Uncle Sam Meets the Villains from the Appliances: Internet of Things Security and Government Regulation

By: Henry Holben

Dr. Blouin

Composition

31 October 2017

**Introduction**

The efforts made thus far to make the Internet of Things more secure have been inadequate. When public infrastructure is embedded with internet-connected electronics, that infrastructure becomes susceptible to tampering. The development of the Internet of Things endangers the safety and privacy of American citizens. The danger grows by the day, and if public utilities and infrastructure in the United States is to be sustained, adequate action must be made. As such, the United States government should regulate the Internet of Things.

Keeping that thesis in mind, get outdoors and make for the appliance store. Are you there yet? There are boxes of electronics all around you, innovations designed to save you time, stress, and sweat. Now take a look at the smartphone in your pocket: the default connection between you and the largest library, market, bank, news platform, and social forum in the world. You control this smartphone via touchscreen, noting that most of the devices around you still have their individual controls of analogue buttons and knobs. It’s for this reason, that you can ignore most of the merchandise for now, but do not worry, it will all be assimilated in time. Instead, go over to the home automation isle. The shelves here are stocked with a single word: ‘smart’. Smart watches, smart phones, computers, thermostats, televisions, refrigerators, and washing machines, even smart lawn sprinklers adorn the rows. Take a look, you are holding a box containing a Google Home. You might compare the Google Home, the NEST, or any number of Samsung’s related devices. You could automate your house with these smart home devices. In a house lit by Internet connected lightbulbs, you could set your lights to turn on at the exact time your alarm wakes you in the morning. Clapping the lights on is a cheap trick in a world of connected smart homes. But more than merely turning the lights on, you could pick the color the lights would turn on to, creating the ideal mood for jump-starting your daily routine. You could even have your stereo system play your favorite song for you as you got up. Now think bigger. An internet-connected smart coffee maker could have your morning cup of joe ready and waiting for you when you crawl out of bed. Your home computer could read you the day’s itinerary, or maybe a smart TV nearby could pick up where you left off on your favorite Netflix series. It could all be scheduled, programmed, and integrated. But why set the schedule yourself? These devices are laden down with sensors and cameras, and are “smart” enough to figure out your daily routine on their own. In a word, it could all be interconnected. Now isn’t that smart?

These “Smart home” devices are offering you the chance to make your house a model of a recent trend in internet-development. Gone are the days when the internet merely carried the voices of its users. Today technology developers are making devices and appliances accessible from the Internet. Technologists talk about these devices as though they made up a network of their own. and they often refer to this network as the Internet of Things, often abbreviated a IoT. To clarify, IoT is not a particular network of its own, or any interindividual section of the internet, it is merely a phrase describing appliances, and machines, or “things” that have recently been given a digital upgrade. This is often a point of confusion for the reader or the audience, the phrase refers more the trend of implementing tools and appliances with internet connectivity than any actual part of the internet. A product joins IoT when that product is given internet-connected sensors. A good example of this is Samsung’s line of Internet-compatible Smart refrigerators. The following is a quote from Samsung’s website, advertising an IoT refrigerator.

# “With a connected touchscreen, the Family Hub lets you plan meals, coordinate family schedules and even entertain, helping you organize your home and live better every day…Create shopping lists and peek inside your refrigerator from anywhere. With three interior cameras that take a photo when you close the door, the Family Hub lets you check your refrigerator from anywhere…Set expiration notifications to help you plan ahead and know when you need to go grocery shopping…Sync your family’s shopping lists or buy groceries right from your refrigerator door. The Family Hub makes it easy to coordinate, so everyone gets what they need.”[[1]](#footnote-1)

Technologists expect that in the future IoT compatibility will continue to become a mainstream feature of most consumer products in a stage of development dubbed the ‘IoT revolution’. This technology is nothing new, industrial settings have long since found use for machines that could wirelessly communicate and share information, and now product developers have found a place for IoT in the consumer market. Technologists predict that the IoT revolution will lead to changes in the very nature of consumer products and changes in the lifestyles of people using the technology[[2]](#footnote-2). IoT is also being implemented in public infrastructure with internet-connected traffic lights, cameras, and even smart cement capable of detecting ice on its surface to alert passing drivers.

But all of these new internet-connected devices share a common problem: the malevolent “Black-hat” computer hacker. The hackers need no introduction. Cyber-crime is already an object of public fear. Time and time again, security breaches cost consumers millions. An article by Fawn Ngo and K. Jaishankar commemorating the tenth anniversary of the International Journal of Cyber Criminology acknowledged that there is little in the way of reliable and precise data on the full extent of cyber-crime. The article provided estimates, citing the security software developer McAfee with a rough estimate of one-hundred and ten billion dollars in annual global damages attributable to cyber-crime.[[3]](#footnote-3) From identity theft to manipulating government elections, fingers of blame are quick to fall on the anonymous cyber-thief, often for good reason. The public conscious has come to fear hackers to the brink of hysteria, and the concern is only rising. Now the public consciousness is beginning to fear that developments in IoT are making cyber-crime a far deadlier issue than it ever was. The Federal trade commission (FTC) has already identified IoT as a point of major concern and actions have been taken to force developers to provide their customers with some protection.[[4]](#footnote-4) Nevertheless, IoT becomes further integrated into American life, and the world at large each day. Security penetration testers, sometimes called “pen testers”, or “white hat hackers” have demonstrated their abilities to hack a plethora of IoT devices. An article from wired called “How the Internet of Things Got Hacked” listed, home appliances, cars, baby monitors, pacemakers, and even a sniper-rifle with a “self-aiming scope system” as candidates for IoT hacking.[[5]](#footnote-5) Such penetration testers, have voiced concerns for the minimalistic security features placed in many more IoT products including diabetic insulin pumps. IoT is developing quicker than IoT security, and unless the proper precautions are taken, public infrastructure will be exposed to cyber-attacks and the mass-hysteria must follow it.

