ref=aeg_lp_mdh_d/ref=s9_acss_bw_cg_aegflp_7c1_w?node=17934691011&pf (last visited Sept. 20, 2019).

[31] *See Family Hub*, SAMSUNG, https://www.samsung.com/us/explore/family-hub-refrigerator/connected-hub/ (last visited Sept. 20, 2019).

[32] *Id.*

[33] *Id.*

[34] *Google Nest Learning Thermostat*, GOOGLE, https://nest.com/thermostats/nest-learning-thermostat/overview/ (last visited Sept. 20, 2019).

cause pipes to burst.[35] Examples of the final category of home appliance—home networking devices—include WiFi and Cable TV boxes. These boxes can automatically send diagnostic reports to customer service and allow consumers to monitor their network connectivity through a mobile application.[36] Experts at Amazon anticipate the rate of growth of home appliances to be 18.5% annually.[37] The experts expect an increase from 433 million shipped devices in 2016 to 940 million shipped devices in 2022.[38]

3. Automobile Sensors

Two common types of automobile sensors are Event Data Recorders ("EDRs") and auto insurance telematics devices.[39] EDRs are "devices[s] installed in . . . motor vehicle[s] to record technical vehicle and occupant information for a brief period of time (seconds, not minutes) before, during[,] and after a crash."[40] EDRs collect vehicle data to identify auto safety issues and ultimately improve road safety.[41] While vehicles are not required to have EDRs, if a manufacturer voluntarily includes them, federal regulations regulate what categories of data must be collected.[42] Even though EDRs are not mandatory, the National Highway Traffic Safety Administration estimated that 96% of new vehicles have them because of the benefit they provide to motor vehicle safety.[43] Additionally, manufacturers can use the data collected after vehicle accidents to improve the safety of the cars.

---

[35] *Id.*

[36] *Connected Home – Internet of Things*, *supra* note 28.

[37] *Home of the Future: Building a Connected Home with AWS IoT*, AMAZON WEB SERVICES, https://d1.awsstatic.com/product-marketing/iot/AWS-IoT-Connected-Home-Infographic.pdf (last visited Sept. 1, 2019).

[38] *Id.*

[39] Peppet, *supra* note 15, at 104.

[40] *Event Data Recorder*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/research-data/event-data-recorder (last visited Sept. 1, 2019) ("EDRs may record (1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage/deployment status, and (5) post-crash data such as the activation of an automatic collision notification (ACN) system.").

[41] *Id.*

[42] *See* 49 C.F.R. § 563.3 (2019).

[43] Peppet, *supra* note 15, at 104.

Moreover, auto-insurance companies have begun using internet-connected telematic devices, also called usage-based insurance ("UBI"), to track how safely consumers drive.[44] The insurance companies then use the data collected to set insurance premiums for consumers.[45] The devices usually measure a number of data points such as: "miles driven; time of day; where the vehicle is driven (Global Positioning System or GPS); rapid acceleration; hard braking; hard cornering; and air bag deployment."[46] Progressive, a large auto insurance company, uses a UBI device called Snapshot to determine insurance rates based on how the customer drives.[47] They boast that this technology can save consumers an average of $130 on their insurance premiums.[48]

4. Employee Sensors

A final area of IoT devices is workplace sensors that monitor an employee's performance and activity.[49] Commonly used IoT devices in the workplace include sensors on package delivery trucks, health and wellness apps, and devices that track employee behavior.[50] Examples of the latter category include a performance monitor used by Bank of America and an activity monitor called Biovigil.[51] Bank of America used wearable sensors developed by Ben Waber, president of Sociometric Solutions, on call center employees to study why different call centers had

---

[44] Sarwant Singh, *The Future of Car Insurance: Digital, Predictive and Usage-Based*, FORBES (Feb. 24, 2017), https://www.forbes.com/sites/sarwantsingh/2017/02/24/the-future-of-car-insurance-digital-predictive-and-usage-based/#425849 3152fb.

[45] *Id.*

[46] *Usage-Based Insurance and Telematics*, NAT'L ASS'N OF INS. COMMISSIONERS, https://www.naic.org/cipr_topics/topic_usage_based_insurance.htm (last updated May 17, 2019).

[47] *Snapshot*, PROGRESSIVE, https://www.progressive.com/auto/discounts/snapshot/ (last visited Sept. 20, 2019).

[48] *Id.*

[49] Peppet, *supra* note 15, at 112.

[50] Josh Bersin et al., *Will IoT Technology Bring Us the Quantified Employee?: The Internet of Things in Human Resources*, DELOITTE (May 24, 2016), https://www2.deloitte.com/us/en/insights/focus/internet-of-things/people-analytics-iot-human-resources.html#endnote-sup-11.

[51] Vivian Giang, *Companies Are Putting Sensors on Employees To Track Their Every Move*, BUS. INSIDER (Mar. 14, 2013, 6:23 PM), https://www.businessinsider.com/tracking-employees-with-productivity-sensors-2013-3; BIOVIGIL, http://biovigil.com/ (last visited Sept. 20, 2019). It should be noted that BioVigil was originally called HyGreen.

different levels of employee productivity.[52] The devices recorded the employees' tone of voice, speaking speed, and speaking volume to determine the nature of people's conversations and stress levels.[53] Based on the study, Bank of America concluded that employees are more productive when they take breaks at the same time and, thus, have time to socialize.[54] Using this information, Bank of America changed its break schedule and increased employee productivity by 10%.[55]

Another example of connected employee monitoring devices is the BioVigil hand hygiene system used in many healthcare facilities.[56] In hospitals that use the device, health care workers wear badges that connect, via the internet, with hand-washing sensors that detect when it is time for a hospital employee to wash her hands.[57] Then, the system records the event so that the hospital can track and review its employees.[58] Any time healthcare workers should have washed their hands but did not, the badge turns red to remind employees to do so.[59] Biovigil claims that its device has led to a reduction in medical staff absenteeism by 18%.[60] More importantly, Biovigil claims that it has led to an 83% reduction in hospital-acquired infections.[61]

