

## University of Washington School of Law UW Law Digital Commons

---

Technology Law and Public Policy Clinic

Centers and Programs

---

3-6-2017


# Regulating the Internet of Things: Protecting the "Smart" Home

Beth Hutchens

Gavin Keene

David Stieber

Follow this and additional works at: <https://digitalcommons.law.uw.edu/techclinic>

 Part of the [Computer Law Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Beth Hutchens, Gavin Keene & David Stieber, *Regulating the Internet of Things: Protecting the "Smart" Home*, (2017).  
Available at: <https://digitalcommons.law.uw.edu/techclinic/8>

This Book is brought to you for free and open access by the Centers and Programs at UW Law Digital Commons. It has been accepted for inclusion in Technology Law and Public Policy Clinic by an authorized administrator of UW Law Digital Commons. For more information, please contact [cnyberg@uw.edu](mailto:cnyberg@uw.edu).

**REGULATING THE INTERNET OF THINGS:  
PROTECTING THE “SMART” HOME**

*Beth Hutchens, Gavin Keene, David Stieber*

**PROBLEM**

The Internet of Things (IoT)—the internetworking of “smart” devices for the purpose of collecting and exchanging data—is developing rapidly. Estimates of the number of IoT devices currently in circulation range from 6.4 to 17.6 billion. By 2020, those numbers could reach upward of 30 billion. While the technology encourages innovation and promotes data-driven policymaking, it also compromises consumer privacy, security, and safety. Consumers are generally unaware that IoT devices transmit scores of personally-identifiable information with only rudimentary security protections in place. For some devices, inadequate security measures unnecessarily risk consumer safety by leaving the devices vulnerable to remote manipulation by third parties.

**ISSUE**

Whether IoT-connected devices found in a “smart” home should be regulated to ensure appropriate protections for consumers and their data.

**BRIEF ANSWER**

The IoT should be regulated but not yet. The industry is still in its infancy and the current political climate is too unstable. Over the next decade, the industry should be closely studied and regulation should be revisited once all of the main risks are assessed.

## DISCUSSION

### I. The Emerging and Pervasive Nature of the Internet of Things Triggers a Number of Privacy, Security, and Consumer Protection Concerns

British Technologist Kevin Ashton coined the phrase “the Internet of Things” in 1999 during a presentation to Procter and Gamble when he stated, “[a]dding radio-frequency identification and sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception.”<sup>1</sup> Since then, variations of that description have emerged to try to capture the ubiquitous and dynamic technology.<sup>2</sup> As a general matter, there is no universally-accepted definition but the common thread appears to be “smart” tangible objects that receive input from their surroundings and transmit that input to other tangible and intangible objects through the Internet, where it is aggregated.

While the Internet of Things (“IoT”) was originally envisioned as a way to streamline manufacturing,<sup>3</sup> the generally-accepted first IoT-connected device was the Carnegie Mellon Coke machine.<sup>4</sup> In 1982, students at Carnegie Mellon University programmed a Coke vending machine to keep track of its beverages, including the number of bottles remaining and how cold the bottles were—information that was uploaded to the Internet in real time, where students could remotely track the machine’s stock.<sup>5</sup> Since then, the IoT has grown exponentially, revolutionizing nearly every industry.

---

<sup>1</sup> <http://www.rfidjournal.com/articles/view?4986>

<sup>2</sup> A White House report defined it as “the ability of devices to communicate with each other using embedded sensors that are linked through wired and wireless networks.” Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values 2* (2014); The Federal Trade Commission (FTC) describes it as the connection of “physical objects to the Internet, and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing” ([tinyurl.com/nhvju4z](http://tinyurl.com/nhvju4z)).

<sup>3</sup> Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805 (2016).

<sup>4</sup> See, e.g., <http://ewahome.com/internet-of-things-iot/history-of-internet-of-things/>

<sup>5</sup> [https://www.cs.cmu.edu/~coke/history\\_long.txt](https://www.cs.cmu.edu/~coke/history_long.txt)

### **A. Devices Connected to the Internet of Things Have Proliferated**

The IoT industry and IoT technology are expanding and evolving rapidly. In 2016, over 5 million new devices were connected each day.<sup>6</sup> Depending on the type of devices included, estimates of the total number of devices currently in circulation range anywhere from 6.4 to 17.6 billion.<sup>7</sup> Those same estimates predict that by 2020, the number will have risen to anywhere from 20.8 to 30.7 billion.<sup>8</sup> This rapid materialization represents the most significant era of innovation and growth since the launch of the Internet.<sup>9</sup> From fitness trackers to “smart” thermostats and from connected toys to connected cities and healthcare services, society is on the cusp of a new technological era.<sup>10</sup> Drawing parallels to Rockefellerian oil exploits, the IoT and the data it aggregates are considered by some to be the “rocket fuel of the digital economy”<sup>11</sup>—the catalyst of industry in this new frontier.