The fears of the people, the demonstrations of the pen testers and the actions of the authorities raise some important questions: What is the proper position of the government toward IoT products that will make the safeguarded information of its citizens more vulnerable than ever before? What actions should and should not be taken in a capitalist nation to restrict developers from endangering civilian information and safety? As the homeland for many information technology companies, the United States ought to set a precedent for its respect of its citizens’ technological rights. Additionally, the United States government should regulate the implementation of the Internet of Things on American soil, perhaps by requiring developers to include security and data encryption features in all Internet connected devices they submit for U.S. patent review.

**Weighing the Risks Against the Benefits of IoT**

Innovation usually comes with some risks. Developments in aeronautical technology have made possible both the commercial airlines used for peaceful transportation, as well was the interatomic missiles with which nations threaten each other. The same technology of the atomic bomb can be harnessed to provide clean, efficient power. Even man’s primitive discovery of how to build and maintain a fire has brought both prosperity and devastation. There is the potential for both positive and negative consequences in most decisions humans make. When trying to make a rational decision, one must consider the positive and negative consequences as well as the likelihood of each possibility. Consider a common example: even one who follows every law of the road, and every automobile safety precaution can still be made victim to a car accident. Even if not at fault a driver can be injured or killed. This is no new information for the reader, only a reminder. Every day you choose to drive, you make an interesting presumption. By taking the road, you are showing your belief that you will navigate from point A to B without accident or injury. In fact, you are betting your life on it. Americans spend a good deal of time in and around automobiles regardless: the rewarded speed and efficiency outweighs the danger. The adoption of government regulation is no exception. If a decision for or against government intervention in the IoT market is to be made, it must be founded on sound reason. The existence of the danger alone is not enough to make a rational argument for IoT regulation. Both the risks and the benefits of the IoT itself should be considered, as well as the available solutions. The temptation in this discussion is to succumb to fear and replace rationale with emotion. As Bruce Schneier, a notable writer on security issues wrote in an essay titled “Worst-Case Thinking” has put it,

“There's a certain blindness that comes from worst-case thinking. An extension of the [precautionary principle](http://en.wikipedia.org/wiki/Precautionary_principle), it involves imagining the worst possible outcome and then acting as if it were a certainty. It substitutes imagination for thinking, speculation for risk analysis, and fear for reason. It fosters powerlessness and vulnerability and magnifies social paralysis. And it makes us more vulnerable to the effects of terrorism.”[[6]](#footnote-6)

Therefore, before any argument for or against the government regulating IoT can be made, the benefits, the risks, and the alternatives to a government regulated IoT must be considered.

IoT is a useful industry that is beyond worthy of American investment. This paragraph can only describe a few of the countless benefits IoT offers to countless applications. The following quote by Alasdair Gilchrist from his book, *A Consise Guide to the Internet of Things for Executives* lists some of the numerous applications.

“IoT is already with us and if you take a look around you will see the evidence in the real world applications currently deployed, but we take them for granted. Examples of these IoT applications are: Smart Cities… Smart Environment… Smart Water… Security & Emergencies… Smart Retail…Smart Logistics…Industrial Control… Smart Agriculture…Smart Animal Farming… Smart Homes… eHealth”[[7]](#footnote-7)

On a macroeconomic scale, IoT is paving the way for information to be gathered, processed, and put to use within seconds, leading to a decrease in production costs of nearly all industries. The global internet as a whole is now able to effectively and quickly gather information about everything mankind has imbedded with a sensor and given internet capabilities. For smart home security systems this means that the petty house thief is about to go extinct.

As an example of how IoT can improve industrial production, consider how the implementation of the Internet of Things can improve agricultural production. Imagine you want to grow a tomato patch in a vegetable garden, but want to do a minimal amount of work to maintain that garden after your initial setup. IoT offers a solution: fill the rows with internet-connected sensors.

When Internet connected smart sensors are stationed to collect data, farmers are enabled to check on their crops speedily, thoroughly, and easily. A device can examine plants and the terrain the grow in. An article published by the International Research Journal of Engineering and Technology (IRJET) reported on this application of IoT in agriculture.