II. WHY REGULATION OF IOT DEVICES IS NECESSARY

The above descriptions of IoT devices demonstrate that these devices have infiltrated almost every aspect of our daily lives. And, because of the indispensable benefits they provide, it is unlikely that we will discontinue their use. In fact, it is likely that the number and potential uses of IoT devices will continue to grow. Due to the increasing prevalence of these devices in our lives, it is important to enact legislation that protects consumers from the risks associated with large amounts of data collection while still allowing for technological advancement. The more IoT

---

[52] Giang, *supra* note 51.
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] BIOVIGIL, *supra* note 51.
[57] BioVigil, *BioVigil in Action*, YOUTUBE (July 11, 2018), https://www.youtube.com/watch?v=0EhEqKuHY8Q&feature=youtu.be.
[58] BIOVIGIL, *supra* note 51.
[59] BIOVIGIL, *supra* note 57.
[60] BIOVIGIL, *supra* note 51
[61] *Id.*

devices used, the higher the risk of the misuse of data. The FTC has split the risks associated with IoT devices into two categories: security risks and privacy risks.[62]

A. Security Risks

The primary security risks to consumers identified by participants in an FTC workshop are: "(1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating [physical] safety risks."[63]

1. Unauthorized Access to Data and Attacks on Other Systems

The first two risks identified are closely aligned because they concern hackers or other unauthorized third parties that may take advantage of vulnerabilities in technology and the lack of regulation to gain access to personal data stored on IoT devices. Once accessed, hackers can then use personal data in inappropriate ways or to attack other systems and devices.[64] While these risks have been present for a long time in connection with computers and mobile phones, the impact of the risks will increase as the number of IoT devices increases.[65]

An example of an instance where hackers took advantage of the vulnerabilities in technology is *United States v. Vtech Electronics Limited*.[66] There, the FTC sued Vtech, the manufacturer of an electronic toy and corresponding application called Kid Connect, for failing to comply with the Children's Online Privacy Protection Act ("COPPA").[67] Vtech developed a program in which parents could set up an account for their child by providing the child's name, date of birth, gender, and a profile

---

[62] FED. TRADE COMM'N, *supra* note 6, at 10.

[63] *Id.*

[64] *Id.* at 11.

[65] ELEC. PRIVACY INFO. CENTER, *Comments of the Electronic Privacy Information Center to the Federal Trade Commission: On the Privacy and Security Implications of the Internet of Things*, at 16 (June 1, 2013) https://www.epic.org/apa/comments/EPIC-FTC-IoT-Cmts.pdf [hereinafter EPIC] ("[M]any of the same data security risks that currently threaten our data will only expand in the Internet of Things."); *see also* FED. TRADE COMM'N, *supra* note 6, at 11 ("[A]s consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.").

[66] Complaint at 1, United States v. Vtech Elecs. Ltd., No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018) [hereinafter Vtech Elecs.].

[67] *Id.* at 1.

picture.[68] Once registered, the children could use the chat function to communicate with each other and even send pictures and audio messages.[69] In 2015, hackers were able to acces the information of both the parents and the children even though it had been encrypted because the database included the decryption keys, so the hackers could view the data in a readable format.[70] Due to the nature of the information collected, "if a child had submitted a photo through Kid Connect, the hacker could have found the photo, along with [the] physical address" of the family.[71]

Another alarming example of hackers accessing IoT devices is *In the Matter of TRENDnet, Inc.*[72] There, the FTC sued TRENDnet, the manufacturer of Internet Protocol cameras, for violating the Federal Trade Commission Act (the "FTC Act").[73] The cameras allow consumers to monitor their homes or businesses over the internet by accessing live video and audio feeds.[74] In 2012, hackers were able to access the live feeds and obtain the IP addresses of hundreds of consumers.[75] The hackers then posted links to the live feeds of almost 700 cameras.[76] The feeds "displayed private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[77]

---

[68] *Id.* at 4.

[69] *Id.* at 5.

[70] *Id.* at 8–9.

[71] *Id.* at 9.

[72] Complaint, *In re* TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014), 2014 WL 556262. This matter was settled in 2014. *See FTC Approves Final Order Settling Charges Against TRENDnet, Inc.*, FTC (February 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc. TRENDnet is prohibited from misrepresenting the security of its products. *Id.* It was also required to improve its secuirty program and notify customers of the prior security issues. *Id.*

[73] *Id.* at 1.

[74] *Id.*

[75] *Id.* at 3.

[76] *Id.*

[77] *Id.* It is important to note that TRENDnet is not the only video camera company that has had these issues. Parents in Ohio, using a camera manufactured by Foscam, woke up to "the sound of a man shouting, 'Wake up, baby!' " from a man who was watching their child sleep. *Home, Hacked Home: The Perils of Connected Devices*, *supra* note 1. "The problem arose even though Foscam had taken all the right steps in response to the initial breach, which shows how hard it is to protect devices hooked up to the internet." *Id.*

2. Physical Safety Risks

Even more unsettling than the exposure of personal data are the risks to a consumer's physical safety. Physical safety risks manifest in two ways. First, hackers can physically threaten consumers by analyzing data from their devices to further the commission of a crime. An example of this situation would be where a hacker monitors a consumer's IoT devices to determine whether that person is home and then uses that data to commit a burglary.[78] Second, hackers can cause direct physical harm to consumers by accessing and controlling their devices—for example, where a person hacks into the telematic device of a consumer's car and takes control of the engine and brakes.[79]

One particularly disturbing possibility is a hacker accessing a person's IoT medical device to obstruct its beneficial purpose. For example, Jerome Radcliffe, a researcher, demonstrated that hackers could access insulin pumps to control the amount of insulin distributed to diabetics.[80] He explained that a hacker could cause the device to display a higher blood sugar level than actually exists, meaning that "[a] diabetic could be manipulated into administering more insulin then [sic] needed, potentially causing a hypoglycemic condition."[81] If it is possible for hackers to access insulin pumps, it is easy to imagine that it would be possible for hackers to access other medical devices, such as pacemakers.[82]

B. Privacy Risks

When the FTC conducted a workshop on the IoT, participants outlined several privacy risks associated with IoT devices. These included the "collection of sensitive personal

---

[78] EPIC, *supra* note 65, at 16–17; *see also* FED. TRADE COMM'N, *supra* note 6, at 13 ("[A] thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.").

