WHEN THE INTERNET OF THINGS FLOUNDERS: LOOKING INTO GDPR-ESQUE SECURITY STANDARDS FOR IOT DEVICES IN THE UNITED STATES FROM THE CONSUMERS' PERSPECTIVE

Jeremy Siegel*

I. Introduction

The "Internet of Things" can be described as "objects with sensors networked together that are capable of communicating with one another."[1] With the rising prevalence and sheer number of uses Internet of Things ("IoT") devices can be deployed, Americans are facing more vulnerabilities and risks of having their data breached than they ever have before.[2] With an increase in the number of devices the

* J.D. Candidate, Suffolk University Law School, 2020; B.S. in Business Management, Roger Williams University, 2012. Jeremy can be reached at jsiegel607@gmail.com.

[1] *See* Dalmacio V. Posadas, Jr., *After the Gold Rush: The Boom of the Internet of Things, and the Busts of Data-Security and Privacy*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 75–76 (2017) [hereinafter *After the Gold Rush*] (providing a basic overview of the Internet of Things, including how it is changing the way the world is conducted, data is processed, and how incredibly complex it is); *see also* SAMUEL GREENGARD, THE INTERNET OF THINGS 15 (2015) (defining the Internet of Things to "quite literally [mean] 'things' or 'objects' that connect to the Internet—and each other"). For purposes of this Note, the author intends an "IoT device" to primarily be an everyday consumer device.

[2] *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 133 (2014) (highlighting that as far back as 2013, security firm Symantec "discovered a new Internet work that targeted small Internet of Things devices—particularly home routers, smart televisions, and Internet-connected security cameras—in addition to traditional computers"); *see also* Nick Ismail, *The Internet of Things: The security crisis of 2018?*, INFORMATION-AGE (Jan. 22, 2018), *archived at* https://perma.cc/3AXF-YL3L (illustrating that because of the vast amount of devices

average person interacts with on a regular basis comes more access points where a breach could occur, and consumers are not even aware of this risk.[3] The Internet of Things spans across every socioeconomic and demographic group in the world, including the homeless community, which utilizes smart phones to keep in touch with family and social workers.[4] The Internet of Things is also helping developing countries propel businesses, education, agriculture, and healthcare.[5]

The vast majority of everyday, average consumers use these devices to help make their lives easier by streamlining routine functions, despite not knowing how their information is being secured

the consumer uses in their daily lives, combined with the lack of security standards for these devices, creates entry points for potential breaches); *see also* Rishi Bhargava, *Your IoT Is Probably Not A-OK*, FORBES (July 16, 2018), *archived at* https://perma.cc/98MU-4RWN (explaining that because of the variety of Internet of Things devices, from medical devices to toys, over twenty billion devices will be connected to one another by 2020).

[3] *See* Alfred NG, *IoT attacks are getting worse -- and no one's listening*, CNET (Mar. 15, 2018), *archived at* https://perma.cc/XT2L-YK35 (suggesting that while consumers are increasing the number of devices they have, it actually means increases in vulnerabilities). For purposes of this Note, such smart devices the Author is referring to are wearable electronics, automobiles, and home appliances all connected via Wi-Fi. One issue that is not being addressed is older technology from years ago that does not have the ability to update its operating system.

[4] *See* Rosie Spinks, *Smartphones are a lifeline for homeless people*, THE GUARDIAN (Oct. 1, 2015), *archived at* https://perma.cc/6NET-UZD9 (showcasing that often times homeless people are given smart phones by friends, family, and caseworkers to give them an easy way to communicate, check on their safety, and give them empowerment to get back on their feet); *see also* Claire Cain Miller, *Fighting Homelessness, One Smartphone at a Time*, N.Y. TIMES (Apr. 14, 2015), *archived at* https://perma.cc/79RU-X2DD (explaining how a nonprofit in California called Community Technology Alliance receives smartphone donations from Google to be given to the homeless community in San Francisco); *see also* Rob Goodier, *How the Internet of Things Is Improving Lives and Livelihoods in Developing Countries*, ENGINEERING FOR CHANGE (July 1, 2016), *archived at* https://perma.cc/2DMK-VH5X (illustrating that people in third world or developing countries that may not have access to electricity, sanitation, or clean water, do have access to 2G cellular networks).

[5] *See* Kai Goerlich, *How the Internet of Things is Turbocharging Developing Economies*, DIGITALIST MAG (June 29, 2016), *archived at* https://perma.cc/5AMC-BEUA (highlighting how mobile phones in Africa are becoming a lifeline for businesses and educational institutions, and the potential for IoT to help farmers improve efficiency and productivity in their crops and livestock).

on these devices, or how secure the devices themselves are.[6] Aside from the dangers that consumers face when IoT devices are hacked, businesses also face considerable risks given the vast amount of customer data they hold, which is an attractive target for hackers.[7] As data breaches increase in regularity, especially amongst corporations such as Capital One and Marriott, consumers are becoming numb to these stories, are not taking the risks seriously, and do not know how to protect themselves.[8]

The risks of data breaches caused by IoT devices are grave, and unfortunately, there are a variety of barriers preventing injured consumers from obtaining a proper remedy if they are injured by one.[9] From a purely legal cause of action perspective, there is not a single tried and tested, successful legal theory that consumers can rely on to bring a cause of action against an IoT manufacturer.[10] From a

[6] *See Kaspersky Lab Survey Finds North American Consumers Plagued by Cyber-Stress*, BUSINESS WIRE (May 1, 2018), *archived at* https://perma.cc/DKW6-ZPW3 (highlighting that consumers are aware that the risk of data breaches is becoming a part of their daily lives). Consumers are growing weary of these risks, yet they do not know how to protect themselves. *Id.*

[7] *See* Juan Salazar, *ARE CONSUMERS ACCEPTING DATA BREACHES AS THE NEW NORMAL?*, DATACONOMY (Nov. 10, 2016), *archived at* https://perma.cc/C2UV-VEYV (examining the 2013 Target hack where cybercriminals stole the identity of millions of customers, in addition to other national retailers).

[8] *See id*. (proffering that consumers don't think that breaches will happen to them, and because they have not suffered any major consequences from the breach, or cannot picture injury in the future from a breach, it is an afterthought); *see also* Josh Dhyani, *Science-Based Food Labels: Improving Regulations & Preventing Consumer Deception Through Limited Information Disclosure Requirements*, 26 ALB. L.J. SCI. & TECH. 1, 2–3 (2016) (inferring that consumers could protect themselves if they were able to make informed decisions, similar to making an informed decision to buy organic food in the grocery store).

[9] *See* Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1326 (2017) (explaining that difficulties for consumers who have been breached includes proving they have been hacked, satisfying the imminent injury requirement for standing, and the lack of comprehensive federal statutes that consumers can use to bring a cause of action).

[10] Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, Jan. 2014, at 2, 8–9, 2014 WL 10442 (depicting the difficulty a consumer that is victim to a data breach has in bringing a cause of action, assuming they are able to show causation; a nearly impossible feat to accomplish). After that, traditional contract law claims fail because showing a binding promise by the breached company is tough. *See id.* at 5. In making a tort law claim, negligence and unjust

procedural stand point, recent cases have shown the difficulty that victims of data breaches face when trying to satisfy the standing requirement that stems from Article III of the U.S. Constitution, halting any chance of recovering damages.[11] Despite the legal theory and procedural fences faced by consumers, there have been some recent successes where courts have recognized standing for breached consumers that could not show they suffered a tangible "injury-in-fact."[12] Though companies are continuing to invest in security

enrichment, among others, have proven unsuccessful. *See id.* at 6–7. *Compare id. with* Tanya Murray, *How to Slay the Hydra: Adopting Charles Alan Wright's "The Law of Remedies as a Social Institution" as a Framework for Preventing Data Breaches*, 94 U. DET. MERCY L. REV. 127, 128–29 (2017) (concluding that Charles Alan Wright's "five principles for a socially useful law of remedies" should be applied for the singular goal of preventing harm).

[11] *See* Clara Kim, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 557–58 (highlighting that courts are reluctant to establish the "injury-in-fact" requirement because credit card companies and financial institutions will give refunds for fraudulent activity, and because claiming future injury is difficult to demonstrate); *see also* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (holding that plaintiffs did not satisfy the standing requirement, and their argument of an "enhanced risk of future identity theft" was too speculative). This case further discusses the circuit split regarding standing. *See Beck*, 848 F.3d at 274; *see also* Katz v. Pershing, L.L.C., 672 F.3d 64, 80 (1st Cir. 2012) (concluding that plaintiffs argument that an increased risk that someone "might access her data" is not sufficient of Article III's requirement of actual or impending injury); *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (holding that the plaintiff class action suit did not satisfy Article III standing because the injury was not imminent or certainly impending).

[12] *See In re* Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018) (holding that information obtained by hackers gave rise to the risk of identity theft, which was sufficient to satisfy the injury-in-fact requirement). This case acknowledges that the plaintiffs' potential for future injury is less about standing and more about causation problems. *Id.* at 1029; *see also* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018) (holding that plaintiffs did have standing because the data theft could have led breached consumers to spend money and time for credit-monitoring services, which was sufficient to be considered injury); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016) (holding that even though the victims of a data breach could not prove that there was literal certainty that their data would be misused, the costs of mitigating the imminent harm of that misuse was sufficient to satisfy Article III standing); *see also* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015) (holding that the mere fact that hackers stole consumers' information is enough to satisfy the injury requirement for standing). The court reasoned, rather simply, that "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

infrastructure to prevent data breaches, there is still no widely accepted or recognized definition of what "negligence" or "standard of care" is for IoT companies.[13] This lack of a definition is leading to a lot of uncertainty regarding how consumers can protect themselves.[14]

Federal legislation in the United States revolving around cyber security – whether it's guidelines for companies, specific industries, the government, or how consumers should be notified if they are a victim to a data breach – is incredibly dispersed and lacking in clarity.[15] Because federal legislation is very ad-hoc and piece meal in the United States, with various industries and verticals supported by different acts instead of one general branch or statute, consumers affected by a data breach have a difficult time determining what legislation to rely on.[16] Compared to federal laws, each of the fifty states have their own way of handling data breaches.[17] The European

See Remijas, 794 F.3d at 693; *see also* Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–42 (9th Cir. 2010) (affirming that the negligence and breach of implied contract argument was sufficient to satisfy injury-in-fact requirement for standing).

[13] *See* Kim, *supra* note 11, at 577–78 (articulating that the standard of care is not clear for data breaches).

[14] *See* Kim, *supra* note 11, at 578 (adding that because there are no "baseline data security standards," companies have to develop their own best practices by paying attention to developments in the field or by showing the problems arising from lack of best practices or standards of care). *See also* Tony Bradley, *Gartner Predicts Information Security Spending To Reach $93 Billion In 2018*, FORBES (Aug. 17, 2017), *archived at* https://perma.cc/US6E-6N2N (relying on Gartner report that the amount of money companies will spend on information security products will grow to around $93 billion in 2018).

[15] *See* Stephen Jones, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH L. REV. 783, 791 (2018) (explaining that federal legislation is industry-specific and does not give consumers a proper cause of action); *see also* Ted Schlein, *The United States needs a Department of Cybersecurity*, TECHCRUNCH (Apr. 16, 2018), *archived at* https://perma.cc/H95G-ZG65 (implying that the Department of Homeland Security, FBI, Department of Justice, and Department of Defense all have similar functions regarding cybersecurity but do not work together, causing friction).

[16] *See A Glance at The United States Cyber Security Laws*, APPKNOX (Oct. 16, 2018), *archived at* https://perma.cc/78QU-P4DJ (outlining current United States federal and state legislation regarding cyber security law, and how there are specific acts designed to protect the financial services industry and the consumers' medical records).