### **B. The Internet of Things Will Provide Substantial Benefits**

Proponents of IoT technology anticipate that the benefits to consumers, industry, and society will be substantial. Consumers are promised convenience, time-saving, and even life-changing technologies. Industry is promised increased productivity and cost savings. Society at large is promised energy conservation, increased food supplies, and physical safety.

Fanciful notions of the IoT conjure up images of a Jetsonian future—one “that includes ‘smart’ refrigerators that sense when you are out of milk; smart clocks that alert your smart coffee machine that it’s time to start the morning brew; smart cars that automatically notify your smart thermostat that you are almost home; smart sheets that track your restlessness; smart glucose monitors that send signals directly to your doctor; smart light switches, ovens, security

<sup>6</sup> <http://www.gartner.com/newsroom/id/3165317>

<sup>7</sup> <http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>

<sup>8</sup> *Id.*

<sup>9</sup> <http://otalliance.actonsoftware.com/acton/attachment/6361/f-0099/1/-/-/-/OTA%20IoT%20Vision%20Paper.pdf>

<sup>10</sup> <https://otalliance.org/resources/role-connected-devices-recent-cyber-attacks>

<sup>11</sup> <https://www.forbes.com/sites/sap/2016/09/22/how-the-internet-of-things-makes-dumb-devices-smart/#27d1bb7a5b42>

systems, toothbrushes, and toilets.”<sup>12</sup> The IoT industry is in the process of fundamentally changing the consumer experience.

### **C. The Proliferation of Connected Devices Has Exposed Consumers and Their Data**

While there are tremendous benefits to be gained from IoT, the benefits come with a cost. In the rush to bring connected devices to market and capitalize on the myriad commercial and technological opportunities available, “security and privacy is often being overlooked.”<sup>13</sup> As built-in sensors constantly collect and transmit information, the amount of data collected and digitally stored by IoT devices is growing at an unprecedented pace. The devices themselves, their supporting applications, and the back-end cloud services are left susceptible to all forms of hacking—and the scores of data that they collect to all forms of misappropriation.

#### **1. Security Concerns**

Similar to most other internet-based technologies, the IoT presents a number of security concerns. Its inborn level of connectivity “allows every node, device, data source, communication link, controller and data repository attached to IoT to serve as a security threat and be exposed to security threats.”<sup>14</sup> Indeed, a 2014 study conducted by Hewlett Packard’s security unit, Fortify, determined that 70% of popular consumer IoT devices can be “easily hacked.”<sup>15</sup>

Supportive anecdotal evidence from across the industry is not hard to come by.

Benevolent hackers have shown the ease with which they can hack into “smart” homes,<sup>16</sup> cars,<sup>17</sup>

---

<sup>12</sup> Jamie Lee Williams, *Privacy in the Age of the Internet of Things* (2016), p. 14.

<sup>13</sup> <https://otalliance.org/news-events/press-releases/ota-finds-100-recently-reported-iot-vulnerabilities-easily-avoidable> (quoting Craig Spiegle, Executive Director and President, OTA).

<sup>14</sup> David Z. Bodenheimer, *The Internet of Things’ Tsunami of Legal Conundrums* (2016), pg. 74.

<sup>15</sup> [http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WP\\_xAVPytsN](http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WP_xAVPytsN)

<sup>16</sup> David Jacobi hacked his own smart home; researchers at the University of Michigan found they were able to hack into the Samsung SmartThings platform and even control an entire home automation system.