[79] FED. TRADE COMM'N, *supra* note 6, at 12–13 ("Although the risks [of hacking into cars] currently may be small, they could be amplified as fully automated cars, and other automated physical objects, become more prevalent.").

[80] Jerome Radcliffe, *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System*, at 1, https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

[81] *Id.*

[82] Adrian Baranchuk et al., *Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?*, 71 J. AM. C. CARDIOLOGY 1284, 1284 (2018) (discussing the "relatively new threat in light of recent incidents involving the potential for hacking of cardiac devices").

information, such as precise geolocation, financial account numbers, or health information."[83] These privacy risks are further exacerbated by the fact that data collected across numerous IoT devices for a single person could facilitate the drawing of inferences about that person's behavior patterns.[84]

1. Collection of Sensitive Personal Information

The collection of sensitive personal information from smart devices could reveal "information with potential for commercial value."[85] If third parties have access to this kind of information, it "could lead to the commercialization of intimate segments of consumers' lives."[86] For example, in *FTC v. Vizio, Inc.*, the Commission sued the television manufacturer Vizio under the FTC Act for selling consumers' data to third parties without consent.[87] Vizio collected "second-by-second information about video displayed on the smart TV" and "append[ed] specific demographic information to the viewing data, such as sex, age, income, marital status, household size, education level, home ownership, and household value."[88] Vizio then sold this information to third parties for the purpose of measuring audiences, analyzing advertisement effectiveness, and targeting advertising to particular consumers.[89]

Smart TV manufacturers are not the only companies that have sold consumer data to third parties.[90] As a result, data collection could lead to a greater power imbalance between

---

[83] FED. TRADE COMM'N, *supra* note 6, at 14.

[84] EPIC, *supra* note 65, at 10 ("One of the primary risks that internet users will face as the Internet of Things expands is the fact that the ubiquitous collection and storage of data about users can reveal sensitive behavior patterns.").

[85] *Id.* at 12 ("Smart devices could reveal a wealth of information about consumers' location, media consumption, activity patterns, associations, lifestyle, age, income, gender, race and health . . . .").

[86] *Id.*

[87] Complaint at 1, FTC v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 14, 2017) [hereinafter Vizio Complaint].

[88] *FTC, 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 Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it [hereinafter Vizio].

[89] Vizio, *supra* note 88.

[90] EPIC, *supra* note 65, at 12–13 (noting that General Motors, Verizon, and Internet providers can or already have provided consumer data to third parties).

consumers and corporations.[91] The more information a company has about consumers, the more power the company has over them because they have an increased "ability to influence or direct the behavior of consumers."[92] Examples of where this might occur are insurance companies, like Progressive, that use EDRs to determine insurance premiums based on driving behavior, or rental car companies that use EDRs to "charge numerous 'gotcha fees' for driving outside of specified regions or using certain services."[93] As a result, companies that provide important services leave consumers "relatively disempowered and without meaningful choice."[94] For many important services, such as phone service, consumers can choose from only a limited number of companies, which provide long, form contracts that are dictated by the companies.[95] If consumers do not have a meaningful choice to choose a service provider, they are essentially forced to agree to the terms of a contract without the ability to protect themselves from unwanted data collection.

2. Behavioral Pattern Inferences

The immense volume of data collected across various IoT devices allows those with access to that data to analyze it and make inferences.[96] One participant in the IoT workshop noted that one data point is generated every six seconds in households that use his company's product, or 150 million data points daily for 10,000 consumers collectively.[97] These data points can contain sensitive personal information, such as "precise geolocation, financial account numbers, or health information."[98] However, the data points can also include "personal information, habits, locations, and physical conditions over time."[99] Then,

---

[91] *Id.* at 13.

[92] *Id.* at 14 ("Information is power, and smart devices will provide much more information about consumers' behavior to companies than has been traditionally available.").

[93] *Id.* at 15.

[94] *Id.* at 13; *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 51 (2012) ("[A] 'take it or leave it' approach is problematic from a privacy perspective, in markets for important services where consumers have few options.").

[95] EPIC, *supra* note 65, at 13.

[96] FED. TRADE COMM'N, *supra* note 6, at 15.

[97] *Id.* at 14.

[98] *Id.*

[99] *Id.*

these data points can be "used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; [and] overall well-being."[100] These inferences could be used to "make credit, insurance, and employment decisions."[101]

An example of a device that could facilitate this amount of data collection is the Smart Grid. The United States is currently moving towards switching over utilities to a smart grid system.[102] A smart grid "will be capable of monitoring everything from power plants to customer preferences to individual appliances."[103] This technology has many indispensable benefits for the economy, such as integrating alternative energy sources like solar and wind power, enabling electric vehicles, allowing for large-sale storage, and enabling the use of green buildings.[104] At the same time, this technology creates serious privacy risks because "[i]nformation about a power consumer's schedule can reveal intimate, personal details about their lives, such as their medical needs, interaction with others, and personal habits."[105] In order for such important technology to be successfully integrated into our economy, we must first enact legislation to protect the public from misuses of data.

III. CURRENT LEGISLATION AVAILABLE

Despite the growing privacy and security risks associated with the IoT, there are currently no IoT-specific regulations on the federal level. In fact, in 2013, the FTC conducted a workshop where they stated that such legislation was not necessary at the time.[106] Since then, California has enacted two important pieces

---

[100] *Id.* at 15.

[101] *Id.*

[102] U.S. DEP'T OF ENERGY, THE SMART GRID: AN INTRODUCTION 2.

[103] *Id.* at 13.

[104] *Id.* at 15.