[17] *See* Hilary G. Buttrick et al., *The Skeleton of a Data Breach: The Ethical and Legal Concerns*, 23 RICH. J.L. & TECH. 2, 14–16 (2016) (explaining that some states require businesses to notify the attorney general in the event of a breach, some require a

Union recently enacted the General Data Protection Regulation ("GDPR"), in May 2018, which is a lengthy answer to a lot of data privacy concerns.[18] The GDPR allows consumers to request their data be deleted from the hands of companies, requires companies to notify consumers when their information is breached, and clearly defines the repercussions for companies that do not comply with all of the provisions.[19] GDPR's impact, while only having been enacted for a brief period of time, is already affecting global corporations, because they need to ensure they are compliant with GDPR's requirements in order to continue doing business on a regular basis in the European Union.[20]

Only with enacting similar legislation to the GDPR in the United States, combined with defining what security standards should be for IoT devices, can consumers sleep soundly at night, knowing they are protected if one of their devices is breached. In Part II, this Note will map out the history of data breaches, how companies and consumers are equally affected, and what companies are doing currently to help curtail breaches from occurring. This section will include an in depth look into the rise of cloud computing and how companies rely on cloud computing for data storage and security. Following this in Part III, there will be an overview of the components that make up IoT devices, and why security is lackluster on these devices. Finally, current legislation in the United States will be surveyed. After going through the procedural and legal issues that

specific time frame, and most states require businesses to impose an obligation on businesses to use reasonable security to protect consumer data).

[18] *See* Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), *archived at* https://perma.cc/7BLN-ZXHV (giving a high-level overview of GDPR's enactment).

[19] *See id.* (outlining GDPR and its effect on American companies, in that any company that does any business in the European Union must comply with the GDPR regulations); *see also* Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 72 [hereinafter *GDPR*] (subjecting failure to meet the requirements of the Act to the harsh €20 million or 4% of their previous year's revenue penalty).

[20] *See* Satariano, *supra* note 18 (referring to companies like Facebook that have had to deploy thousands of people across all job functions just to make sure that they will not violate the GDPR); *see also* Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S. – Based Business*, FORBES (Dec. 4, 2017), *archived at* https://perma.cc/MGP2-AXFM (suggesting that U.S. companies that have a strong Web presence need to be weary of how they conduct business as it pertains to controlling their customers' information).

consumers face, in Part IV this Note will suggest a security standard for their IoT device manufacturers to follow, and a Balancing Test for the Cybersecurity and Infrastructure Security Agency to use for companies that are hacked despite adhering to this proposed industry standard.

II. History

A. Data Breaches Today

Data breaches have affected billions of people around the world since 2000, despite the fact that the overall amount that companies spend on IT security rose to $93 billion in 2018.[21] Data breaches now cost companies an average of $3.86 million for each breach.[22] Data breaches can occur in a multitude of ways, with varying routes of how a company's security infrastructure is penetrated, how the data is obtained, and the motive behind the hack.[23] One main reason that breaches occur is due to an error in the underlying coding

[21] *See* Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Jan. 26, 2018), *archived at* https://perma.cc/K72S-GUVR (outlining companies that have been breached in the last twenty years with the number of people effected ranging from 22 million to 3 billion). Such companies included here are Equifax, Yahoo, Target, and Uber—four high profile companies that were heavily scrutinized after their breaches. *Id*. *See also* Susan Moore, *Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017*, GARTNER (Aug. 16, 2017), *archived at* https://perma.cc/3HAX-PVSV (highlighting that $86.4 billion will likely go towards the security testing market, security services, and IT outsourcing); *see also* Tova Cohen, *Microsoft to continue to invest over $1 billion a year on cyber security*, REUTERS (Jan. 26, 2017), *archived at* https://perma.cc/W2XQ-LBQV (articulating that a company as large as Microsoft invests over $1 billion a year on cybersecurity just for themselves). Spending has increased because of the rise in popularity of cloud computing. *Id.*

[22] *See* Herb Weisbaum, *The total cost of a data beach—including lost business—keeps growing*, NBC NEWS (July 30, 2018), *archived at* https://perma.cc/5RZJ-95RL (showing that the costs of these breaches mostly results from technical investigations, regulatory filings, lost business, negative impact on reputation, and employee time spent on recovery).

[23] *See* Marian K. Riedy & Bartlomiej Hanus, *Yes, Your Personal Data is at Risk: Get Over it!,* 19 SMU SCI. & TECH. L. REV. 3, 12−13 (2016) (explaining that the most common causes of a breach include intentional malicious activity, accidental publication, and lost or stolen computers).

of the security software.[24] Part of the reason that breaches occur is because companies may still be using "legacy" (outdated) hardware that requires difficult, intricate updates (also known as "patching") that may be incompatible with any modern components in a company's infrastructure.[25]

B. Cloud Computing for the Modern Company

Companies have various options to protect the data held in their networks, such as traditional hardware like firewalls; however, companies are increasingly migrating to a cloud based model, due to its elasticity and low maintenance costs.[26] Cloud computing takes

[24] *See id*. at 13 (inferring that this is human error, and regardless of whose fault it is, it is still a vulnerability); *see also* Sarah Perez & Zack Whittaker, *Everything you need to know about Facebook's data breach affecting 50M users*, TECHCRUNCH (Sept. 28, 2018), *archived at* https://perma.cc/EK2Z-D4ZC (illustrating the way hackers gained access to Facebook's most recent data breach was via three vulnerabilities in their video uploader feature that Facebook personnel introduced themselves).

[25] *See* Buttrick et al., *supra* note 17, at 24−25 (suggesting that in order to impede cybercrime a company has to constantly be updating its actual IT infrastructure, including the hardware, operating system, and security patches). The authors go on to explain that a cybercriminal is able to gain access to a company's network via older software, as a result of them not keeping up to date on patches. *Id*. *See also* Katherine Britton, *Handling Privacy and Security in the Internet of Things*, 10 J. INTERNET L. 3, 4 (2016) (alluding to the fact that it is difficult to patch an entire legacy system without having to replace the entire system itself); *see also* Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. TECH. L. & POL'Y 229, 253 (2011) (explaining that employee error may cause data breaches).

[26] *See* Quentin Hardy, *'Where Does Cloud Storage Really Reside? And Is It Secure?'*, N.Y. TIMES (Jan. 23, 2017), *archived at* https://perma.cc/3YTZ-7K28 (giving a basic breakdown on cloud storage). Instead of personal data being stored on your own physical, personal devices, such as a laptop, your information is stored on servers owned by massive companies, but is made readily available to you through the internet. *Id.* It is important to point out that the idea of cloud computing to someone without any experience with it is incredibly complex, but the overall concept is attainable. *Id.* Essentially, companies are deciding to ditch the traditional model of housing and owning their own physical servers and data warehouses. *Id.* Companies are instead hiring other companies such as Amazon and Microsoft to hold their data, give them environments to test applications on, use as back up services, and more. *Id.* The benefits are endless, but cannot be adequately discussed further in this Note. *See* Steve Ranger, *What is cloud computing? Everything you need to know about the cloud, explained*, ZDNET (Dec. 13, 2018), *archived at* https://perma.cc/VK56-443F

away the need for companies to manage their IT infrastructure in a physical on premise datacenter, thereby outsourcing the burdensome maintenance to a company like Amazon Web Services.[27] The security aspects of cloud computing are favorable for many companies – it takes away the pressure of companies needing their own security processes in place, because they have entrusted the cloud service provider to monitor and maintain their systems at all times in a central environment, or data center.[28] Despite the advantages of cloud computing for companies, problems arise with IoT devices because they are constantly gathering data that brings a new stream of traffic to a network, in addition to a company's normal network traffic.[29]

(breaking down in depth what cloud computing entails, the differences between Public, Private, Hybrid cloud structures, IaaS, PaaS, and SaaS).

[27] *See Definition of: software stack*, PCMAG (Sept. 1, 2019), *archived at* https://perma.cc/4GA5-UL2E (outlining the way that the software stack is designed to function); *see also Types of Cloud Computing*, AWS-AMAZON (Sept. 9, 2019), *archived at* https://perma.cc/6QPR-W3PC (showing how the three main cloud models, IaaS, PaaS, and SaaS, represent each layer of the software stack, and how a company may choose one model over another). Amazon Web Services ("AWS") is Amazon's cloud computing arm and is currently a leader in the industry. *See Types of Cloud Computing*, *supra*. The benefits of cloud computing are palpable; it allows cash-strapped emerging growth startups for example, to pay Amazon to manage cloud-based servers, storage space, and bandwidth to run their entire IT infrastructure. *Id.* By paying only for the amount of cyber-space in the cloud that are appropriate for their business, it alleviates the need for traditional physical hardware, which requires lots of square footage that increases proportionately with a company's growth. *Id*.

[28] *See* Zach Lanich, *The Benefits Of Moving To The Cloud*, FORBES (May 19, 2017), *archived at* https://perma.cc/5XTR-ML3Y (highlighting that all cloud data centers, such as Amazon's AWS, are designed with the highest level of protection, using only industry best practices for security). The article goes on to explain that the CIA made a $600 million purchase with AWS; clearly showing their confidence with AWS securing their data. *Id. See also* Michael Blanding, *How Amazon Web Services Changed the Way VCs Fund Startups*, FORBES (May 10, 2017), *archived at* https://perma.cc/Z8C6-V8PA (paraphrasing that startups rely on the capabilities of AWS because it "has allowed startups to cheaply rent server space and development tools in the cloud and scale up as needed rather than purchasing their own expensive hardware and software").

[29] *See* Christine Parizo, *Cloud security and IoT are the new peanut butter and jelly*, TECH PRO RESEARCH (Oct. 3, 2017), *archived at* https://perma.cc/L9X4-K5LE (suggesting that a company segregate their IoT traffic from normal network traffic because many current cloud computing providers are still developing proper security for IoT devices); *see also* Nick Feamster, *Mitigating the Increasing Risks of an Insecure Internet of Things*, 16 COLO. TECH. L.J. 87, 99–100 (2017) (proposing that

Cloud computing is gaining in popularity, but despite its attractive utilitarian purposes, there are still security risks and ambiguities associated with it that do not get enough attention.[30] These issues include cloud service providers outsourcing some of their needs to other cloud service providers, making for an unclear boundary for who is responsible for the data.[31] Large global corporations that have the financial and legal resources to spend a lot on cloud computing will have greater leverage to ensure that their information is secure, whereas smaller companies are at a disadvantage purely from an economies of scale perspective.[32] Companies that contract with cloud service providers are able to recover some liability relief in the event of a breach, but the main liability is still in the company's hands.[33] There are a variety of factors that contribute to how data is stored in

if consumers were able to control and monitor the devices that are being used via their home network firewall it would allow them to have more "visibility and control over the traffic flows that these devices send").

[30] *See* J. Nicholas Hoover, *Compliance in the Ether: Cloud Computing, Data Security and Business Regulation*, 8 J. BUS. & TECH. L. 255, 260–66 (2013) (describing the risks of cloud computing for security purposes). This includes how massive public clouds are easy targets for hackers because they are delivered online. *See id.* at 261. Additionally, the number of pathways hackers can use to gain access to attack the cloud, as well as the fact that the cloud is distributed and internet-based leaves them open for attacks. *See id.*; *see also* Matt Day & Sarah Frier, *Amazon Cloud Storage Dilemma Exposed in Facebook's Latest Leak*, BLOOMBERG (Apr. 3, 2019), *archived at* https://perma.cc/5ABH-F57T (recognizing that even AWS is prone to simple errors that may leave companies at risk).

[31] *See* Hoover, *supra* note 30, at 262 (highlighting that this makes customers of cloud service more demanding about who is controlling their information).

[32] *See* H. Ward Classen, *Cloudy with a Chance of Rain: Avoiding Pitfalls in Cloud Computing*, 45 MD. B.J. 18, 21 (2012) (explaining that cloud service providers achieve the best economies of scale when all of their customers are standardized); *see also* Kevin McGillivray, *Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU*, 17 TUL. J. TECH. & INTELL. PROP. 217, 228 (2014) (emphasizing the cost benefits of cloud computing for startups).