<sup>17</sup> <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>; <http://www.latimes.com/business/autos/la-fi-hy-car-hacking-20150914-story.html>

car washes,<sup>18</sup> police surveillance systems,<sup>19</sup> fitness bands,<sup>20</sup> baby monitors,<sup>21</sup> printers,<sup>22</sup> toasters,<sup>23</sup> e-cigarettes,<sup>24</sup> toilets,<sup>25</sup> and even light bulbs.<sup>26</sup> Cybercriminals showed the damage they can inflict when they compromised hundreds of thousands of connected devices to take websites like Amazon, Twitter and Netflix offline,<sup>27</sup> or when they seized control of the digital locks on hotel rooms at a resort in Austria and locked guests out of their rooms.<sup>28</sup> More recently, hackers successfully infiltrated the networks of a number of hospitals in the UK, compromising patient data and the connected devices used in those hospitals.<sup>29</sup>

For IoT systems—integrated networks of IoT devices that communicate among themselves, usually in concert with computers, allowing automated and remote control of many independent processes—security breaches can cause catastrophic damage. A hacker attack on a smart grid system could turn off power to millions of households and businesses, disrupting operations, creating massive economic and environmental harm, or threatening health and safety. Even worse, such a breach could jeopardize national security or public safety.<sup>30</sup>

For more common IoT devices, security weaknesses appear to stem primarily from a combination of rudimentary hardware and software, the general ignorance of manufacturers and consumers, and a lack of standards for sharing and protecting data across industries.<sup>31</sup> IoT devices are ultra-simple, generally to keep down manufacturing costs.<sup>32</sup> When comprised of many devices, an “IoT system’s security is limited to the security level of its least secure

<sup>18</sup> <http://www.darkreading.com/vulnerabilities---threats/hackin-at-the-car-wash-yeah/d/d-id/1319156>

<sup>19</sup> <https://blog.kaspersky.com/internet-of-crappy-things/7667/>

<sup>20</sup> <http://www.businessinsider.com/kaspersky-researcher-demonstrates-smart-bracelet-hack-2015-3>

<sup>21</sup> <https://arstechnica.com/security/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/>

<sup>22</sup> [http://www.slate.com/blogs/future\\_tense/2014/12/30/the\\_internet\\_of\\_things\\_is\\_a\\_long\\_way\\_from\\_being\\_secure.html](http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_being_secure.html)

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

<sup>26</sup> <https://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs/>

<sup>27</sup> <https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/>

<sup>28</sup> <http://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers>

<sup>29</sup> [https://www.theregister.co.uk/2017/05/12/nhs\\_hospital\\_shut\\_down\\_due\\_to\\_cyber\\_attack/](https://www.theregister.co.uk/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack/)

<sup>30</sup> Lucy Thompson, *Insecurity of the Internet of Things* (2016), pg. 34.

<sup>31</sup> <http://www.peak10.com/top-internet-things-iot-security-concerns/>

<sup>32</sup> <http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Security-risks-from-the-internet-of-things>

component.”<sup>33</sup> And, generally-speaking, manufacturers of traditional in-home devices, which are now becoming “smart,” have typically never had to think about the privacy or security of their consumers’ data before because they never collected any data.<sup>34</sup> Now the stewards of scores of personal information, these manufacturers face realities of a brand new world they know nothing about.<sup>35</sup> This technological illiteracy is worse among users of connected devices. Studies indicate that they do not seem to bother with security at all.<sup>36</sup>

## 2. Privacy Concerns

In addition to their inherent security weaknesses, IoT-connected devices often collect data in ways that seriously undermine privacy rights. This is because the IoT is by design a system of surveillance.<sup>37</sup> Connected devices collect, transmit, and share highly-sensitive information about their users and environment for the purpose of aggregating the data and learning something from it. To that end, devices collect information such as an individual’s music preferences, running routes, exercise efforts, eating habits, alcohol consumption, sleeping patterns, medical symptoms, gender, zip code, geolocation, financial information, and “even the stride or cadence of a person’s walk or run.” Often times the collected information falls outside of the protections of laws like HIPAA and HITECH.<sup>38</sup>

While the collected information may appear piecemeal at first blush, the “enormous data trove that will result will contain a wealth of revealing bits of information that . . . may present a deeply personal and startlingly complete picture of each of us.”<sup>39</sup> Seemingly innocent pieces of information when viewed in isolation can paint a full picture of an individual when pieced together. Companies certainly make efforts to address these concerns, but the anonymization of

---

<sup>33</sup> David Z. Bodenheimer, *The Internet of Things’ Tsunami of Legal Conundrums* (2016), pg. 74.

<sup>34</sup> Jamie Lee Williams, *Privacy in the Age of the Internet of Things* (2016), p. 14.