[105] EPIC, *supra* note 65, at 11; *see also* ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 04/2013 ON THE DATA PROTECTION IMPACT ASSESSMENT TEMPLATE FOR SMART GRID AND SMART METERING SYSTEMS ('DPIA TEMPLATE') PREPARED BY EXPERT GROUP 2 OF THE COMMISSION'S SMART GRID TASK FORCE 5 (2013) [hereinafter DPIA TEMPLATE] (explaining that "[f]rom . . . the smart meters, a lot of information can be inferred regarding the consumers' use of specific goods or devices, daily routines, living arrangements, activities, lifestyles and behaviour," thus creating risks of "price discrimination, profiling for behavioural advertisement, taxation, law enforcement access, [and] household security").

[106] FED. TRADE COMM'N, *supra* note 6, at 2–3, 48.

of legislation that "represent a dramatic expansion of data privacy law that will impact the products and processes of many companies."[107] While the new California laws are not perfect to fix all the issues with data privacy, they are a good starting point that Congress should use as a model to enact federal level IoT legislation.

A. FTC Recommendation

After conducting a workshop on the IoT in 2013, the FTC published its recommendation on how to improve IoT security in 2015.[108] At the workshop, the FTC consulted the advice and opinions of many participants who noted the various security and privacy risks associated with the IoT.

1. Description of the Provisions

Most notably, the FTC noted that the "[s]taff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time."[109] The Commission reasoned that "legislation aimed specifically at the IoT at this stage would be premature" because of the "great potential for innovation."[110] Instead, the Commission recommended that companies take a self-regulatory approach and adopt best practices concerning "data security, data minimization, and notice and choice."[111] Additionally, the Commission urged Congress to "enact strong, flexible, and *technology-neutral* legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach."[112]

In the meantime, the Commission stated that it will rely on existing laws to hold IoT companies liable for any harm to consumers.[113] These laws include the FTC Act, the Fair Credit

---

[107] *New California Security of Connected Devices Law and CCPA Amendments*, GIBSON DUNN (Oct. 5, 2018), https://www.gibsondunn.com/new-california-security-of-connected-devices-law-and-ccpa-amendments/. In 2018, California passed the California Consumer Privacy Act and a new law that specifically regulates internet connected devices. *Id.* Both laws went into effect on January 1, 2020. *Id.*

[108] *See* FED. TRADE COMM'N, *supra* note 6, at 48–53.

[109] *Id.* at 48.

[110] *Id.* at 49.

[111] *Id.* at 27.

[112] *Id.* at 49 (emphasis added).

[113] *Id.* at 53.

Reporting Act ("FCRA"), COPPA, and "the health breach notification provisions" of the Health Information Technology for Economic Clinical Health Act ("HI-TECH Act").[114] The Commission also stated that it will educate consumers and businesses on how to protect themselves, work with groups to consider "guidelines related to the Internet of Things," and advocate for courts and other agencies to "promote protections in this area."[115]

2. Issues with the FTC Recommendation

Even though the FTC determined in 2015 that enacting IoT-specific legislation was too premature—given the growing number IoT devices and the growing number of data breaches and harms to consumers—it is no longer premature to enact this kind of legislation. In 2018, the Identity Theft Resource Center published a study showing that the total number of data breaches has doubled since 2015.[116] The main problem with the FTC's recommendation for IoT security is that the existing laws that it plans to rely on protect consumers only to a limited extent.[117] An IoT specific law is needed to address the gaps in the FTC Act, FCRA, COPPA, and the HI-TECH Act.

a. FTC Act

Specifically, the FTC recommends relying on § 5 of the FTC Act for "[u]nfair methods of competition."[118] This section declares that the "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce" are unlawful.[119] Additionally, the Act only permits the FTC to bring an action against "persons, partnerships, or corporations" that are in violation of the Act.[120] Private citizens have no right to bring a claim, meaning that consumers must

---

[114] *Id.*

[115] *Id.*

[116] *See ITRC Data Breach Overview 2005 to 2017*, IDENTITY THEFT RESOURCE CTR. (2018), https://www.idtheftcenter.org/images/breach/Overview20052017.pdf (showing that the number of data breaches in 2015 was 780, while the number of data breaches in 2017 was 1,579).

[117] FED. TRADE COMM'N, *supra* note 6, at 53.

[118] 15 U.S.C. § 45(a)(1) (2018).

[119] *Id.*

[120] *Id.* § (a)(2).

rely on the "FTC's willingness to act."[121] The primary issue with relying on the FTC Act for IoT-related security issues is that it does not afford consumers a private right of action. Furthermore, it fails to protect consumers against situations in which a party did not act unfairly or deceptively, yet the consumer is still injured. For example, if a manufacturer is merely negligent in its privacy protocols and a consumer is injured, the consumer would not have a private right of action against the manufacturer.

It may be argued that while there is not a private right of action in the FTC Act, every state has enacted its own Unfair and Deceptive Acts and Practices statute ("UDAP") which provides consumers with a private right of action.[122] While this is true, these statutes vary widely in terms of their strength.[123] For example, a few states have civil penalty maximums of $1,000, while others have civil penalty maximums as high as $50,000.[124] Furthermore, states vary in the scope of their coverage.[125] While some states offer strong protections for credit and insurance issues, other states provide relatively weak protections.[126] Given the fact that IoT-related privacy and security risks tend to span across states, it would be more efficient if consumers could bring claims in federal court, under a uniform law where they could receive similar remedies for similar injuries.

b. FCRA

Even though the FTC has yet to bring an IoT claim under the FCRA, the Commission still recommends its use to protect against IoT security and privacy risks. However, the FCRA is insufficient for this purpose because it is limited in scope and would apply to few IoT-related cases. The purpose of the FCRA

---

[121] *Id.*; *see also* Marshall A. Leaffer & Michael H. Lipson, *Consumer Actions Against Unfair or Deceptive Acts or Practices: The Private Uses of Federal Trade Commission Jurisprudence*, 48 GEO. WASH. L. REV. 521, 523 (1980).

[122] *Unfair & Deceptive Acts & Practices*, NAT'L CONSUMER L. CTR., https://www.nclc.org/issues/unfair-a-deceptive-acts-a-practices.html (last visited Sept. 21, 2019).

[123] CAROLYN CARTER, NAT'L CONSUMER LAW CTR., CONSUMER PROTECTION IN THE STATES: A 50-STATE EVALUATION OF UNFAIR AND DECEPTIVE PRACTICES LAWS 9 (2018).