[33] *See* Harshbarger, *supra* note 25, at 238 (explaining that cloud computing companies do have to make sure their security is to a high standard to ensure that companies will want to entrust their sensitive data with them). These companies lay out how a cloud provider should contract with its clients; primarily, by providing that they will be compliant with all applicable data security laws, ensuring they have insurance, and being aware of any strict liability clauses. *Id.* at 249–52.

the cloud, what solution is being used, what kind of data it is, and how it's encrypted – all of which are major concerns for customers.[34]

C. Technical Components of IoT Devices

The inherent allure for consumers to invest in IoT devices is because they allow for sensors or devices to "talk" to the cloud and monitor routine activities, all of which is made capable by the specific hardware components in each device.[35] All of the components in a device, which are often designed, built, and assembled by different companies around the world, tend to not work very cohesively together.[36] What escalates this problem is that any compromises in the device will go unnoticed because it is the software underneath the surface that will be breached, not the physical hardware; so the device will seemingly function as normal until the user recognizes the issue.[37] The sheer complexity in the underlying code to operate computer software is vast, and with the amount of users that are using these devices, there are more access points for potential attacks.[38] With the

[34] *See* McGillivray, *supra* note 32, at 234 (proposing that all of these factors allow for security breaches and loss of customer data). The fact that there is a lot of transparency as to who is controlling the data in flight and what servers are controlling the data along the way causes concern for customers. *Id.*

[35] *See* Britton, *supra* note 25, at 3 (summarizing that IoT components include RFID, or Radio-frequency identification, are "low-energy electronic circuits that can be imbedded into any object to make it able to interact with RFID readers"). Other technologies include NFC (near-field communications) that is also a low-power wireless way "to transfer small amounts of data between devices," and M2M transmissions, which "refer to direct communications between machines" such as wearable devices and a monitoring hub. *Id. See also* Calum McClelland, *IoT Explained – How Does an IoT System Actually Work?*, LEVEREGE (Oct. 29, 2016), *archived at* https://perma.cc/M8YS-F53Y (breaking down an IoT device, to include sensors (such as a camera or GPS), connectivity (Wi-Fi, Bluetooth, etc.), data processing (the software that does some sort of processing), and some sort of user interface, which allows the user to modify or check in on the device).

[36] *See* Sarah Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 167 (2018) (explaining that because the "market has prioritized features and cost over security," IoT devices' security features are often lackluster because they are based off of different international standards of security).

[37] *See id.* at 167–68 (recognizing that the device will still serve its purpose even after the software becomes insecure).

[38] *See* Britton *supra* note 25, at 4 (suggesting that many devices that are connected may not have strong encryption due to trying to keep costs down, and there being

number of variables involved with how an IoT device gets from the retailer to your hands, how the device is used, and how it's connected to a wireless network, the vulnerabilities are endless and gives hackers ample access to implement an attack.[39]

The underlying capabilities that allow a device to have "smart" functions are inherently cheap to build into a device, and are becoming more prevalent in ordinary devices that do not necessarily require these capabilities.[40] The rationale behind ordinary household items like children's toys and kitchen toasters to have "smart" functionality is

---

little incentive for developers to make security a priority). Commercial software could have 20 to 30 bugs for every thousand lines of code, so 50 million lines of code could mean 1 million potential errors that could lead to a breach. *See id. See also* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 11 (2015) (inferring that algorithms are self-learning and are a component in many IoT devices because "the power of these devices, in essence, is their ability to sample information millions of times more often than we as people can"); *see also* Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy you are Looking for,* 16 Duke L. & Tech. Rev. 18, 34–37 (2018) (explaining that algorithms are self-learning and are a component in many IoT devices).

[39] *See* Britton, *supra* note 25, at 5 (implying that the weakest link in an IoT system will be the weak spot where a hacker could gain control of the device). So, if a consumer has a litany of products ranging from smart light bulbs, security cameras in their home, applications on their smart phone, and smart wearable watches, a hacker has many ways they can infiltrate and wreak havoc on a consumer's life. *Id. See also After the Gold Rush*, *supra* note 1, at 98–99 (explaining that if one IoT device that has vulnerabilities is on a network it will make other devices connected on the same network equally vulnerable). Additionally, it is easy for hackers because many IoT devices are connected via home routers that are notoriously unprotected. *See id.*; *see also Careful Connections: Building Security in the Internet of Things*, FTC (Jan. 17, 2019) [hereinafter *Careful Connections*], *archived at* https://perma.cc/E2GX-46BL (outlining the variables involved in manufacturing IoT devices).

[40] *See* Danny Palmer, *Internet of Things security: What happens when every device is smart and you don't even know it?*, ZDNET (Mar. 20, 2017), *archived at* https://perma.cc/3EP9-B2DV (proposing that the processors for IoT devices will eventually become free, and normal household items will have inferior connectivity problems); *see also* Brett Jurgens, *Redefining the Smart Home*, FORBES (June 7, 2018), *archived at* https://perma.cc/QLX7-G67V (articulating that "just because a device can be remade 'smart' doesn't mean it adds inherent value"); *see also* Thierer, *supra* note 38, at 5–6 (highlighting that because of advances in circuits and software, it's incredibly easy to put IoT components like microchips, sensors, and cameras into devices).

ultimately to let companies and industries collect more data, and the trend to have everything connected at all times.[41] One reason why security is an issue with IoT devices is that they are being manufactured by consumer goods companies that are not traditionally known for making computer hardware or software.[42] In the past, security issues have been addressed after software has been implemented; but with IoT devices that are constantly "on," that standard is no longer practical.[43] Unlike computers, tablets, and our smartphones that have security built directly into the device itself, IoT devices have "little-to-no protections" that have been implemented into their operating systems.[44] The same reason that makes IoT

[41] *See* Jane E. Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 460 (2018) (highlighting that devices collect sensitive data, including health data from children's toys); *see also* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 426 (2018) (recognizing that "data generation and collection does not end after the consumer purchases a device online or in a store, but instead increases once the consumer begins to use the IoT device, as well as the websites and mobile applications that are frequently required to access and operate the device"); *see also* Melissa W. Bailey, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1053 (2016) (suggesting that the motivation behind an IoT manufacturer collecting data is that it provides "location, biorhythmic data, fitness information, driving habits and more"). All of this information is "valuable to employers, insurance companies, or other third parties, and IoT manufacturers are increasingly capitalizing on this value by selling the data to third parties." *Id.*

[42] *See* Peppet, *supra* note 2, at 135 (inferring that engineers that are making IoT devices at companies that typically do not focus on these products may be inexperienced with data-security problems).

[43] *See id.* at 136 (suggesting that because IoT devices are constantly connected, proper security measures need to be built in from the ground up); *see also* Dalmacio V. Posadas, Jr., *The Internet of Things: The GDPR and the Blockchain May be Incompatible,* 21 J. INTERNET L. 1, 19 & 20 (2018) [hereinafter *The Internet of Things*] (recognizing that devices like an Amazon Echo and Google have microphones that are always on and listening, which is susceptible to hacking). Furthermore, because IoT devices engage in "machine learning," which allows them to "quickly ident[ify] patterns as IoT users engage with the device," and the hardware components in the devices that makes each user distinguishable from one another, allowing users to be tracked. *See The Internet of Things*, *supra.*

[44] *See* Wendy Zamora, *Internet of Things (IoT) security: what is and what should never be*, MALWAREBYTES LABS (Dec. 22, 2017), *archived at* https://perma.cc/U8U6-8BFR (explaining that because of the cost of security for a developer and the speed at which these devices need to get to market, security is often lackluster); *see also* Peppet, *supra* note 2, at 135–36 (agreeing that the operating system of an IoT device

devices so popular among consumers, the fact that they are often small and sleek, is also why security is sub-par on these devices – it's difficult to build sufficient security into such a small physical space.[45]

D. Hacks in the Least Likely Places

Hacks have occurred in innocent consumer IoT devices such as children's toys, and also automobiles, suggesting that consumers and manufacturers alike are tremendously unaware of how vulnerable IoT devices can be.[46] The primary reasons or motivations a hacker

is not designed to have constant patches and updates like a laptop or smart phone is; they are "often less malleable and robust" which leads to inferior security); *see also* Terrell McSweeney, *Consumer Protection in the Age of Connected Everything*, 62 N.Y.L. SCH. L. REV. 203, 212–13 (understanding that many IoT devices do not have adequate security built into them, and the problems that are posed when the consumers are not aware that a slightly cheaper product may have big implications regarding how secure it is).

[45] *See* Peppet, *supra* note 2, at 135–36 (highlighting that due to the small stature of the devices, battery life is often limited, and therefore, cannot support added security such as encryption). Furthermore, these devices are designed to simply be sent to market, without an additional afterthought that they should be updated constantly and retooled. *Id.*; *see also* Andrea M. Matwyshyn, *CYBER!*, 2017 B.Y.U. L. REV. 1109, 1117–19 (2017) (outlining that when Sony was breached in December 2014, it became clear that they had a long history of subpar security and affected the company and its customers significantly).

[46] *See* Kirtley & Memmel, *supra* note 41 (illustrating one consumer hack example where a father went into his baby's bedroom, heard an unfamiliar male voice saying "wake up little boy, daddy's looking for you," then realized that someone had hacked into the baby monitor and was spying on his family); *see also* Beale & Berris, *supra* note 36, at 164–65 (highlighting in 2015 when Fiat Chrysler claimed that 1.4 million of their Jeep Cherokees were hacked publicly, showing that the hackers were able to "turn the steering wheel, briefly disable the brakes, and shut down the engine," all by using the car's infotainment system as the medium for access); *see also* Sarah Ensenat, *Smart Baby Monitors: The Modern Nanny or a Home Invader*, 26 CATH. U. J. L. & TECH. 72, 72 (giving an overall view of the baby monitor hacking example); *see also* Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons From Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761, 805–06 (2017) (showing another example of how prone to hacks IoT devices are); *see also* Donica Phifer, *BABY MONITOR HACKED: CHILD THREATENED WITH KIDNAPPING, OTHER LEWD COMMENTS MADE BY HACKER*, NEWSWEEK (Dec. 19, 2018), *archived at* https://perma.cc/FC9Z-56MS (highlighting a recent baby monitor hack where the hacker threatened to kidnap the baby through the baby monitor, causing hysteria for the parents); *see also* Aimee Picchi, *Your kids' toys could be spying on your family*, CBS NEWS (Dec. 7, 2016),

will decide to attack an entity or consumer include "terrorism, national aggression, pranking, election tampering, and money extortion."[47] The rise in popularity of medical devices with IoT capabilities is also expanding, with similar security risks as other devices, but with potential for more severe consequences.[48] People are racing to make their homes "smart," with the use of IoT devices to monitor and manage security, lightbulbs, and refrigerators – connected via Wi-Fi and managed via a smart phone, all with glaring vulnerabilities.[49]

E. Cybersecurity Legislation in the United States

archived at https://perma.cc/X2MM-RL5J (explaining that children's toys can be hackable "because any smartphone or tablet with 50 feet can connect via Bluetooth, with no authentication code needed, the complaint asserts").

[47] *See* Beale & Berris, *supra* note 36, at 168 (explaining some people's motivations behind hacking, including the "fourteen-year-old [who] hacked a train system for a prank; the Iranians hacked a dam apparently as an act of terrorism; the extortionists attacked the 911 system for money; and the disgruntled employee hacked into cars sold by his former employer for revenge").

[48] *See* Mauricio Paez & Kerianne Tobitsch, *The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues*, 62 N.Y. L. SCH. L. REV. 217, 241 (2018) (suggesting that electronic medical devices that are connected to one another have risks such as a patient receiving the wrong amount of medication, which could lead to death); *see also* Beale & Berris, *supra* note 36, at 166 (highlighting that researchers have already found and exposed vulnerabilities in implanted medical devices).

[49] *See After the Gold Rush*, *supra* note 1, at 85−86 (reviewing an FTC lawsuit against TRENDnet in 2013, an IoT company that produces home webcam services because hackers were able to gain access to the live feed displaying "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"); *see also* David Z. Bodenheimer, *The Internet of Things' Swelling Technology Tsunami and Legal Conundrums*, 12 ABA SCITECH LAW. 4, 5 (2016) (explaining that a smart home can "permit remote control of lighting, security, HVAC (heating, ventilating, and air conditioning), and appliances" and lighting systems can be controlled from a smartphone); *see also* Andrew Gebhart, *Google Home's 2018 in Review: Owning the Smart Home*, CNET (Dec. 27, 2018), *archived at* https://perma.cc/VJ6T-VYAV (paraphrasing that Google is making a push for its smart home, and its new Google Assistant can work with 5,000 devices, and works with every major brand, so you can connect your home via Google Assistant to any device you already own); *see also* Andy Greenberg & Kim Zetter, *How The Internet of Things Got Hacked,* WIRED (Dec. 28, 2015), *archived at* https://perma.cc/T3MF-KZY8 (showing how a Samsung smart fridge was insecure, allowing consumers' Gmail credentials open to hackers).