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> Christin S. McMeley, *Protecting Consumer Privacy and Information in the Age of the Internet of Things* (2014), pg. 74.

<sup>39</sup> Former FTC Commissioner Edith Ramirez.

IoT data is practically difficult to achieve.<sup>40</sup> In 2012, German researchers demonstrated the insights to be gained from seemingly innocent pieces of information by intercepting unencrypted data from a home's smart meter device to determine what television show someone was watching at that moment.<sup>41</sup>

The sheer amount of data that IoT devices can collect is staggering. A Federal Trade Commission report entitled "Internet of Things: Privacy & Security in a Connected World" found that fewer than 10,000 households can generate 150 million discrete data points every day.<sup>42</sup> We are truly living through the "golden age of surveillance."

Moreover, companies are far from transparent about their data collection practices. Consumers are often kept in the dark about when and how IoT devices are gathering data and what the companies that collect the data are doing with it. For example, smart devices with voice recognition technology can record what we say, even when we don't realize it. This was made clear in early 2015 after news broke that the privacy policy for Samsung's SmartTV warned users that the device could eavesdrop on what consumers said in the home: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."<sup>43</sup>

The collected data are then used by vendors for any number of purposes. Most consumers are aware that data are often sold and/or used to serve us with targeted advertising or marketing. It has been predicted that the data will, in the near future, be sought by employers, banks, and insurance companies in order to make inferences about employment potential, creditworthiness,

---

<sup>40</sup> <http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf>

<sup>41</sup> <https://www.cnet.com/news/researchers-find-smart-meters-could-reveal-favorite-tv-shows/>

<sup>42</sup> <http://www.businessinsider.com/internet-of-things-security-privacy-2016-8>

<sup>43</sup> Jamie Lee Williams, *Privacy in the Age of the Internet of Things* (2016), p. 14–15; <https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf>



and health. In 2014, data from a Fitbit fitness tracker was admitted as evidence in a personal injury lawsuit.<sup>44</sup> Legal scholars have predicted that similar data could be used in a divorce court as evidence of an extramarital affair.

And this is just the data collection we (ostensibly) consent to. Hackers intensify the privacy concerns. Recently, toy company Spiral Toys came under fire for the weak privacy and security protections built into its *CloudPets* line—IoT-connected stuffed animals, used to exchange heartfelt audio messages between parents and kids. Hackers infiltrated the unprotected devices as well as the company’s online database containing consumer data collected from the devices, and used the toys to surveil and harass children.<sup>45</sup> Similarly, Genesis Toys was criticized for the weak protections built into its *My Friend Cayla* doll line—IoT-connected dolls with built-in microphones that transmit audio recordings via Bluetooth.<sup>46</sup> Its privacy and security protections were so weak that Germany banned both its sale and ownership.<sup>47</sup>

### 3. Consumer Protection Concerns

While the security and privacy implications alone are sufficiently troubling, what makes IoT uniquely dangerous is that its actions can be executed in the physical—rather than merely digital—world: doors are unlocked, temperatures are lowered, insulin is delivered, and fire suppression systems activated.<sup>48</sup> If the integrity of the data or device is compromised,

---

<sup>44</sup> See Parmy Olson, Fitbit Data Now Being Used in the Courtroom, FORBES TECH (Nov. 16, 2014), <http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim>.

<sup>45</sup> <http://mashable.com/2017/02/27/internet-of-things-cloudpets-hacking/#7HequdVN4Sq>

<sup>46</sup> <http://www.snopes.com/2017/02/24/my-friend-cayla-doll-privacy-concerns/>

<http://www.npr.org/sections/alltechconsidered/2016/12/20/506208146/this-doll-may-be-recording-what-children-say-privacy-groups-charge>

<sup>47</sup> <http://www.npr.org/2017/02/20/516292295/germany-bans-my-friend-cayla-doll-over-spying-concerns>

<sup>48</sup> <http://otalliance.actonsoftware.com/acton/attachment/6361/f-0099/1/-/-/-/OTA%20IoT%20Vision%20Paper.pdf>, pg. 2

connectivity interrupted, or the functionality remotely controlled by a malicious actor, the consequences can be catastrophic, even lethal.<sup>49</sup>

Security researchers have demonstrated that both insulin pumps and pacemakers can be hacked. Drug infusion pumps (used for delivering morphine drips, chemotherapy, and antibiotics) can be remotely manipulated to change the dosage given to patients; Bluetooth-enabled defibrillators can be manipulated to deliver random and unwarranted shocks to a patient's heart or to prevent one from occurring; the temperature settings on refrigerators used for storing blood and/or drugs can be reset; digital medical records can be altered.<sup>50</sup> This can cause physicians to misdiagnose a patient, prescribe the wrong drug, or administer unwarranted care, among other things.