[124] *Id.* at 2.

[125] *See id.* at 5–8.

[126] *Id.* at 5 (showing that Alabama offers strong credit and insurance protections and that Arizona offers weak credit and insurance protections).

is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable."[127] One application of this Act is to "third-party consumer reports used for credit or employment purposes."[128] Generally, this Act does not apply to the parties that first collect the data.[129] In other words, the Act would not "cover IoT device manufacturers that do their own in-house analytics" or "companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions."[130] For example, car insurance companies, like Progressive, could use UBI devices to collect data about consumers, and use that data to make insurance decisions without risk of violating FCRA.[131]

c. COPPA

COPPA is similar to the FTC Act in that it "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet."[132] Some notable differences are that COPPA applies only to children under the age of thirteen[133] and states that any collection of a child's personal information requires parental consent.[134] The most important difference is that COPPA requires companies that collect personal information from children to "maintain reasonable procedures to protect the confidentiality, security, and integrity" of the information.[135]

For example, in the *Vtech* case, the Commission used COPPA to hold a toy manufacturer liable when hackers were able to access children's information.[136] One of the counts of the

---

[127] 15 U.S.C. § 1681(b) (2018).

[128] Katherine Britton, *IoT Big Data: Consumer Wearables, Data Privacy and Security*, AM. B. ASS'N. (Nov. 1, 2015), https://www.americanbar.org/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/.

[129] *Id.*

[130] *Id.*

[131] *Snapshot*, *supra* note 47.

[132] FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2013).

[133] § 312.2.

[134] § 312.5(a).

[135] § 312.8.

[136] *See* Vtech Elecs., *supra* note 66, at 1–2, 9–10.

complaint alleged that the company violated the Act because of its failure to maintain reasonable security measures to protect the children's information.[137] While COPPA is limited because it only applies to information of children under the age of thirteen, a provision requiring reasonable security measures for people of all ages would better help to protect consumers than the currently available federal laws.

d. HI-TECH Act

Finally, the FTC recommends reliance on the health breach notification portion of the HI-TECH Act. This section of the HI-TECH Act provides that entities that keep consumers' health information should "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result" of breach of such information.[138] Data breach notification laws of this kind generally serve two purposes: to "recognize that an individual has a 'right to know' about unauthorized misuse of his or her personal information and notice of the incident enables mitigation of subsequent identity theft"; and to "encourage organizations to adopt better security practices" because of the negative reputational effects of reporting a data breach.[139] While this law is helpful in encouraging companies to increase security measures, it is not enough to remedy IoT security issues because it is primarily a retroactive provision that does not actually prevent data breaches in the first place.[140] Furthermore, it only applies to health data, so it does not provide a remedy for another kind of data breach.

---

[137] *Id.* at 10.

[138] 42 U.S.C. § 17932(a) (2018).

[139] Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 78–79 (2011).

[140] *Id.* at 126 ("[Data breach notification] laws should not be viewed as a 'be all end all' solution to problems relating to the inadequate protection of personal information by corporations. Data breach notification laws are extremely useful at highlighting problems but that does not mean they necessarily have the regulatory tools to remedy the problems that they uncover.").

B. California Consumer Privacy Act and Connected Devices Bill

The California Consumer Privacy Act ("CCPA") was approved by the Governor on June 28, 2018, and went into effect on January 1, 2020.[141] The bill was passed in part as a response to the Cambridge Analytica scandal in which millions of people's personal information was misused.[142] The scandal, along with the increase in personal consumer data,[143] caused the California legislature to realize that it has "not kept pace with" the developments in the collection of personal information.[144] The aim of the bill is to further the right to privacy by "giving consumers an effective way to control their personal information."[145] While the CCPA and the Connected Devices Act, discussed below, are not perfect, they are a model that Congress could look to in crafting specific IoT regulations.

1. Provisions of the CCPA

The CCPA grants consumers the following rights: (1) "to know what personal information is being collected"; (2) "to know whether their personal information is sold or disclosed and to whom"; (3) "to say no to the sale of personal information"; (4) "to access their personal information"; and (5) "to equal service and price, even if they exercise their privacy rights" under this Act.[146] The CCPA defines personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[147] It applies to any business that meets one of the following characteristics: (1) "[h]as annual gross revenues in excess of twenty-five million dollars"; (2) receives "the personal information of 50,000 or more consumers"; or (3) "[d]erives 50 percent or more of its annual

---

[141] Assemb. B. 375, Ch. 55, 2017–18 Reg. Sess. (Cal. 2018).

[142] § 2(g).

[143] § 2(c) ("It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information.").

[144] § 2(d). "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals . . . ." § 2(f).

[145] § 2(i).

[146] *Id.*

[147] CAL. CIV. CODE § 1798.140(o)(1) (West, Westlaw current through urgency legis. through Ch. 40 of the 2019 Reg. Sess.) (effective Jan. 1, 2020).

revenues from selling" personal information.[148] Additionally, the CCPA does not apply to "personal information if every aspect of that commercial conduct takes place wholly outside of California."[149]

For the most part, the CCPA does not provide a private right of action. Instead, most violations can be pursued only by the attorney general.[150] However, there is one exception where a consumer has a "private right of action in connection with . . . a consumer's nonencrypted or nonredacted personal information."[151] Notably, the law does not restrict businesses in regard to "information that is deidentified or in the aggregate consumer information."[152]

2. Provisions of the Connected Devices Act

On September 28, 2018, the California Governor approved of the Connected Devices Act that took effect on January 1, 2020.[153] The Connected Devices Act goes one step further than the CCPA and provides that a manufacturer of a device that connects to the internet should be equipped "with a reasonable security feature" that protects "any information contained therein from unauthorized access, destruction, use, modification, or disclosure."[154] Similar to the CCPA, this law does not provide consumers with a private right of action.[155] Notably, the bill does

---

[148] *Id.* § 1798.140(c)(1)(A)–(C); *see also* Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)* 2, (Santa Clara Univ. Legal Studies Research Paper, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 ("The IAPP conservatively estimated that over a half-million businesses are regulated by the law, 'the vast majority of which are small- to medium-sized enterprises.' ").