Legislation in the United States pertaining to data breaches is regulated by specific industry statutes, and they do not give consumers a legitimate path to a proper cause of action.[50] One of the main federal statutes is the Cybersecurity Act of 2015, which regulates the "authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats."[51] The Cybersecurity Information Sharing Act of 2015, which falls under Title I of the Cybersecurity Act of 2015, was greeted with a lot of criticism, mostly because it made consumers' private information more widely available to the government and organizations like the National Security Agency ("NSA") and Central Intelligence Agency ("CIA").[52] The Federal Trade Commission ("FTC") is the federal agency that is responsible for bringing actions against companies that do not have proper security standards or

[50] *See* Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L. J. 555, 559−60 (2018) (highlighting that the Health Insurance Portability and Accountability Act of 1996 and the Gramm-Leach-Bliley Act set standards for storing medical information and financial institutions).

[51] *See* 6 U.S.C.A § 1503 (2015) (articulating that a private entity can operate a defensive measure when it's applied to "an information system of such private entity in order to protect the rights or property of the private entity"); *see also*; *see also* Jocelyn Aspa, *What is the Cybersecurity Act?*, INVESTINGNEWS (Jan. 16, 2018), *archived at* https://perma.cc/H6YJ-ZFRQ (explaining that the act's main purpose was to "detect and prevent cybersecurity threats or security weakness" and "to protect the privacy rights of an individual by ensuring that personal information is not shared or divulged unnecessarily"); *see also* Orin Kerr, *"How does the Cybersecurity Act of 2015 change the Internet surveillance laws?"*, WASH. POST (Dec. 24, 2015), *archived at* https://perma.cc/TTR4-CH68 (giving an overview of the act, which allows entities to monitor their networks to protect them from vulnerabilities if they have subject intent). This gives them the authority to use defensive measures and the ability to share data. *See* Kerr, *supra*.

[52] *See The Cybersecurity Act of 2015*, SULLIVAN & CROMWELL LLP (Dec. 22, 2015), *archived at* https://perma.cc/5KTG-VA2S (recognizing that the Cybersecurity Act of 2015 contains four titles, the first being the Cybersecurity Information Sharing Act of 2015); *see also* Graeme Caldwell, *Why You Should Be Concerned About The Cybersecurity Information Sharing Act*, TECHCRUNCH (Feb. 7, 2016), *archived at* https://perma.cc/MZU6-NCF6 (highlighting that companies like Amazon, Apple, Dropbox, Google, Facebook, and Symantec all came out with public statements expressing their disdain for the legislation).

misrepresent their data.[53] But, there is not a statute that actually gives the FTC this authority.[54]

In November 2018, President Trump created the Cybersecurity and Infrastructure Security Agency ("CISA"), finally giving the United States a federal agency dedicated to cybersecurity.[55] The CISA is designed to provide comprehensive cyber protection, infrastructure resilience, and emergency communications, all for the purposes of "collaborating among a broad spectrum of government and private sector organizations."[56] While the CISA was developed to be under the Department of Homeland Security to regulate the public sector, it will also be used to regulate private companies as well.[57]

---

[53] *See About the FTC*, FEDERAL TRADE COMMISSION (Feb. 21, 2019), *archived at* https://perma.cc/US8C-XTVW (stating that the FTC's mission is to protect "consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity"); *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement*, and *Rulemaking Authority*, FEDERAL TRADE COMMISSION (Apr. 2019) [hereinafter *Brief Overview of FTC*], *archived at* https://perma.cc/57D8-PDE6 (explaining that the FTC "must still seek the aid of a court" when they believe an entity has violated regulation rules).

[54] *See* Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 188 (2017) (recognizing that the FTC "is authorized to regulate unfair or deceptive practices," and it was not until 2014 that their authority extended to regulate data security as an unfair practice).

[55] *See* Catalin Cimpanu, *Trump signs bill that creates the Cybersecurity and Infrastructure Security Agency*, ZDNET (Nov. 16, 2018), *archived at* https://perma.cc/YYX4-WQ2M (recognizing that the CISA is an agency inside of the Department of Homeland Security, and is "in charge of overseeing civilian and federal cybersecurity programs"); *see also* Cat Zakrzewski, *The Cybersecurity 202: Trump set to make a new DHS agency the top federal cyber cop*, WASH. POST (Nov. 16, 2018), *archived at* https://perma.cc/M8CF-KWAS (highlighting that the CISA will "make it easier for the private sector to work with the government on cybersecurity threats").

[56] *See CISA*, DEPT. OF HOMELAND SECURITY (Feb. 19, 2019), *archived at* https://perma.cc/6KXD-TNG7 (understanding that the CISA is there to lead "the national effort to *defend* critical infrastructure against the threats of *today*, while working with partners across all levels of government and in the private sector to *secure* against the evolving risks of *tomorrow*").

[57] *See* Zakrzewski, *supra* note 55 (paraphrasing that the government and private sector will collaborate together on cybersecurity issues). The CISA was also created in response to the Russian hacking allegations during the 2016 Presidential Election. *Id.*

Each state has laws that "require companies to notify customers, regulators, and credit bureaus of data breaches."[58] The details of what information is actually disclosed is also determined by a state by state jurisdiction basis, with varying requirements from each one.[59] The problem with a mix of state and industry-specific federal legislation is that companies who do business in all states have to decipher and comply with every states' laws and determine what they are obligated to do, instead of having one federal statute to adhere to.[60] Federal acts such as HIPAA and the Fair Crediting Report Act ("FCRA") are designed to regulate the privacy of medical records and consumer information respectively.[61] Thus, in the event that a consumer is breached via an IoT device affecting these subject matters, a consumer could recover under these statutes.[62] California is currently the state leader in passing and enacting strict cybersecurity legislation, partially because of the number of large internet based companies that are headquartered there.[63] With federal legislation lacking, IoT devices becoming more advanced and popular, and the known fact that there is no such thing as "perfect security", there are many concerns about how consumers can protect themselves in the event that one of their IoT devices is compromised.[64]

---

[58] *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1014 (2017) (explaining that some states are stricter than others). For instance, North Dakota requires notification of the disclosure of personal information like mother's maiden name. *Id.*

[59] *See id.* at 1015 (illustrating that Massachusetts does not require the data breach notification to include specific information about the content of the breach).

[60] *See id.* at 1014−15 (suggesting that this will be a complex and time-consuming process, particularly for small and midsized companies that have small information security and legal teams).

[61] *See* Alexander H. Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J. L. & SOC. PROBS. 263, 275 (2017) (highlighting that these statutes, although not explicitly designed to regulate IoT devices, can be used to compensate an injured consumer).

[62] *See id.* (noting how some state statutes provide remedies for injuries caused by IoT devices, but they do not cover injuries from the actual sensor data in the devices).

[63] *See* Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 205 (2017) (listing companies like Amazon, Apple, and Google that have been regulated because of California's online privacy and data collection laws).

[64] *See id.* at 207−08 (suggesting that federal change has not been initiated because privacy advocates and companies that sell consumer information "cannot settle on whether to support a legislative solution to fill the gaps in the current framework or

III. Facts

A. Consumers Have Nothing to Stand On – Article III Standing & Data Breaches

Plaintiffs who seek to hold a company liable for a data breach face extensive legal procedural issues – namely, satisfying Article III standing.[65] In *Clapper*, the Supreme Court held that despite the plaintiff taking costly and burdensome measures to "protect the confidentiality of their communications," because they took these measures based on "hypothetical future harm," they did not satisfy the impending injury requirement.[66] There is a continuing split among the Federal Court of Appeals about how to deal with Article III standing in data breach cases, and based on *Clapper*, the Supreme Court could very well lean either way in its next decision.[67] On one side, the Seventh and Ninth Circuit have ruled on cases and have granted

allow the data industry to self-regulate" and they cannot even manage to clearly define what "internet tracking" even means).

[65] *See* Clapper v. Amnesty Intern. USA, 568 U.S. 398, 409 (2013) (holding that in order to establish Article III standing, an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling"); *see also* Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 66 (2017) (highlighting that many data breach plaintiffs rely on an argument that there is an "objectively reasonable likelihood" that there will be *future* financial harm/injury/identity theft). The court in *Clapper* rejected this "objectively reasonable likelihood" standard. *See* Bugni, *supra*.

[66] *See Clapper*, 568 U.S. at 416 (alluding that the plaintiffs cannot manufacture standing and that they did not face a real threat of having their privacy compromised). *But see* Christiana Modesti, *Incentivizing Cybersecurity Compliance in the New Digital Age: Prevalence of Security Breaches Should Prompt Action by Congress and the Supreme Court*, 36 CARDOZO ARTS & ENT. L.J. 213, 228 (explaining that the presence of "emotional and psychological harms" along with monetary costs are factors to help win an Article III standing argument).

[67] *See* Mank, *supra* note 9, at 1327−28 (suggesting that if a plaintiff can show actual injury then standing will be found). The Seventh Circuit's decision in *Remijas* could help these kinds of plaintiffs. *Id.*; *see also* Kim, *supra* note 11, at 558 (explaining that the Seventh and Ninth Circuits have decided in cases that the threat of future harm is sufficient to establish standing). Kim suggests that even though *Clapper* did not make stricter standing requirements, it has been read as doing exactly that. *See* Kim, *supra* note 11, at 558. Accordingly, some United States District Courts have dismissed data breach cases for lack of standing. *Id*. at 561−62.

standing where there was no real injury-in-fact, but the increased risk of identity theft was sufficient to find standing.[68] Alternatively, the Third Circuit has held that the future risk of identity theft is insufficient to meet the requirements for Article III standing, as seen in *Reilly v. Ceridian Corp.*[69] If a plaintiff's impending future injury does not occur within the couple years that is generally required for standing, the courts will be more reluctant to find injury in fact, essentially negating their injury argument.[70]

B. Contract Law as a Means of Seeking Recourse

When plaintiffs have been able to hop over procedural barriers of entry to litigate a data breach claim, using a breach of contract argument has been inadequate.[71] Breach of implied contract claims arguments have been tried, but to no avail.[72] In many states, in order to succeed on a breach of contract claim, one requirement is showing

[68] *See* Kim, *supra* note 11, at 558−59 (highlighting the *Krottner v. Starbucks* case, where an employee laptop was stolen from a Starbucks and the increased risk of identity theft was sufficient to constitute injury-in-fact).

[69] *See id.* at 569 (clarifying the circuit split among the Court of Appeals); *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (holding that Article III standing was not found).

[70] *See* Bugni, *supra* note 65, at 70–71 (inferring that the clock starts ticking and when more time passes "without the alleged future harm actually occurring," the plaintiff's argument is not as strong, given that their cause of action is based on future harm that never actually occurs).

[71] *See* Justin C. Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 WM. & MARY L. REV. 975, 992–93 (2016) (suggesting that in a data breach where one's information is stolen via an electronic payment device in a retail store, the banks have a contract between them and the merchant, and they have to "persuade the court to recognize the issuing bank as a third-party beneficiary to the contract, thus allowing them to bring a breach of contract claim").