#### **D. Consumers Are Concerned**

As more and more cases of data breaches, identity theft, and state-sponsored espionage come to light, consumers and businesses alike are becoming increasingly reticent about sharing their personal and business data. Nine in ten Americans state that controlling the information that is collected about them is important.<sup>51</sup> At the same time, users' confidence that their data is secure and private is at an all-time low.<sup>52</sup> When it comes to IoT, consumers' fears about security and privacy are cited as the two biggest barriers to IoT adoption. If individuals and businesses cannot trust that their personal and proprietary data will be kept secure and private, large-scale adoption of IoT—and its accompanying benefits to consumers and commercial entities—will not be realized.

#### **E. Voice-Enabled IoT Devices in the Home Amplify the Risks**

---

<sup>49</sup> *Id.*

<sup>50</sup> Jamie Lee Williams, *Privacy in the Age of the Internet of Things* (2016), pg. 15

<sup>51</sup> <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>

<sup>52</sup> *Id.*

Amplifying the privacy and security risks are voice-enabled devices like Amazon Echo and Google Home. Despite their great functionality, to date, these devices do not have sufficient user authentication. While some devices have options to limit direct purchasing of additional products and services, few if any controls are in place to curb “unauthorized voices” issuing commands.

When these devices are found in the home, connected to a home hub, the damage that can be done expands drastically.<sup>53</sup> Connected devices in the home can include door locks, motion detectors, sprinkler systems, alarm systems, lighting, HVAC (heating, ventilating, and air conditioning), and a number of appliances. Craig Young, a cybersecurity researcher at Tripwire, says the most common hack is to break into a connected home hub, which then provides access to any of the connected devices inside. It does not take much imagination to realize the risk and impact of physical harm which could occur. Someone outside of a home yelling through a window, a voice on a TV or even a message left on an answering machine could issue commands such as “open my door” or “turn my heat off.”<sup>54</sup>

On the privacy front, connected energy meters can track when we are home, who is there, and what we do, including the appliances we use. In 2010, the head of regulatory affairs at Siemens Metering Services, a leader in the smart meter industry, stated:

“We, Siemens, have the technology to record [energy use] every minute, second, microsecond, more or less live. From that we can infer how many people are in the house, what they do, whether they’re upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data.”

Such smart devices have already entered the front door and will multiply rapidly within the smart home market. A recent Consumer Electronics Association study predicts “smart

---

<sup>53</sup> <http://www.csoonline.com/article/3077537/internet-of-things/security-concerns-rising-for-internet-of-things-devices.html>

<sup>54</sup> <https://www.ntia.doc.gov/files/ntia/publications/ota-docket170105023-7023-01.pdf>

thermostats, door locks, smoke detectors and light switches will expand from 20.7 million units in 2014 to 35.9 million units in 2017.”<sup>55</sup> In other words, these threats are real and the dangers are imminent.

## **II. Current Regulatory Schemes and their Applicability to IoT Devices in Smart Homes**

Generally speaking, current regulatory schemes (either pending or in place) do not place a large distinction between IoT devices found in a smart home versus other types of IoT devices (such as autonomous vehicles, wearables, smart phones and other connected technologies).<sup>56</sup> The existing U.S. legal framework is comprised of a patchwork of frequently outdated laws and regulations at both the federal and state levels, which often apply to particular industry segments, specific types of data, or certain activities. As it stands, and in addition to the existing federal patchwork, several states have, or are in the process of, creating their own regulatory approaches to IoT. There are also several industry trade groups publishing guidance and best practices.

### **A. Pending Federal Legislation**

There is no comprehensive federal statute or regulation that protects the privacy of personal information held by the public sector. “Instead, federal law tends to employ a sectoral approach to the regulation of personal information.”<sup>57</sup> In fact, IoT technologies are covered by more than thirty different congressional committees.<sup>58</sup>

In the current political and legislative climate, new legislation that comprehensively addresses these issues is unlikely in the near future. Therefore, existing privacy-specific laws—such as the Children’s Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-

---

<sup>55</sup> David Z. Bodenheimer, *The Internet of Things’ Swelling Technology Tsunami and Legal Conundrums* (2016), pg. 5.