[149] CAL. CIV. CODE § 1798.145(a)(6) (effective Jan. 1, 2020) ("[C]ommercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.").

[150] Assemb. B. 375, Ch. 55, 2017–18 Reg. Sess. (Cal. 2018).

[151] *Id.*

[152] CAL. CIV. CODE § 1798.145(a)(5). " 'Deidentified' means information that cannot reasonably identify . . . a particular consumer . . . ." § 1798.140(h). " 'Aggregate consumer information' means information that relates to a group or category of consumers, from which individual consumer identities have been removed . . . ." § 1798.140(a).

[153] S.B. 327, Ch. 886, 2017–18 Reg. Sess. (Cal. 2018).

[154] CAL. CIV. CODE § 1798.91.04(a)(3) (West, Westlaw current with urgency legis. through Ch. 40 of the 2019 Reg. Sess.) (effective Jan. 1, 2020).

[155] § 1798.91.06(e).

not provide a specific definition for "reasonable" security measures. However, the Connected Devices Act does specify that the reasonable security provision will be met "if a connected device is equipped with a means for authentication outside a local area network . . . if either of the following requirements are met: (1) The preprogrammed password is unique to each device manufactured"; or "(2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time."[156]

3. Issues with CCPA and the Connected Devices Act

Taken together, the CCPA and the Connected Devices Act take important steps to further the protection of consumers against the security and privacy risks associated with the IoT. In crafting a federal-level statute, these acts could be models for Congress with regard to the reasonable security feature provision, and in some reliance on notice and consent. However, there are three main issues with these California statutes that should be addressed: (1) the CCPA does not apply to de-identified data; (2) the CCPA places too much emphasis on the role of the consumer and on notice and consent by the manufacturer; and (3) neither the CCPA nor the Connected Devices Act provides a private right of action for the consumer.

a. De-identification

The CCPA expressly does not extend to information that has been de-identified.[157] De-identified data refer to data in which "all explicit identifiers" have been removed, "such as name, address, and phone number," so that the data collected cannot be identified and attributed to a specific person.[158] The issue with excluding de-identified data from protection is that the excluded data are fairly easy to re-identify with only a few specific data points.[159]

---

[156] § 1798.91.04(b).

[157] § 1798.145(a)(5).

[158] Latayna Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000), https://dataprivacylab.org/projects/identifiability/paper1.pdf.

[159] *Id.*; *see also* Peppet, *supra* note 15, at 129.

Numerous studies have emerged showing how easily data can be re-identified. For example, in an important study by Latayna Sweeney in 2000, Sweeney discovered that 87% of the United States population could be identified by zip code, gender, and birth date alone.[160] Sweeney was even able to track down the Massachusetts Governor's hospital records with these data points and mailed them to him as proof of her theory.[161] Furthermore, in 2006, AOL released the internet search histories of 657,000 Americans after removing identifying information.[162] However, it was quickly realized that individuals could be re-identified.[163] Bloggers were able to track down, among others, Thelma Arnold of Georgia based on her internet searches for landscapers, dog training tips, single men, and other queries.[164] Similar to the AOL scandal, in 2006 Netflix "released one hundred million records revealing how nearly a half-million of its users had rated movies" as part of a contest.[165] Arvind Narayanan and Vitaly Shmatikov used this Netflix data to show how easy it is to re-identify data.[166] They were able to show that 64% of users could be re-identified by knowing two of their movie ratings and the dates that they were rated.[167]

b. Notice and Consent

The CCPA's reliance on notice and consent is too heavy because it requires the consumer to learn about the privacy policies of the manufacturer and then take action if the policies are unsatisfactory.[168] Notice and consent provisions can be important because they give consumers the opportunity to make informed decisions, particularly in situations concerning

---

[160] Sweeney, *supra* note 158.

[161] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1719–20 (2010).

[162] Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol.html; *see also* Ohm, *supra* note 161, at 1717 (explaining that AOL "suppressed any obviously identifying information such as AOL username and IP address" and "replaced these identifiers with unique identification numbers").

[163] Barbaro & Zeller, Jr., *supra* note 162.

[164] *Id.*

[165] Ohm, *supra* note 161, at 1720.

[166] ARVIND NARAYANAN & VITALY SHMATIKOV, THE UNIV. OF TEX. AT AUSTIN, HOW TO BREAK ANONYMITY OF THE NETFLIX PRIZE DATASET 1 (2018).

[167] *Id.* at 2.

[168] It should be noted that the FTC report also suggests that the companies should rely on notice and consent. FED. TRADE COMM'N, *supra* note 6, at 39.

sensitive information.[169] But, while these provisions are a necessary component of consumer protection, they alone are not sufficient because they place too much emphasis on the actions of consumers rather than focus on preventing data breaches in the first place.

A major problem with notice and consent provisions is that a majority of consumers do not read them. In one study, researchers set up a fake social media website and participants were asked to register an account.[170] In the process, participants were asked to agree to the terms and conditions.[171] Researchers measured the amount of time users spent reading the policy and included two "gotcha clauses" to determine whether the participants actually read the policy.[172] The first "gotcha clause" stated that the company website could transfer any information to third-parties.[173] The second "gotcha clause" stated that "by agreeing . . . participants would give up their first-born child."[174] The results showed that 96% of participants spent less than five minutes reading the policy, even though it was estimated to take half an hour.[175] Additionally, 93% of participants agreed to the "gotcha clauses," allowing the transfer of their information to third parties and giving up their first born child.[176] This study

---

[169] *Id.*

[170] Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services* 6 (TPRC 44: The 44th Research Conference on Communication, Information & Internet Policy, 2016, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

[171] *Id.* at 2.

[172] *Id.* at 11–12.

[173] *Id.* at 11.

[174] *Id.* at 12.