[72] *See* Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 632–33 (7th Cir. 2007) (arguing that the defendant did not adequately protect the plaintiff's personal confidential information, and under Indiana law, you cannot bring a breach of contract claim unless you are alleging cognizable damages); *see also Reilly*, 664 F.3d at 38 (alleging breach of contract resulting from the increased cost of monitoring their credit activity post-security breach); *but see* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (affirming the District Court's decision that there was no breach of an implied contract because plaintiffs did have sufficient standing under Article III).

they have suffered actual monetary damages.[73] Some plaintiffs have succeeded under an unjust enrichment contract theory, which is an equitable theory that requires the plaintiff having "actually conferred an unjust benefit on the defendant."[74] Contract theory also provides a theory of "unconscionability," which allows for recovery if there is inherent unfairness in a procedural and substantive manner.[75] Nonetheless, when a defendant has not used proper security standards to secure their systems and they get hacked, the ease of bringing a breach of contract claim will be much easier.[76]

C. Tort Law as a Means of Seeking Recourse

Under a traditional tort theory such as products liability, most customers have to accept an End User License Agreement ("EULA") when they purchase an IoT device, which allows for companies to disclaim liability for damages incurred by those devices.[77] These EULA contracts are like a double edged sword; in most cases, if a consumer wants to access the full array of features in their IoT device they have to sign a EULA, but in doing so, they give up the right to

[73] *See* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, *1, at *7 (N.D. Ill. July 14, 2014) (highlighting that damages are an essential element of a breach of contract claim).

[74] *See* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion and the Modern Data Breach*, 69 FLA. L. REV. 771, 814 (2018) (explaining that in order for a plaintiff to succeed on an unjust enrichment action, they must have bought a product or service from the data custodian, or entity that received personal information from the plaintiff).

[75] *See* Kirtley & Memmel, *supra* note 41, at 508 (explaining that unconscionability will also show an inference there is an unequal bargaining power between the two parties, such as a massive company versus the average consumer).

[76] *See* Patco Const. Co., Inc. v. People's United Bank, 684 F.3d 197, 214–15 (1st Cir. 2012) (emphasizing that because the defendant bank clearly did not use "commercially reasonable" security standards, and in conjunction with UCC Article 4A, there may be higher standards imposed on the bank). This case explains that the bank authorized fraudulent several withdrawals from the plaintiff's account for over $500,000 total, and had multiple security measures that it could have implemented, and chose not to. *Id*. at 204.

[77] *See* Kirtley & Memmel, *supra* note 41, at 507 (suggesting that EULA contracts and software licenses make it difficult for consumers to recover damages when their products do not work as anticipated, or have security flaws).

sue for damages that are caused by that device.[78] A plaintiff may argue that their breach was caused by the negligence of a company that had some involvement in allowing the breach to occur – such as the manufacturer of an IoT device, their bank, or their retailer – but this is difficult to prove.[79] However, there has been recovery by a plaintiff asserting negligence where the defendant causes an identifiable class of people injury where it owes a duty of care.[80] As of now, there is not any kind of tort liability standard that gives consequential damages for a company that has "inadequate or negligent cybersecurity measures."[81]

Injured consumers in potential tort claims where IoT devices are involved are at a disadvantage based on the sheer fact that IoT devices are incredibly complex, and require expertise to dissect and determine how the data was actually compromised.[82] Comparatively, in the event of a truly massive data breach, such as the Equifax breach, it is nearly impossible to determine if it was *that* breach that caused harm to one specific consumer, or if it was one of the countless prior

[78] *See id*. at 507–08 (highlighting the EULA agreement that Nest home camera systems require their customers to sign); *see also* Elvy, *supra* note 41, at 444 (discussing that the privacy policies that come with IoT devices permit companies to "share consumer data with various third parties"). Companies such as Nest, Amazon, and Apple have provisions in their privacy policies that state when consumer data may be transferred or used. *See* Elvy, *supra* note 41, at 444.

[79] *See* Mills & Harclerode, *supra* note 74, at 807−08 (articulating that the plaintiff will argue that the company had a duty to "exercise reasonable care," and that the economic loss rule will typically preclude recovery by the plaintiff). Furthermore, when there is not actual financial harm suffered, there can be no economic loss. *Id*. at 809.

[80] *See* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013) (recognizing that the "identities, nature, and number of victims are easily foreseeable"); *see also* Meal, *supra* note 10, at 6 (articulating the difficulty for a plaintiff to prove that the defendant company owed them a duty of care).

[81] *See* Paul Rosenzweig, *When Companies Are Hacked, Customers Bear the Brunt. But Not for Long.*, THE NEW REPUBLIC (Oct. 15, 2013), *archived at* https://perma.cc/M4TL-LBS8 (elaborating that there has not been any development in a tort like this, but if one were created, it would require the federal government to distinguish what security best practices are, and require them to be adopted by entities that control mass amounts of data).

[82] *See* Kirtley & Memmel, *supra* note 41, at 508−09 (proffering that under traditional laws, it's difficult to figure out when something goes wrong, in addition to if the consumer whose device was compromised should have to prove their injury stemming from the device manufacturer).

hacks before it.[83] Habitual users of IoT devices know how to use their devices, but the vast majority are not aware of potential security vulnerabilities in them, and are not taking the proper measures to ensure that their devices are secure.[84] The worst part about this problem is that consumers are "blindly" trusting the manufacturers of their IoT devices, and most of the time they will not feel the pains of not securing their devices.[85]

D. Current Lack of Federal Legislation

The United States does not have a very organized set of federal laws in place to either compensate the consumer in the event of a breach, or to hold breaching companies liable.[86] Companies are left to rely on industry best practices, such as the 2014 National Institute of Standards and Technology ("NIST").[87] These companies prescribe

[83] *See* Alfred Ng & Erin Carson, *Equifax data hack: What are your legal options?*, CNET (Sept. 8, 2017), *archived at* https://perma.cc/9KRM-2BPR (highlighting that up to 143 million people were affected by the breach); *see also* Brenda R. Sharton & David S. Kantrowitz, *Equifax and Why It's So Hard to Sue a Company for Losing Your Personal Information*, HARV. BUS. REV. (Sept. 22, 2017), *archived at* https://perma.cc/DW63-YTXQ (explaining that in the case of the Equifax breach, because plaintiffs do not directly give Equifax their information, but instead it is "given" to corporate customers, who then relay that information to Equifax). The article explains that it is incredibly difficult to get past the pleading or motion to dismiss stage for most plaintiffs. *See* Sharton & Kantowitz, *supra*.

[84] *See* Feamster, *supra* note 29, at 93 (identifying that people that have simple Internet connections at home are poor at doing the necessary software updates, and they are simply unaware of the "security and privacy risks associated with the devices that they are deploying in their networks").

[85] *See id.* (suggesting that consumers do not have a lot of incentive to take the initiative to secure their devices).

[86] *See* John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 458 (2018) (outlining that the United States system of laws for data breaches and privacy is not unified, and rather, is addressed via federal agencies including the Department of Homeland Security, the Department of Defense, the National Security Agency, and the Federal Trade Commission); *see also* Kosseff, *supra* note 58, at 1026 (recognizing that the United States does not have a Department of Cybersecurity, the responsibilities of cyber security are spread among many agencies, and the most apt cybersecurity professionals are working for the National Security Agency).

[87] *See* Chung, *supra* note 86, at 460 (detailing that it relies on "existing standards, guidelines, and practices" in the industry, and that because technology is constantly

industry standards for how companies should run their IT infrastructure and manage cybersecurity risks, but even that has its flaws.[88] The Cybersecurity Act of 2015 was designed to open up a line of communication with the government and the private sector regarding potential vulnerabilities and cyber threats.[89] However, the CSA neglected to properly define the term "cybersecurity," and critics of it suggest that it gives business entities too much immunization from liability.[90] Ultimately, what this disheveled mess of different agencies, regulations, and statutes allows for is breaching companies to slide by without any major repercussions.[91] Up until November 2018, the United States did not have its own dedicated cybersecurity agency; the closest thing they had is the FTC.[92]

changing and updating at a fast pace, it is difficult to mandate regulations that would not become ineffective so quickly).

[88] *See id.* at 460–61 (distinguishing the problem that arises when companies in the private or public sector have to formulate their own security standards).

[89] *See id*. at 462−63 (suggesting that because the Internet is so open, there isn't a huge benefit to isolate and segregate the private and public sector concerns). *See also* Sarah E. Hsu Wilbur, *What Does this Mean? Examining Legislative Ambiguities in the Cybersecurity Act of 2015 and the Potential for a Future Circuit Split on Interpretation*, 48 SETON HALL L. REV. 275, 289−90 (2017) (explaining that CISA has three sections). The first provision allows companies to monitor their IT systems and data for cybersecurity purposes, the second allows for private entities to have defensive measures to protect their property, and the third allows for liability protection for these entities that choose to volunteer their information with the CSA's requirements. *Id*.

[90] *See* Kosseff, *supra* note 58, at 1021−22 (inferring that the CSA's goals of improving companies' cybersecurity and protecting consumer's privacy rights are not achieved due to the Act's voluntary or open-ended nature despite the CSA requirement to disclose cyber-threats to the government without consumers' personal information attached).

[91] *See id*. at 1030 (asserting that an identified vulnerability may remain open while a company attempts to comply with federal and state procedural requirements); *but see Is it Really 'FDA Approved?'*, U.S. FOOD & DRUG ADMIN. (Jan. 17, 2017), *archived at* https://perma.cc/AAQ2-5JLG (showing how the FDA, a federal agency, approves new drugs and medical devices before companies can market them in interstate commerce, which could be a model for how IoT devices are developed and sold).

[92] *See* Cimpanu, *supra* note 55 (summarizing the recent development of the Cybersecurity and Infrastructure Security Agency); *see also* Kosseff, *supra* note 58, at 1011 (showing that the FTC has regulatory control but no authority to bring a proper cause of action); John W. Chandler, *Historic overview – Federal regulations requiring installation of seat belts*, HMVAC § 1A:3 (2018) (highlighting that in the early 1960s Congress "decided to improve the design and safety features of passenger vehicles by imposing mandatory standards for seat belts"). Congress only

Despite the messy ad-hoc method that the federal government relies upon, some states are taking significant steps forward in their own legislation to give more defined and stronger data protection laws.[93] For instance, the California Consumer Privacy Act, newly passed in California and Massachusetts, amends its own data breach notification law.[94] In order for the United States to protect their own citizens from data breaches caused by corporate entities, or even individual hacks that may become more prevalent on consumers' IoT devices, there needs to be a federal statute passed.[95]

chose to implement these standards as a result of the high death rate caused by car accidents, and the need to reduce traffic accidents, injuries, and deaths to its citizens. *See* Chandler, *supra*. *See also* Nikole Davenport, *Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 289 (2016) (articulating that the FDA has regulatory functions and has published data security guidelines for companies to aim to meet); *see also* Sara Shahmiri, *Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of This New Technology*, 18 TEXAS REV. ENT. & SPORTS L. 25, 30 (2016) (showing in general what the FTC's powers are).

[93] *See* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (Jun. 28, 2018), *archived at* https://perma.cc/6ZZV-HXDV (highlighting the California digital privacy law passed in June 2018 that loosely mimics GDPR regulations). This law grants consumers the "right to know what information companies are collecting about them" and allows consumers to tell companies to delete their information, and not sell or share their data. *Id.*

[94] *See* Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), *archived at* https://perma.cc/6XRE-DUFT (suggesting that the passing of this law will have broad implications because many companies across various sectors that deal with consumer data have California residents as customers); *see also* David M. Brown, *Massachusetts Enacts Significant Changes to Its Data Breach Notification Law*, JDSUPRA (Jan. 11, 2019), *archived at* https://perma.cc/S3JQ-EAFG (outlining the new legislation, which will require complimentary credit monitoring for 18 months if a Massachusetts resident is a victim of a data breach, and depending on the type of breach, may require more information).

[95] *See* Marcus, *supra* note 50, at 581 (arguing that a national data security law would be beneficial because it would be more efficient instead of having consumers litigate against each company when they are a victim of a data breach, and it would create uniform standards for how companies' should collect, store, and use data); *compare id. with* Tara B. Ratanun, *Genetically Modified Organisms and Environmental Justice: Should Labeling be Mandatory on Products Containing Genetically Engineered Ingredients?*, 42 W. ST. L. REV. 111, 127 (2014) (discussing organic food and non-GMO manufacturers, who will conspicuously label their packages to show that it is an organic product, allowing consumers to make an informed decision).