<sup>56</sup> See, generally, “Who’s in Charge of Regulating the Internet of Things?” available at: <http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/>

<sup>57</sup> <https://fas.org/irp/crs/RL31730.pdf>, pg. CRS-5

<sup>58</sup> David Z. Bodenheimer, *The Internet of Things’ Tsunami of Legal Conundrums* (2016), pg. 75.

Bliley Act (GLBA)—can be directly applied to connected devices and their data-collection activities. Unfortunately, these existing laws are often too narrowly drafted to cover all implementations of new technology.

### **1. The DIGIT Act<sup>59</sup>**

In March of 2016, the second session of the 114<sup>th</sup> Congress introduced Senate Bill 2607, otherwise known as the “DIGIT Act,” to ensure that policies governing the IoT “maximize the potential and development of the growing number of connected and interconnected devices to benefit businesses, governments, and consumers.”<sup>60</sup> The bill requires the Department of Commerce to convene a working group of federal stakeholders to provide recommendations and a report to Congress regarding the IoT. The working group must: (1) identify federal laws and regulations, grant practices, budgetary or jurisdictional challenges, and other sector-specific policies that inhibit IoT development; (2) consider policies or programs that encourage and improve coordination among federal agencies with IoT jurisdiction; (3) implement recommendations from the steering committee; (4) examine how federal agencies can benefit from, use, and prepare for the IoT; and (5) consult with nongovernmental stakeholders. It also creates a Steering Committee that must advise the working group about laws, budgets, spectrum needs, individual privacy, security, small business challenges, and any international proceedings or negotiations affecting the IoT.

The bipartisan bill has broad support across the technology industry, including the U.S. Chamber of Commerce, the Competitive Carriers Association (CCA), the Telecommunications Industry Association (TIA), the Semiconductor Industry Association (SIA), the Consumer Technology Association (CTA), the Information Technology Industry Council (ITI), and the

---

<sup>59</sup> S.2607, “To ensure appropriate spectrum planning and interagency coordination to support the Internet of Things”, *Available at:* <https://www.congress.gov/bill/114th-congress/senate-bill/2607>

<sup>60</sup> <https://www.congress.gov/bill/114th-congress/senate-bill/2607>

National Association of Manufacturers. It was reintroduced in January 2017 as House Resolution 686 and was assigned to the House Energy and Commerce committee which will consider it before possibly sending it on to the House or Senate as a whole.<sup>61</sup> Skopos Labs predicts that the Resolution has an 18% chance of being enacted. A companion bill for this bill, s88-115, has not yet been enacted, but faces equally low chances of passage.<sup>62</sup>

### **B. Federal Regulations**

Federal agencies have fragmented approaches to regulating and numerous Congressional committees technically have oversight authority. An October 2015 Congressional Research Service (CRS) report identified eleven different federal entities with at least partial regulatory jurisdiction over some slice of IoT.<sup>63</sup>

In theory, the FTC's Section 5<sup>64</sup> authority over unfair or deceptive trade practices should provide adequate protections regarding IoT devices.<sup>65</sup> Similarly, there is a cadre of sector-specific regulations that would come into play if, for example, health information or children's information was being collected.<sup>66</sup> IoT devices also present a unique problem in that they touch both privacy and security concerns, which at a minimum, would trigger the need for a privacy notice and a data breach notification policy. The question then becomes one of how to properly craft such a notice and a policy given the numerous, and sometimes conflicting, local, state, and federal regulations that concern both privacy and security.<sup>67</sup>

### **C. State and Local Legislation and Regulations**

---

<sup>61</sup> <https://www.govtrack.us/congress/bills/115/hr686>

<sup>62</sup> <https://www.govtrack.us/congress/bills/115/s88>

<sup>63</sup> <https://fas.org/sgp/crs/misc/R44227.pdf>, pg. 9–10

<sup>64</sup> 15 U.S.C. § 45.

<sup>65</sup> Internet of Things: Privacy & Security in a Connected World, FTC Staff Report, January, 2015.

<sup>66</sup> See, e.g., HIPPA, COPPA, FRCA, and others.