[175] *Id.* at 16. For many popular apps and websites, reading the terms and conditions would take multiple hours, and, therefore, it would be unreasonable to expect consumers to read them. For example, it took one man eight hours and fifty-nine minutes to read the terms of use on Amazon. Johnny Lieu, *Terms and Conditions Are Too long, Just Ask a Guy Who Read Amazon's for 9 Hours*, MASHABLE (Mar. 15, 2017), https://mashable.com/2017/03/15/reading-amazons-terms-conditions/#kabwyEF28Oq1. The Washington Post published a study showing that it takes 193 minutes to read the iTunes terms and conditions, 95 minutes to read the Candy Crush terms and conditions, and 117 minutes for LinkedIn's. Rick Noack, *How Long Would It Take To Read the Terms of Your Smartphone Apps? These Norwegians Tried It out*, WASH. POST (May 28, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/05/28/how-long-would-it-take-to-read-the-terms-of-your-smartphone-apps-these-norwegians-tried-it-out/?utm_term=.ad8ebfceaeba.

[176] Obar & Oeldorf-Hirsch, *supra* note 170, at 17.

illustrates that even though notice and consent provisions seem like a good idea, they are ineffective because consumers do not generally take advantage of the protections they provide. Because of the consumer apathy in this area, more emphasis should be placed on the actions of the manufacturers, rather than the actions of consumers to protect their privacy.

c. Lack of A Private Right of Action

The final issue with the CCPA and the Connected Devices Act is that neither one provides a private right of action for consumers.[177] Without a private right of action, consumers must rely on the government to address the wrongs committed by IoT manufacturers. Additionally, any remedy ordered by the court would not always be paid directly to the consumer. For example, in some of the cases described above, where consumers did not have a private right of action, they barely received any remedy for the breach of their sensitive information. In *In the matter of TRENDnet*, where hackers accessed home security cameras, the only remedy offered to consumers was that the company had to notify any affected customers and aid them in disabling the cameras.[178] Likewise, in *Vizio* and *VTech*, the parties sought monetary judgments, but those judgments were to be paid out to government agencies rather than consumers.[179]

As with *TRENDnet*, *Vizio*, and *Vtech*, any claim brought under the CCPA is not likely to directly compensate the consumer. Under the CCPA, any monetary judgment is to be paid to a "[c]onsumer [p]rivacy [f]und" and the money in the fund "shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title."[180]

---

[177] Assemb. B. 375, Ch. 55, 2017–18 Reg. Sess. (Cal. 2018). It should be noted that the FTC Act also does not provide a private right of action. 15 U.S.C. § 45(a)(2) (West, Westlaw current through P.L. 116-29).

[178] Complaint at 9–10, *In re* Trendnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014), 2014 WL 556262.

[179] Vizio Complaint, *supra* note 87, at 4; Vtech Electronics, *supra* note 66, at 12.

[180] CAL CIV. CODE § 1798.160 (West, Westlaw current with urgency legis. through Ch. 40 of the 2019 Reg. Sess.) (effective Jan. 1, 2020).

IV. RECOMMENDATION

As it currently stands, there is no federal, IoT-specific regulation that adequately aims to protect consumers from the unique risks that IoT devices create. IoT-specific legislation is needed because these "devices may be inherently vulnerable" to privacy and security risks.[181] The sheer amount of data being collected, and the rapid growth of these devices creates risks that must be preemptively addressed to better protect consumers. In 2012, the White House published a report on ways to promote consumer data protection.[182] The report promoted a "Consumer Privacy Bill of Rights" to advance the following objectives: "[i]ndividual [c]ontrol," "[t]ransparency," "[r]espect for [c]ontext," "[s]ecurity," "[a]ccess and [a]ccuracy," "[f]ocused [c]ollection," and "[a]ccountability."[183] The recommendation proscribed by this Note for consumer protection will also attempt to further those same objectives.

While no single regulation available is enough on its own to sufficiently protect consumers, some of the laws described above contain types of provisions that could be effective in an IoT-specific law if they are combined into one regulation. These include: (1) making the manufacturer responsible for installing reasonable security measures into the devices; (2) notice of and consent to the collection, use, and sale of personal data; (3) data breach notification laws; and (4) a private right of action. Additionally, one type of provision that is missing from these regulations that would be wise to include in a new IoT-specific regulation is use-constraints, or constraints on the way manufacturers use and store data.

---

[181] Peppet, *supra* note 15, at 135 ("[T]hese products are often manufactured by traditional consumer-goods makers rather than computer hardware or software firms. The engineers involved may therefore be relatively inexperienced with data-security issues, and the firms involved may place insufficient priority on security concerns.").

[182] *See generally* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012).

[183] *Id.* at 1.

A. A Federal Regulation Should Combine the Following in an IOT-Specific Law: Reasonable Security Measures, Notice and Consent, Data Breach Notification, and a Private Right of Action

Requiring companies to place reasonable security measures on IoT devices is important for two reasons. First, it would prevent the misuse of personal data by manufacturers and unauthorized third parties. Second, unlike notice and consent provisions,[184] it places the burden of consumer protection on the companies who may not otherwise take the extra time and effort to do so.[185] While the FTC and the White House maintain that the § 5 of the FTC Act requires IoT devices to maintain reasonable security measures,[186] as discussed above, the FTC Act is insufficient on its own to protect consumers because it is limited in scope and does not provide a private right of action.[187] Creating a provision that specifically states that manufacturers of IoT devices must provide reasonable security measures to protect consumers' data, like COPPA and the California Connected Devices Act, would promote both security interests and accountability, as recommended by the White House.[188]

While the Connected Devices Act does not define what "reasonable security measures" means, the California Department of Justice published a Data Breach report in 2016 that provided recommendations for technology companies on how to provide reasonable security measures.[189] Some of the

---

[184] Because consumers are unlikely to pay close attention to notice and comment provisions, more emphasis should be placed on the actions of the manufacturers rather than relying on the actions of consumers to protect their own privacy. *See supra* Section III.B.3.b.

[185] *See supra* Section III.B.2.

[186] THE WHITE HOUSE, *supra* note 182, at 29 ("Enforcement actions by the FTC . . . have established that companies' failures to adhere to voluntary privacy commitments, such as those stated in privacy policies, are actionable under the FTC Act's . . . prohibition on unfair or deceptive acts or practices."); FED. TRADE COMM'N, *supra* note 94, at 29 (arguing that the FTC Act provides that companies must implement reasonable security measures).