E. The GDPR – A Model to Strive For

The European Union's adoption of the Global Data Protection Regulation ("GDPR") in May 2018 will allow for consumers to clean up the electronic trail they leave behind while browsing the internet.[96] Further, it will give them the ability to demand their information from business entities, thereby keeping businesses transparent.[97] The GDPR defines holders of data to be either a data controller or a data processor, each with their own distinct but similar duties.[98] GDPR also requires that if a consumer is the victim of a personal data breach, the data controllers have to notify the supervisory authority "without undue delay."[99] The biggest part of the GDPR is that any company in the United States that has a Web presence in the European Union will

[96] *See* Satariano, *supra* note 18 (detailing how businesses show how someone's information is being used by them, and the fines they face if they fail to meet these standards); *see also* Bill Bourdon, *The Avoidable Mistakes Executives Continue to Make After a Data Breach*, HARV. BUS. REV. (Nov. 20, 2017), *archived at* https://perma.cc/AM5D-A5SP (noting companies such as Sony who did not say anything about being breached until two days after it occurred, and the way the facts were unfolded to the public should have been handled differently).

[97] *See* Kim Davis, *GDPR: What Matters to Consumers*, DMN (May 28, 2018), *archived at* https://perma.cc/SJ55-KMDA (highlighting that consumers want transparency regarding how their data is being used).

[98] *See* Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY TECH. L. J. 287, 307 (2018) (discussing that data controllers are "entities that hold personal data and decide what to do with it" and data processors merely follow the instructions from the controller about what to do with it). It's important to note that the difference between data controllers and processors has big implications when determining liability on a breach company, especially if they outsource storage to 3rd party cloud providers. *Id*.

[99] *See* Aaron K. Tantleff, *Equifax Breach Affects 143M: If GDPR Were in Effect, What Would be the Impact?* 19 J. HEALTH CARE COMPLIANCE 45, 46 (2017) (articulating that under GDPR, a notification of a data breach has to include the number and categories of the data subject and personal data that is affected, the data protection officer's contact information, the consequences of the breach, and mitigation efforts); *see also* Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google an Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 3, 95 (highlighting Article 33 of the GDPR which "requires the company encountering a breach to notify the relevant supervisory authority not later than 72 hours after discovery").

be subjected to the GDPR in the event of a breach.[100] This is quite alarming for many companies such as Facebook, Google, Apple, and Amazon.[101] An overarching idea that surrounds GDPR and the way data breaches are communicated and handled in the United States is the idea of consumer privacy, or lack thereof.[102] As a result of the GDPR being enacted, companies in Silicon Valley and Congress are finally realizing that there needs to be a complete overhaul for data privacy regulation, and new federal data protection laws.[103] In order for a new federal data regulation to go into effect, there are many hurdles – including how to enforce such legislation and what the institutional framework will look like.[104] The California Consumer Privacy Act has borrowed many key aspects of the GDPR, and lays a

[100] *See* Faitelson, *supra* note 20 (elaborating that United States companies that do not have a physical presence in the European Union would have to target a data subject in an EU country to be subjected to the GDPR); *see also* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1011 (2016) (highlighting that as it relates to Big Data, the GDPR has strict rules in general that negates what Big Data stands for).

[101] *See* Alex Hern, *Facebook and Google targeted as first GDPR complaints filed*, THE GUARDIAN (May 25, 2018), *archived at* https://perma.cc/XN77-JLJE (showing that the first complaints filed under the GDPR are against Facebook and Google). The article notes that both companies spent 18 months ensuring that they would meet requirements of the GDPR from the start, and have since made their policies clearer and their privacy settings easier to find. *See* Hern, *supra*; *see also* Tal Harari, *Facebook Frenzy Around the World: The Different Implications Facebook Has on Law Students, Lawyers, and Judges*, 19 ILSA J. INT'L & COMP. L. 1, 3 (2012) (explaining that Facebook has well over 500 million users, and has significant global impact given that 70% of user access occurs outside the United States).

[102] *See* McKenzie L. Kuhn, *147 Million Social Security Numbers For Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches*, 104 IOWA L. REV. 417, 422 (2018) (articulating that the United States does not consider privacy to be a fundamental right, and that GDPR aims to make consumer privacy a top priority); *see also* Michael McFarland, *Why We Care About Privacy*, MARKKULA CTR. FOR APPLIED ETHICS (June 1, 2012), *archived at* perma.cc/F2E5-MBNW (articulating the psychological harms one may face if they are a victim of a data breach).

[103] *See* Dan Tynan, *Silicon Valley finally pushes for data privacy laws at Senate hearing*, THE GUARDIAN (Sept. 26, 2018), *archived at* https://perma.cc/VNB9-UJQ7 (explaining that all the witnesses objected some aspects of the GDPR and the new California law with similar features, but they all favored "a federal law that pre-empts existing and pending state regulations").

[104] *See id*. (articulating that Congress has been trying to figure out how to adopt legislation for data protection for 18 years and that it will take a long time to truly figure out).

solid framework for how the United States should build a skeletal outline of their own federal legislation.[105] The United States should consider adopting relevant aspects of the GDPR, in addition to setting forth new industry security standards that holds companies more accountable.[106]

IV. Analysis

A. Roadmap of New Federal IT Security Standards and Legislation

The most vital themes of the GDPR that Congress should enact are the ones that give more authority to the consumer with their right to communication, notification, and a quick access to a judicial remedy.[107] When consumers are injured in a data breach of their IoT device, they need legislative tools to rely on and utilize in two different scenarios.[108] The first scenario is when a company can prove their security infrastructure followed industry best practices, and the second is when a company is merely skating by with extremely subpar security infrastructure in place.[109] In both situations, consumer plaintiffs should have the right to be "made whole" again by the negligent company.[110]

---

[105] *See* Joseph Jerome, *California Privacy Law Shows Data Protection is on the March*, 33 ANTITRUST 96, 96, 98–99 (2018) (recognizing that the GDPR gives individual affirmative rights related to data including the right to know, right of access, right to portability, and right to erasure). This implies that the California Consumer Privacy Act also echoes these rights, and future federal legislation will likely incorporate them as well. *Id.*

[106] *See infra* Section IV.

[107] *See* Tran, *supra* note 61, at 278 (addressing how difficult it is for a consumer to lodge a complaint, and how there are "limited remedies for IoT violations that occur outside the scope of state and federal legislation or FTC authority").

[108] *See* Ensenat, *supra* note 46, at 74 (advocating for federal legislation to help victims of IoT device data breaches).

[109] *See* Buttrick et al., *supra* note 17, at 17 (proposing that there be a federal regulation that would preempt state laws and make things simpler). In general, the proposed bills are not very strong and do not adequately protect consumers. *Id*. at 17–18.

[110] *See* Mills & Harclerode, *supra* note 74, at 809 (showing that plaintiffs have been able to get compensatory damages successfully against a corporate data holder under theory that they should be held "to a standard to exercise reasonable care of the data regardless of direct economic loss").

In Section B of this Note, a new federal industry standard for IoT devices will be introduced.[111] This new standard gives IoT device manufacturers and consumers alike the ability to be on the forefront of stopping breaches.[112] Section C, analyzes how the newly created CISA should be designed with specific processes for reviewing data breach cases that are caused by IoT devices, and how they will apply the proposed Balancing Test.[113] In the event that an appeal goes forward, the federal court tasked with handling it would similarly apply the same test.[114] Following this, Section D will examine how punitive damages should be put in place to penalize companies that are making little effort with improving their IT security infrastructure.[115] Lastly, section E will explain how the proposed security standard and Balancing Test are Congress's answer to the European Union's enactment of GDPR.[116]

B. Federal Security Standards Need to be Implemented for IoT Devices

Even if a company is using the most stringent security standards, it is common knowledge that data breaches are impossible to stop completely.[117] Thus, a formal definition defining an industry standard for security must be put into effect.[118] Building optimal security components into a product at the start of design is not a

[111] *See infra* Section B.
[112] *See* Paez & Tobitsch, *supra* note 48, at 227 (paraphrasing that "security by design" involves "taking into account security at the outset of designing an industrial IoT system").
[113] *See CISA*, *supra* note 56 (showing that the CISA is an agency under the Department of Homeland Security).
[114] *See also Brief Overview of FTC*, *supra* note 53 (understanding that even though the FTC may apply its own rules in determining if an entity has made a violation, the court will ultimately be the one to enforce it).
[115] *See infra* Section D.
[116] *See* Shahmiri, *supra* note 92, at 39 (suggesting that a balancing test would help regulate safer data practices).
[117] *See* Bugni, *supra* note 65, at 87 (recognizing that "there is no such thing as perfect security and data breaches inevitably will happen"). Additionally, hackers are becoming more strategic in the way they implement their attacks. *Id.* at 92.
[118] *See* Marcus, *supra* note 50, at 583 (suggesting that there should be an industry standard of security based on company size and what IT infrastructure they have in place already).

priority for companies.[119] In light of this, many IoT devices are predisposed to data breaches, which should compel Congress to implement uniform security standards based on a combination of industry best practices and FTC guidelines for IoT device manufacturers.[120] The FTC already has best practices available for companies to use as guidelines to help them develop new mobile applications, devices, and other "smart" technologies.[121] These guidelines should be used as a general outline of what IoT device security standards should look like.[122] Using these FTC guidelines, Congress should create an approval system for all devices that are marketed as having "smart" or "Wi-Fi enabled" capabilities with a logo on the packaging to signify this.[123]

---

[119] *See* Britton, *supra* note 25, at 4 (showing that companies have no incentive to build security into their IoT devices because there often is no time in such a competitive market); *see also* Beale & Berris, *supra* note 36, at 199–200 (highlighting that consumers want cheap products, therefore the manufacturers have no incentive to incorporate security into their devices).

[120] *See* Pierce, *supra* note 71, at 989–90 (laying out the twelve basic factors for an industry standard set by the FTC for the Payment Card Industry that companies should adhere to); *see also After the Gold Rush*, *supra* note 1, at 101–02 (outlining that the European Union already has started making companies build more quality into their IoT devices before they even enter into the market); *see also* Trautman & Ormerod, *supra* note 46, at 805–06 (understanding that IoT sensors like RFID technology "can be produced for under a penny"). Major companies like LG, that are setting the market standard for implementing smart technology into everyday consumer items, are causing "low-end competitors" to try and mimic their products, but with inferior security. *See* Trautman & Ormerod, *supra* note 46, at 805–06.

[121] *See* Kirtley & Memmel, *supra* note 41, at 473 (recognizing the guidelines that the FTC has in regulating IoT security standards).

[122] *See Careful Connections*, *supra* note 39 (listing a variety of considerations a company should take if they are manufacturing an IoT device). These considerations include designing a product from the ground up with security in mind, how to limit permissions, and taking advantage of readily available security tools. *Id.*

[123] *See* Paez & Tobitsch, *supra* note 48, at 240–41 (articulating that the FDA already has measures in place to regulate medical devices that have IoT or Wi-Fi related functions); *see also* Kosseff, *supra* note 58, at 1005 (suggesting that the FDA could impose fines on companies for lackluster security on their devices); *see also* Matwyshyn, *supra* note 45, at 1179–80 (proclaiming that there is no uniform way for companies to submit to security audits); Shahmiri, *supra* note 92, at 35 (paraphrasing that the FTC has consent orders for companies that become subject to FTC enforcement orders, and although they are not binding precedent, part of these consent orders includes security audits).

Congress should create this approval system and name it "Safe Smart Device," or "SSD" compliant.[124] This regulation will be comparable to organic food or FDA approval; only after sending their devices to the CISA for them to run security or hacking tests and approve that the product is safe and secure for consumer use will that device be considered SSD compliant.[125] Once SSD compliant, the IoT device manufacturers will be allowed to use the logo designation, which will be conspicuously placed on the outside of their device packaging for consumers to see.[126] A consumer shopping in a grocery store can make an informed decision to buy organic or non-GMO food based on the specific labeling on the food package, and rest easy knowing they are investing in a healthy product.[127] Similarly, with this proposed SSD logo on IoT device packages, consumers can make the decision to buy an IoT device that is theoretically safer and more secure to use than one that has not been through rigorous testing.[128] When a company decides they have a viable product ready to be sold to the public, they will have the option to certify their device is SSD compliant by paying $10,000 and sending a sample product to the CISA for them to conduct security tests on the device.[129] If the product

[124] *See After the Gold Rush*, *supra* note 1, at 102 (recognizing the need for devices to come "right out of the box" with stronger data encryption); *see also* Marcus, *supra* note 50, at 585 (highlighting that a national data security law would help implement an industry standard).