<sup>67</sup> The question remains as to what the regulatory landscape might look like where ISPs are concerned. Unless and until there is significant movement in that arena, it stands to reason that federal regulations pertaining to Internet and Broadband providers in the context of IoT devices is beyond the scope of this paper. However, the DIGIT Act requires the FCC to seek public comment on the IoT's spectrum needs, regulatory barriers, and growth with licensed and unlicensed spectrum and to submit a summary of those comments to Congress.

Currently, Arizona, Delaware, Indiana, Kansas, Massachusetts, Michigan, Nebraska, North Dakota, Texas, Utah, Virginia and Wisconsin have been applauded for adopting pro-innovation policies that are thought to create good jobs and fuel economic growth. Overall, these states have set the pace and tone for key technology practices (e.g., strong right-to-work legislation, fast internet access, robust entrepreneurial climate, open posture to new business models and technologies, tax policy, tech workforce, investment attraction, STEM degrees, unmanned innovations and sustainability policies) that promote innovation and help avoid sending valuable talent and economic growth to a neighboring state.<sup>68</sup> New York City has developed special guidelines to help city agencies understand the risks associated with the IoT and best practices to mitigate these risks.<sup>69</sup>

#### **D. Self-Regulation**

In the absence of clear guidance for emerging technologies like IoT devices, many industries and stakeholders develop and implement self-regulatory programs. These include, for example, incorporating best practices and principles such as the FIPPs, the NIST framework, the ISO standards, and various industry-specific platforms. Many stakeholders remain skeptical that IoT device companies can (or will) effectively self-regulate. However, considering the privacy, data protection, and information security guidelines under the existing patchwork of federal, state, and local legal frameworks, self-regulation may be the only viable option for the time being.

Technology sectors and companies that collect, store, and monetize large data sets are, not surprisingly, overwhelmingly in favor of self-regulation. They argue the benefits of leveraging large amounts of data to simplify daily tasks would be hamstrung by adding IoT

---

<sup>68</sup> See Consumer Technology Association, *Internet of Things: A Framework for the New Administration*, November, 2016 available at: <https://www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf>

<sup>69</sup> See NYC Guidelines for the Internet of Things, Available at: <https://iot.cityofnewyork.us/about/>

specific regulations in an already complex legal landscape. Additionally, there are already industry-led initiatives and best-practices guidelines as the preferred method for ensuring appropriate handling of sensitive data. However, self-regulation has not always lead to ideal results, so it is highly likely that the subject will be revisited as the legal landscape takes shape.

### **III. Other Countries Have Made Efforts to Regulate**

#### **A. The European Union’s GDPR Will Encompass Much of the IoT**

The European Union has established a set of privacy regulations that will greatly affect the way that the IoT is regulated. These rules, called the “General Data Protection Regulation,” or “GDPR,” will form a cohesive set of regulations covering all data collectors and processors in the EU, or those dealing with an EU resident’s data. These rules govern data collectors and privacy, establish a new regulatory structure, and also explicitly grant certain privacy rights to EU citizens and residents. These will all affect the way the IoT develops in Europe, and worldwide.

The GDPR applies to all companies that are based in the EU. The GDPR also regulates any corporation anywhere in the world that collects or processes any data originating from a user in the EU. The GDPR distinguishes between data “controllers” (which collect data from EU residents, e.g. App manufacturers, IoT device manufacturers) and data “processors” (which use or process that data on behalf of the controller or the user, e.g. cloud service providers). By regulating both controllers and processors, the GDPR will affect all IoT device manufacturers that operate in the European Common market. The GDPR also will regulate any company that collects or processes personal data relating to an individual in the EU, even if that company gets that information from a non-EU source.



The GDPR establishes a new regulatory framework to handle these new regulations efficiently. Prior EU regulations required member nations to pass equivalent legislation in their own governments, then relied on the regulatory apparatus of the member nation to enforce the regulations. The GDPR, in contrast, will take effect without any of the EU member nations creating their own equivalent legislation. The GDPR will be administered not by the existing regulatory apparatus of member nations, but by a designated “Special Authority” within each member nation. The Special Authority will function like a “one stop shop” for regulatory action within the member nation, overseeing the hearing and administration of complaints, the levying of sanctions, and the approval of licenses for regulated companies. The Special Authorities of all the member nations will coordinate via the “European Data Protection Board.”