[187] *See supra* Section III.A.2.a.

[188] *See supra* Section III.B.2.; THE WHITE HOUSE, *supra* note 182, at 19, 21 ("SECURITY: Consumers have a right to secure and responsible handling of personal data . . . . ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.").

[189] KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, CALIFORNIA DATA BREACH REPORT 27–38 (2016).

recommendations the report proposes include: (1) a stronger authentication process for consumers to access devices that contain sensitive personal information, stronger than just a username and password combination; and (2) encrypting consumers' personal information.[190]

Furthermore, notice and consent may promote the control and transparency objectives set out by the White House's Consumer Privacy Bill of Rights. Notice and consent are important because they offer consumers the option to be in control of their own information,[191] and these provisions can also provide consumers with access to information so they can better understand what their data is being used for.[192] However, as discussed earlier, notice and consent are inefficient on their own because consumers rarely take the time to read privacy policy statements. Moreover, with regard to essential services, like phone services, consumers may not really have a meaningful choice since the privacy policies across phone companies tend to be similar.[193] Therefore, notice and consent must be paired with other protections to be effective in protecting consumers.

Additionally, data breach notification laws provide consumers with control and transparency because such laws give consumers an opportunity to take steps to protect themselves. For example, if credit card information is breached, a consumer could take steps to immediately cancel the card and order a new one before significant financial harm is inflicted. Finally, a private right of action may permit consumers to hold companies accountable for failure to comply with IoT regulations without having to rely on the government to bring an action.[194]

B. Use Constraints

One area where the current legislation is lacking is in putting use constraints on IoT manufacturers. Use constraints limit how manufacturers use and store sensitive data collected about consumers. These constraints could address the final three

---

[190] *Id.* at v–vi.

[191] THE WHITE HOUSE, *supra* note 182, at 11 ("Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.").

[192] *Id.* at 14 ("TRANSPARENCY: Consumers have a right to easily understandable and accessible information about privacy and security practices.").

[193] *See supra* Section III.B.3.b.

[194] *See supra* Section III.B.3.c.

objectives set out by the White House: respect for context, access and accuracy, and focused collection.[195] In a report by the FTC in 2012, the Commission explained some types of use constraints that could be applied to data privacy protection, including limiting the type of data collected, disposing of any data collected after a certain time period, and ensuring that the data collected about a consumer is accurate.[196]

If companies were to limit the type of data being collected to only data that is necessary to accomplish a goal that is reasonably related to the consumer's use of the device, then it would serve both the "respect for context" and "focused collection" objectives.[197] This limitation would also allow consumers to be more aware of what information is being collected since it would be information that consumers would reasonably expect to be collected.[198] Additionally, limits on data collection could prevent discrimination based on harmful inferences that can be made from certain types of data.[199] In its 2012 privacy report, the FTC provided an example of a company successfully limiting its data collection to that which is necessary. Takers of the Graduate Management Admission Test ("GMAT") became concerned about providing fingerprints to gain admission to the test because of the potential that they may be "cross-referenced against criminal databases."[200] GMAT responded to the concern by using palm prints to identify test-takers, rather than fingerprints.[201] Palm prints are just as accurate as fingerprinting at identifying individuals, but they are less commonly used as identifiers, so there is less risk that they can be used as a cross reference in a criminal database.[202]

---

[195] THE WHITE HOUSE, *supra* note 182, at 1.

[196] FED. TRADE COMM'N, *supra* note 94, at vii.

[197] THE WHITE HOUSE, *supra* note 182, at 15 ("RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."); *id.* at 21 ("FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain.").

[198] FED. TRADE COMM'N, *supra* note 94, at 37.

[199] Peppet, *supra* note 15, at 90 (explaining that large amounts of data collection "are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities," which can lead to discrimination).

[200] FED. TRADE COMM'N, *supra* note 94, at 27.

[201] *Id.*

[202] *Id.* (noting that the counsel for the GMAT test "received a privacy innovation award for small businesses for its work in this area").

Furthermore, requiring that companies dispose of data after a reasonable period of time serves the White House's objective of respect for context and security.[203] What qualifies as a reasonable amount of time would depend on the nature of the device and its expected use. Disposal of data not only helps maintain the most recent, accurate consumer data but also significantly decreases the amount of data left vulnerable to misuse by unauthorized third parties.

Finally, ensuring that data are accurate serves the White House's objectives of access and accuracy.[204] Inaccurate data could lead to incorrect inferences about a consumer, which in turn could harm consumers in matters of employment, insurance coverage, and more.[205] As discussed above, the FCRA imposes accuracy requirements on companies, but it is limited in scope and does not apply to many IoT devices.[206] The FTC notes that data used for different purposes could have different standards for accuracy. For example, "[c]ompanies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy" than "companies using data for marketing purposes."[207] Therefore, an IoT-specific regulation could require different standards for accuracy based on the sensitivity of the type of data collected or the vulnerability of the consumer concerning specific kinds of technology.

CONCLUSION

IoT devices are an ever-increasing force of nature in our daily lives. They provide a multitude of essential benefits that we as a society have come to rely on. Thus, IoT devices are likely to continue to become irreplaceable tools. With the many benefits that these devices bring, they also bring a vast array of privacy and security issues that our society has not had to face until recently. Because of the new and prevalent risks associated

---

[203] *See supra* notes 191, 200.

[204] THE WHITE HOUSE, *supra* note 182, at 19 ("ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequence to consumers if the data is inaccurate.").

[205] *See supra* Section II.B.2. For example, inaccurate information collected by usage-based insurance devices could cause consumers to pay more in insurance premiums. *See supra* Section I.B.3.

[206] *See supra* Section III.A.2.b.

[207] FED. TRADE COMM'N, *supra* note 94, at 30.

with the IoT and because of the increasing harms to consumers, it is time for Congress to enact an IoT-specific data privacy and security law. Some of the provisions that Congress should consider including in such a law are reasonable security measures, notice and consent, data breach notification, a private right of action, and constraints on the way that manufacturers use and store consumer data.