[125] *See* Peppet, *supra* note 2, at 140–41 (outlining that many IoT devices such as Fitbit and Nest Thermostats do not include anything in their packaging about privacy or data-related information, which means that a consumer may "purchase such a device with no notice that it is subject to a privacy policy").

[126] *See* Edwards & Veale, *supra* note 38, at 76 (suggesting that there be an FDA for algorithms given that because of the reliance of companies on algorithms there should be regulation for them as well).

[127] *See* Dhyani, *supra* note 8, at 30 (recognizing that consumers buying organic food should make purchases with "accurate beliefs and expectations" of the quality of food they are buying).

[128] *See id.* at 41 (showing that proper labeling is used to help consumers make decisions for themselves that align with their values).

[129] *See* Davenport, *supra* note 92, at 289 (highlighting that the FDA already has cybersecurity measures in place to regulate medical devices). It is designed with labeling in mind, which allows consumers to know exactly what the devices can and cannot do. *See* Davenport, *supra* note 92, at 289; *see After the Gold Rush*, *supra* note 1, at 102 (proffering that companies should have their devices come with "stronger data encryption" right out of the box, and that would be seen as a marketable selling point to consumers in general).

passes the rigorous, standardized federal testing, the company will be afforded the benefit of having the SSD label displayed on their packaging to distinguish themselves as a company that is investing in making secure products.[130]

The benefit of this approval system for consumers is that they can make an informed decision whether or not they wish to invest in a product that is SSD compliant.[131] The societal benefit of SSD compliance is that for the first time, there will be an industry standard of security with definitive, tangible terms, alongside "security by design."[132] Companies will receive the satisfaction of knowing that their product has already been through exhaustive federal testing before it's sent to market, while also allowing consumers to make an informed purchasing decision.[133]

C. Balancing Test – Addressing the Reality that Data Breaches will Always Occur

The unescapable fact is that hacks of every shape and size will never fully go away, even if companies have the most technologically sound security in place – so how can we simultaneously provide relief

[130] *See* Davenport, *supra* note 92, at 289 (recognizing that the FDA has lengthy, albeit nonbinding, guidelines in place for manufacturers of medical devices).

[131] *See* Peppet, *supra* note 2, at 140–43 (showcasing that with many IoT devices, the packaging and the user guides lack any material related to privacy or data-related information). The consumer may not be interested in what their Fitbit or Nest Thermostat offers in terms of security because the consumer's primary interest is in the device's functionality. *See id.* This Note aims to making consumers aware that security should be at the forefront of IoT devices and consumer purchases. *But see* Ratanun, *supra* note 95, at 127–28 (suggesting that if food companies are mandated to label their packages properly, then it would "help disseminate information much more reliably" for the consumer, allowing them to make an informed purchase). Just like consumers can choose to buy organic or non-GMO food in the grocery store, as opposed to foods that have not met those standards, the same informed buying process should be implemented into buying IoT devices. *See id.*

[132] *See* Marcus, *supra* note 50, at 585 (articulating that there should be industry standard guidelines based on a company's size and their current security infrastructure, and that a federal statute would help create a uniform industry standard).

[133] *See* Shahmiri, *supra* note 92, at 48 (suggesting that if companies had federal guidelines they had to follow, companies would be better able to self-regulate and consumers' privacy would be protected).

to injured consumers, and also punish companies?[134] Simply, companies that seek to market their products having "smart" or "Wi-Fi" enabled capabilities should understand and recognize that their products have a global impact.[135] Despite these common-sense norms and an understanding of the expanding use of IoT devices, the current fines under Article 83 of the GDPR are too strict for a company that is using best practices.[136] To compensate injured consumers who fall victim to a data breach with SSD compliant products, Congress should use a Balancing Test that examines factors to consider when the company at fault can prove that they are following appropriate security standards.[137]

This Balancing Test would first consider the actual cause of the breach.[138] The next factor to consider would be what security was in place at that company – were they using best practices and were their IoT devices SSD Certified?[139] The third factor to consider would be

[134] *See* Bugni, *supra* note 65, at 87 (highlighting that the FTC has said that "there is no such thing as perfect security and data breaches inevitably will happen"); *see also* Riedy & Hanus, *supra* note 23, at 21–22 (relaying that hacks will never go away, and hackers are only becoming more sophisticated in their attacks).

[135] *See* Bodenheimer, *supra* note 49, at 7 (recognizing that the Internet of Things connects tens of billions of devices around the world and has potential to generate trillions of dollars in economic activity); *see also* Paez & Tobitsch, *supra* note 48, at 220 (showing that the global impact of IoT devices could be $500 billion of GDPR by 2020).

[136] *See GDPR*, *supra* note 19, Art. 83 (defining the fines of a company that violates the provisions of the GDPR to be €20 million or 4% of the previous year's revenues).

[137] *See* Mills & Harclerode, *supra* note 74, at 790 (outlining that the Supreme Court has already used a balancing test in data breach cases); *see also* Shahmiri, *supra* note 92, at 40–41 (suggesting that the FTC should apply a balancing test in IoT breach cases).

[138] *See* Harshbarger, *supra* note 25, at 253 (understanding that employee or human errors occur and could be the cause of a data breach as it relates to cloud computing); *see also* Mills & Harclerode, *supra* note 74, at 786 (finding that 14% of all data breaches in 2016 were caused by employee error). Additionally, hackers with malicious intent are another cause of breaches. *See* Mills & Harclerode, *supra* note 74.

[139] *See* Kirtley & Memmel, *supra* note 41, at 473 (outlining that the FTC already published best practice guidelines for companies to implement into their IT security); *see also* McSweeney, *supra* note 44, at 212–13 (inferring that if a company already has shown that they do have ample security built into their products, then they should be distinguished from a company that is using subpar security measures); *see also* Peppet, *supra* note 2, at 96 (suggesting that there be best practices in place to regulate the Internet of Things); *see also* Pierce, *supra* note 71, at 997–98 (articulating that

considering the extent of the injury to the consumer – did injury occur, is it imminent, or is it unlikely.[140] This factor would also look into how a consumer should be compensated for non-material losses such as emotional distress, akin to a hack of the baby monitors.[141] And finally, the last factor would consider if the company had a history of prior breaches, and if so, how they have responded and communicated in those situations.[142] Once the test is complete, compensatory damages will be determined via the CISA, and potentially a federal court.[143]

A Balancing Test would be critical for both parties – the damaged consumers, who have a right to compensation, and the companies because no two company's security systems are alike and it would be unfair to compare them to a federal standard.[144]

based on the FTC security best practices for the Payment Card Industry, Congress should implement best practices in general based on that standard).

[140] *See* Mank, *supra* note 9, at 1330 (articulating the Supreme Court's three-part test to determine Article III standing); *see also* Bugni, *supra* note 65, at 73–74 (distinguishing the differences between the plaintiffs in *Clapper* where the plaintiffs alleged that they might be a victim in the future as a result of the data breach they suffered versus in some class actions suits where the plaintiffs have argued that they were *specifically* targeted as a victim in a breach); *see also* Kim, *supra* note 11, at 566–67 (clarifying in *Clapper* that the court held that claims of future harm can satisfy Article III standing "if the harm is 'certainly impending', but 'allegations of possible future injury are not sufficient"'). Also, in the *In re Adobe Systems* case, the facts made it clear that they were targeted by hackers, and some of the information was already by hackers online, leading to more imminent injury. *See* Kim, *supra* note 11, at 565.

[141] *See* Phifer, *supra* note 46 (understanding that if a parent had their baby monitor hacked and did not have any way to truly remedy the scenario, the emotional stress and uncertainty would be vast). The idea of emotional distress suffered by a consumer after a hack on an IoT device has become increasingly relevant. *Id.* With the number of devices connected, and the prevalence of children using these devices, the possible scenarios where children could be exposed to dangerous situations, and the parents left helpless, are extreme. *Id.*

[142] *See* Riedy & Hanus, *supra* note 23, at 23 (recognizing the need for a well-trained incident response team in a company); *see also* Matwyshyn, *supra* note 45, at 1121 (generally analyzing that if a company has a longstanding problem of vulnerabilities, it is likely because it is not being made a priority at an organizational level).

[143] *See Brief Overview of FTC*, *supra* note 53 (highlighting the authority the FTC has).

[144] *See* Shahmiri, *supra* note 92, at 40–41 (outlining the benefits of a balancing test deployed by the FTC); *see also* Matwyshyn, *supra* note 45, at 1123–25 (recognizing that there are security vulnerabilities in the private and public sector that often overlap, and there are flaws in the underlying code of IoT products); *see also* Elvy,

Companies that knowingly market their products globally should always be evolving and be held responsible for the global reach of their products.[145] These companies should not be let off unscathed because they can prove they are using sufficient security.[146] Fittingly, this Balancing Test analysis is aimed at giving companies the benefit of the doubt.[147] The combination of affording companies the chance to certify their IoT devices are SSD compliant, with the consumers' ability to make informed purchasing decisions, holds everyone accountable and allows the consumer to get compensation more efficiently than the old route of having to prove liability.[148] When the company can show SSD compliance, the Balancing Test awards compensatory damages, whereas when the company is negligent, the test is a vehicle to allocate punitive damages.[149]

supra note 41, at 448–49 (paraphrasing the risks that consumers have regarding the amount of IoT data out there, and the disclosure to third parties has problematic consequences to the consumers).

[145] *See* Riedy & Hanus, *supra* note 23, at 26–27 (highlighting that businesses and their data are "increasingly interconnected in the global economy" and that companies should be aware of the liabilities that accompany them by simply doing business in today's world).

[146] *See* Shahmiri, *supra* note 92, at 41 (recognizing that instead of punishing a company immediately for a data breach, a company should be measured by what security practices they have in place).

[147] *See id.* at 41 (showing that if a customer is using best practices, they "should be dealt with more generously"). Shahmiri goes onto include an analysis of whether the breaching company faced any physical limitations in their device that may have led to a security flaw. *Id.* at 42. She suggests that a balancing test would lead to more industry self-regulation, and also proposes that contributory negligence on the part of the consumer should be addressed; all factors that distinguish her analysis as being more defendant-friendly. *Id. See also* Posadas, *supra* note 1, at 98–99 (highlighting that because IoT devices are connected via Wi-Fi, it is considered "low-hanging fruit" for hackers.).

[148] *See* Houser & Voss, *supra* note 99, at 95–96 (addressing that an open line of communication is important); *see also* Riedy & Hanus, *supra* note 23, at 31–32 (discussing that legal standards for specifying a wrongdoer make it difficult for a plaintiff to recover, especially in a "run-of-the-mill data breach" in a retail store, where it would be particularly difficult to pinpoint liability); *see also* Meal, *supra* note 10, at 6 (outlining the causation problems with proving negligence by a company in a data breach case); *see also* Kim, *supra* note 11, at 566–69 (outlining the difficulties a plaintiff has in trying to identify Article III standing).

[149] *See* Tran, *supra* note 61, at 290 (paraphrasing that punitive damages to compensate a victim in an IoT breach case would be effective in punishing the company while also compensating the victim).