The GDPR also requires a new position called a “Data Protection Officer” be established at all corporations that deal with large amounts of data. This includes all “public authorities or bodies” (including all “national, regional, and local authorities”<sup>70</sup>), and at all Data Controllers or Data Processors whose “core activities” include either processing large amounts of personal data, or the regular and systemic monitoring of Data subjects. The Data Protection Officer is responsible for ensuring compliance with the GDPR, and is supposed to be competent to manage both technical and legal aspects of regulation.

The GDPR also provides new personal rights of privacy for “Data Subjects” (end users) within the EU. These include the right to erasure, formerly known as the right to be forgotten. The right of erasure is more limited than the previous right to be forgotten; it allows data subjects to request the deletion of data, when the legitimate interests of the controller are overridden by interests or fundamental rights of the data subject that require the protection of personal data.

---

<sup>70</sup> “Guidelines on Data Protection Officers,” Retrieved May 10, 2017, at [http://ec.europa.eu/information\\_society/newsroom/image/document/2016-51/wp243\\_en\\_40855.pdf](http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf)

Data subjects also have the right to “not have a decision made purely by algorithm,” meaning a subject is entitled to have an algorithmic decision explained and rationalized by a human person, which the data subject then has the right to challenge. It is unclear how either of these rights are to be prosecuted, but they are in the GDPR.

The GDPR also mandates that Privacy be designed into the technology of the data controller and processor. In both design and execution, the Data Collectors and Processors must “implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization.” This new duty “take[s] into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity.”<sup>71</sup> Privacy must be implemented through both technical and organizational measures, to ensure that non-essential personal data not be processed, and not be stored. These obligations exist in considering what data to collect, how to process it, and how to store it. The GDPR also requires the Processor to be able to demonstrate affirmative compliance with this regulatory regime, and for the consent of the data subject to be verifiable, even after being granted. These responsibilities fall on the Data Protection Officer.

#### **IV. Attempting to Craft Broad, All-Encompassing Rules Regulating “Smart” Devices is Premature**

As a general matter, cybersecurity for the IoT is a poor fit for prescriptive regulation. As the FCC Chairman said last year, “[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking.”<sup>72</sup> In its current state, the very concept of IoT belies definition. There is much left to discover with respect to use cases, consumer

---

<sup>71</sup> GDPR Article 25, Accessed. May 17, 2017. <http://www.privacy-regulation.eu/en/25.htm>

<sup>72</sup> In re of Protecting and Promoting the Open Internet Framework for Broadband Internet, GN Docket No. 14-28; GN Docket No. 10-127 COMMENTS OF AT&T SERVICES, INC. Heather M. Zachary Christopher M. Heimann Kelly P. Dunbar Christi Shewman Sameer Ahmed Gary L. Phillips Robert A. quoting Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute, Washington, D.C. (June 12, 2014) (discussing the FCC’s new approach to cybersecurity).

demand, device and application supply chains, and the 5G wireless network that any attempt to draft a comprehensive set of regulations is an exercise in futility. Further, the speed with which regulations slog through notice and comment rulemaking or the legislative process coupled with the rapidly evolving technology and marketplace of IoT devices all but guarantees near-instant obsolescence for any regulation that manages to see the light of day.

Policymakers should be vigilant but, in the words of one FTC Commissioner, exercise “regulatory humility.” Regulation threatens to lock in technology, prematurely predict consumer preferences, and stymie efforts to innovate and ensure global harmonization. In the absence of a federal framework, any new set of rules would add an additional layer to an already crowded regulatory environment. It would be best, at least for the time being, to employ existing regulations and their enforcement agencies according to data type, as that would allow for improvements to technology without hamstringing innovation and commerce. Any attempts to regulate a rapidly changing area such as IoT would be premature, imperfect, and in all probability, ineffective.

## **CONCLUSION**

The first fatality in connection with an automobile accident was in 1869. It was not until the 1950s that the first national comprehensive regulatory scheme governing automobiles was enacted. While the Internet of Things emerged as early as the 1980s, it is just starting to come into the main, and interested parties are only recently beginning to grasp its effects on society and consumer populations. Any attempts to regulate now will almost certainly overlook serious risks that, at this stage in the IoT’s evolution, are unforeseeable. As has been proven time and again in the tech sector, any rule or regulation is sure to be obsolete before the technology it attempts to govern is done emerging and evolving. In the interim, to address known risks—

Commented [k1]: I think we can probably cut this... It doesn't track our conclusion or match the section heading

related to privacy, security, and safety—concerned parties should look to existing protections at the both the state and federal level and attempt to update existing frameworks.