D. You Can Lead a Horse to Water, But You Can't Make it Follow Security Standards

Regulations will need to be in place for companies that are selling products that are not SSD compliant or are not following industry accepted best practices.[150] Accordingly, any company that is found liable for a data breach would be subject to punitive damages under the Balancing Test, on top of the compensatory damages already allotted to the consumer by the CISA.[151] This allows the Balancing Test outlined above to act as an incentive for companies to invest in security, while giving consumers access to easy compensation.[152] A consumer who may be financially damaged after a data breach by a company with a high level of security should be treated differently than a consumer who is financially damaged in a breach caused by a company with severely lackluster security.[153] With the opportunity for punitive damages to be awarded, it would hopefully make the appeal of becoming SSD compliant worth it, while also distinguishing companies with poor business practices who do not wish to make security a priority.[154]

E. Legislation to Empower Consumers – Tying it All Together

[150] *See* Posadas, *supra* note 1, at 101 (suggesting that there needs to be a regulation in place of IoT manufacturers, and proposing that the best way to do this is by a "self-imposed privacy-by-design scheme."). Posadas also suggests that blockchain technology would help as a new method of data encryption. *Id.* at 105–06. Primarily, because blockchain technology is decentralized and relies on the trust of its users. *Id.* Accordingly, it is supposedly the "most secure response to privacy concerns for IoT devices." *Id.*

[151] *See* Murray, *supra* note 9, at 154 (alluding that companies that should receive punitive damages if they are not following regulations). This "actually impacts their bottom line" and it should be "significant enough to have a deterrent effect on other corporations whose systems are susceptible to data breaches." *Id.*

[152] *See id.* at 156 (highlighting that specific relief is an equitable remedy that is intended to make the plaintiff whole again). Specific relief is rarely given in modern courts today. *Id.*

[153] *See* Shahmiri, *supra* note 92, at 40 (outlining that the FTC has already recognized that IoT devices and the security that is built into them should be treated differently).

[154] *See* Trautman & Ormerod, *supra* note 46, at 778 (suggesting that it is an issue of corporate governance why companies are not prepared for cybersecurity problems).

Knowing that hacks carried out via IoT devices will eventually become a norm in society, there has to be federal legislation enacted that mimics the GDPR in order to give consumer protection in various capacities.[155] When a consumer is the victim of a breach – whether there is actual injury or mere potential for future injury – the short term effects are incredibly troubling and burdensome, and the GDPR aims to fix that.[156] The GDPR will have an effect on IoT device manufacturers, with their mandatory Data Protection Impact Assessments.[157] These assessments require data breaches be reported if personal data is compromised and institute processes at the company for regularly testing, assessing, and evaluating the security.[158]

In order to keep its citizens more informed, Congress should first address the apathetic communication that consumers receive when there is a data breach, and specifically, what happens when they actually are a victim of one – similar to Article 34 of the GDPR.[159]

---

[155] *See* NG, *supra* note 3 (noting prevalence of electronic devices in society); *see also* Trautman & Ormerod, *supra* note 46, at 805 (recognizing that with the "rapid proliferation" of IoT devices, there comes new problems for manufacturers—primarily, because so many companies are not making security a priority).

[156] *See* McFarland, *supra* note 102 (noting that victims of data breaches suffer psychological harms); *see also* Phifer, *supra* note 46 (explaining that the parents whose baby monitor was hacked, thus subjecting them to lewd oral comments by the hacker, could not be compensated by the baby monitor company); *see also* Marcus, *supra* note 50, at 581 (suggesting that a federal data security law needs to be implemented given that data breaches will continue to happen, and consumers' personal information will continue to be vulnerable).

[157] *See GDPR*, *supra* note 19, Art. 35 (referencing how Data Protection Impact Assessments will be used when companies are implementing new technologies to ensure that data will be protected).

[158] *See id.* Art. 32 (mandating that companies "shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk"); *see also* Kirtley & Memmel, *supra* note 41, at 497–98 (outlining how the GDPR will affect consumers who use IoT devices and IoT device manufacturers); *see also* Paez & Tobitsch, *supra* note 48, at 246 (showing that the GDPR will require companies to "implement technical and organizational measures to protect personal data collected through industrial IoT technologies").

[159] *See* Houser & Voss, *supra* note 99, at 96 (inferring that companies in the United States take their time in determining how elaborate of a breach occurred before sending out notifications to those affected); *see also* Buttrick et al., *supra* note 17, at 17–18 (proposing federal regulation that would preempt state laws and make things simpler, and in general, the proposed bills are not very strong and do not adequately protect consumers); *see also GDPR*, *supra* note 19, Art. 34 (quoting "[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of

Currently, the companies who are victims of data breaches deploy a cycle following the breach that provides little satisfaction to the affected consumers.[160] It starts with a public relations-written press release worded carefully, which is then followed by a statement made by the CEO about how they are investing more into security; this vicious cycle continues onto the next company who is hacked.[161] This incessant, never-ending cycle of "band-aid" fixes is not adequate to consumers who are eagerly trying to determine if they are in any way at risk.[162] As soon as a company realizes they have been hacked and individual information of a data subject has been compromised that individual needs to be notified about the exact information stolen.[163]

Notification of a data breach should include a personalized email to each victim regarding if any of their information was compromised as soon as the company has identified what occurred.[164] It is even more important to notify the individuals if the compromised information was considered sensitive information such as social security numbers, bank accounts, and credit cards.[165] Such notifications should also include detailed instructions about what the victim should do next, and contact information for someone in the company that they can speak to regarding the breach.[166] The goal of

natural persons, the controller shall communicate the personal data breach to the data subject without undue delay").

[160] *See* Kuhn, *supra* note 102, at 438 (showing that consumers are unhappy with the turnaround time when companies inform consumers they have been breached).

[161] *See* Riedy & Hanus, *supra* note 23, at 5 (recognizing that data breaches happen regularly and are in the news).

[162] *See* Bourdon, *supra* note 96 (noting that state laws limit the range of when consumers are notified of a data breach of between fifteen to ninety days).

[163] *See* Kosseff, *supra* note 58, at 1006 (arguing that even though the damage caused by a data breach may already be done, notification should still be completed, and in greater detail than it is now); *see also* Kuhn, *supra* note 102, at 442 (suggesting that Congress require companies to notify consumers after their personal information has been compromised); *see also* Riedy & Hanus, *supra* note 23, at 46 (recognizing that if notification statutes were more sufficient and included information about the circumstances of the breach, litigation costs could be reduced).

[164] *See* Riedy & Hanus, *supra* note 23, at 45–46 (specifying that a stronger notification statute would help if there was a Compensation Fund for victims of data breaches).

[165] *See id.* at 20 (identifying the various direct and indirect costs associated with a consumer breach that need to be considered).

[166] *See id.* at 47 (suggesting that if a victim were notified that they were breached, they could file a claim "as long as their personally identifiable digital data has been

these notifications will hopefully alleviate any concerns consumers have about data breaches, and give them the necessary information for next steps.[167]

Perhaps the most consumer-empowering articles of the GDPR are Articles 77 and 78, which say that "every data subject shall have the right to lodge a complaint" and "[w]ithout prejudice to any other administrative or non-judicial remedy each data subject shall have the right to an effective judicial remedy. . . ."[168] Given the difficulty that consumers have in proving liability of a corporate entity, from a procedural and substantive standpoint, federal legislation in the United States should allow consumers to be able to lodge complaints in detail to the CISA without any restrictions.[169] These articles are crucial because it allows the victim consumer to alert the manufacturer that they are a victim of a breach, when otherwise the manufacturer may not be alerted to it.[170]

The statutory threshold that a consumer must hit in the GDPR in order to get an effective judicial remedy is low – it merely requires that the data subject considers that the processing of his or her

compromised by a hacking incident into the computers or networks of an entity that regularly collects and houses that data for ordinary business purposes").

[167] *See id.* at 35 (understanding that consumers should be notified if they are a victim of a breach, and can possibly prevent frivolous lawsuits).

[168] *See id.* at 37 (generally suggesting that there should be a compensation fund for victims of a data breach, but there is a vast amount of variables to consider in order to make one). Primarily, it may not be worth the cost based on the "nominal amount of monetary harm those victims actually incur" and it's tough to predict how damages may balloon in the future. *Id.*; *see also GDPR*, *supra* note 19 (noting that Article 77 of the GDPR allows for a data subject to lodge a complaint, if they subjectively believe that the way in which their personal data has been processed violates any aspect of the GDPR). This appears to be a pretty low threshold, and seemingly gives data subjects the authority to lodge a complaint as long as they can show they have been affected in some way. *GDPR*, *supra* note 19.

[169] *Compare* Kim, *supra* note 11 (getting past Article III standing issues are difficult, and if there was an easier way for consumers to make a claim it would at least start the process of giving them relief), *with* Kosseff, *supra* note 58, at 1030 (articulating that many data breach notification statutes are backwards looking. These data breach notification statutes require companies to give consumers notifications *after* a breach has occurred, but if they just made security a priority in general, it would overall help stop data breaches. *See* Kosseff, *supra* note 58.

[170] *See* Kuhn, *supra* note 102, at 431 (laying out that the GDPR includes a provision where the consumer has a "right to be informed," which could be applied to them knowing exactly when they may have been a victim of any kind of data breach).

information infringes on the GDPR.[171] Instead, Congress should rely on the experts at the CISA and the Balancing Test outlined previously in this Note to determine how a judicial remedy should be processed.[172] The GDPR also does not provide much by way of what a "judicial remedy" should look like.[173]

By using the aforementioned Balancing Test, Congress can implement aspects of Article 82 of the GDPR, which says that "[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation . . . ."[174] Because Article 82 is lacking in clarity, the idea of "non-material" damages can be addressed via a Balancing Test analysis.[175] Given that consumers may never actually face imminent injury or prove that they have suffered material damages, but may have substantial damages of emotional distress knowing that their private lives have been infiltrated, a provision addressing non-material damages is essential and should be added.[176] In theory, in a future data breach caused by a company or an IoT device, as soon as the consumer

[171] *See GDPR*, *supra* note 19, Art. 77 (providing language to show a low burden using the word "considers").
[172] *See* Zarsky, *supra* note 100, at 1011 (inferring that the GDPR regulations in general are pretty strict against companies, and perhaps a looser test would be more appropriate).
[173] *See GDPR*, *supra* note 19, Art. 77 (outlining the lack of judicial remedy definition).
[174] *See id.* Art. 82.
[175] *See* Kuhn, *supra* note 102, at 444–45 (recognizing that the GDPR requires consumers to get notified of a breach using clear and plain language). Further, in the event that federal legislation should be put in place in the United States, it too should use clear language and "be simple enough for consumers to understand what they are consenting to." *Id.*
[176] *See* Mank, *supra* note 9, at 1356 (suggesting that in the *Spokeo* case, where the "risk of real harm" could satisfy the concreteness requirement for Article III standing, "even if their harms may be difficult to prove or measure"); *see also* Marcus, *supra* note 50, at 566–69 (highlighting the various ways plaintiffs have tried to find "injury in fact," including that a breach "devalues their personal information," and that the breach caused an increased risk of identity theft); *see also* Kim, *supra* note 11, at 573–74 (recognizing the Seventh Circuit's plaintiff-friendly reasoning when it comes to addressing the injury requirement in standing). Due to the number of plaintiffs that get affected by breaches, and how they may experience vulnerabilities that are not tangible, there should be a lower threshold for finding standing. *See* Kim, *supra* note 11.

becomes aware of the breach, the mere increased risk of identity theft would be enough to give them a right to a judicial remedy.[177]

IV. Conclusion

Ultimately, any federal legislation that is passed in the United States needs to give consumers more notification and more authority to lodge complaints. The biggest detriment that faces IoT devices is the fact that they are built from the start without security in mind. Hopefully, by giving companies the ability to certify their devices as SSD Compliant it will make them more accountable for what they are selling to the public. SSD Compliance will also make the consumer more aware of what they are purchasing – distinguishing the manufacturers who view security as an afterthought. Because fully ridding the world of data breaches is unrealistic, the newly created CISA should be tasked with applying the proposed Balancing Test to a company after a consumer lodges a legitimate complaint following a breach. The Balancing Test will allow the CISA to decide appropriate consequences for the company based on what security measures or protocols they had in place, in addition to a proper remedy for the injured consumer. When viewed as a whole, the combination of federal security standards for IoT devices and greater consumer empowerment are essential in keeping anyone with an electronic device in their hands safer and more informed.

[177] *See* Kim, *supra* note 11, at 559 (highlighting in *Krottner* where the Ninth Circuit, similar to the Seventh Circuit, held that "the increased risk" of identity theft caused by stolen laptops was sufficient to establish injury-in-fact).