“The evolution of data over the past decade has started a unique thought in the domain of information technology and data science called Big Data. This technology is acquiring deep consideration as an idea to develop the performance of agricultural systems by combining different systems data and communications platform to reduce redundant crop failures, enhance agricultural governing and agricultural services. It gathers all crop information generated through electronic smart devices (like moisture sensors, electromagnetic sensors, and optical sensors) for a detailed area. These smart devices will generate impressive amounts of data, impelled by record keeping, agreement and regulatory requirements, which are considered as big data.”[[8]](#footnote-8)

That same article described how this technology can even generate advice and instructions for farmers based on the input sensor information.

“The research application is completely based on MAD-cloud architecture ,data are stored according to the co-ordinate and physical and chemical requirements of the crop. The data are stored in methodological form and they are updated by admin and data are collected by sensor, GPS. the data also defines soil texture, humidity, wind speed, rain amount. The user can obtain detain information about related crop which is require to increase the production, the user can select the co-ordinate location and define personal detail like name, place, etc. It also describes crop disease and method to cure.” [[9]](#footnote-9)

In the case of your IoT-enabled garden, you are enabled to watch the progress of your plants from afar. When a problem arises, you could get a notification on your smartphone- with a plentitude of advice of how to respond. Suppose for example it has not rained in a few days, and that moisture sensor you installed just detected a sub-optimal amount of water in your soil. You need to water the tomatoes you planted in your garden. You are far away from the tomato patch at the moment. In past times, that might have been an issue, but not anymore. With a tap and a swipe, you give your gardening system permission to run the lawn sprinklers over the tomato patch. After all, the computer knows the exact volume of water the garden needs to thrive. The lawn sprinklers kick into action, and the sensors begin to detect an ample supply of water. Maintaining your garden just became about as easy as playing an online farming game.

This technology is not merely useful for agriculture but is also useful in city applications. “Smart Concrete Could Improve Levees”, an article by space Daily, reports on the usefulness of “smart concrete”: carbon fibers buried in concrete that can detect stress in the concrete.[[10]](#footnote-10) The article references smart concrete’s inventor, Dr. Deborah D.L. Chung who claimed that this technology can alert a city to a coming earthquake, by detecting the stress underground. Chung additionally claimed that smart concrete can be used to monitor road traffic. In a world of connected “things”, Chung’s smart concrete could be used to send this information wirelessly to a public database. Innovation expert Daniel Burrus, wrote a two-part article for Wired called “The Internet of Things is Bigger Than Anyone Realizes” in which he described several possible applications of IoT including smart concrete. Burrus speculated the smart concrete could detect ice on its surface, and wirelessly send that information to cars on the streets, alerting drivers to the danger. Further, Burrus argued that IoT can manage traffic flow by using internet connected stoplights capable of reacting to the present cars on the street, rather than merely changing the light on fixed intervals. Burrus challenged his readers to dream bigger, suggesting IoT water pipe sensors that could detect the warning signs, and report a leak before it breaks.[[11]](#footnote-11) “There is no one sector where the Internet of Things is making the biggest impact;”[[12]](#footnote-12) wrote Burrus, “it will disrupt every industry imaginable including agriculture, energy security, disaster management, and healthcare, just to name a few.”[[13]](#footnote-13) In summary: IoT development has a beautiful vision for an interconnected future. It asks that perhaps all of man’s inventions might someday be unified into a single invention: an IoT that analyzes, records, and acts upon what it learns. The technology can be used to greatly benefit the American people. Be it in the business place, the home, or the city, IoT is beyond worthy of American investment.

Because IoT is worthy of American investment, the challenges posed by mass inter-connection in the states must be addressed. It should not come as any surprise that the Internet of Things will have flaws and security risks.The frequent need for software developers to release security patches is proof enough of that. Researchers have noted that as more devices are connected to the internet more points of penetration are made available to hackers.[[14]](#footnote-14) Today, the amount of devices on the internet is so high that experts consider the internet to be impossible to study thoroughly.[[15]](#footnote-15) Security researchers have demonstrated flaws in consumer IoT devices that if exploited, could grant the attacker access to a user’s personal information. Shane Dingman, a technology reporter for the Globe and Mail, wrote an article titled *“Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity”*. This article described a demonstration done by Ted Harrington at the 2015 DefCon conference.[[16]](#footnote-16) Harrington notified the developers of the products he was testing several weeks in advance, to give them a head start in securing their devices. Harrington then led a group that successfully several IoT flaws in consumer products including: a flaw in a baby monitoring system that could allow a hacker to watch the video stream live, a flaw in a home stereo system that could be exploited to distribute computer viruses, an internet-controlled toy tank that if hacked could allow the perpetrator to steer the tank and use its camera, a home surveillance camera that if hacked could be turned off, an IoT connected refrigerator that could allow hackers to peruse its user’s E-mail account and two different internet-connected door locks that if hacked, could be unlocked, allowing an intruder easy access into a building.[[17]](#footnote-17) Dingman also commented on a drone hack by Ryan Satterfield (that was witnessed at the same conference) that killed the flying robot in mid-air. Many of the hacks Dingman reported can enable hackers to steal a consumer’s personal information by targeting IoT devices, or even grant hackers passage into a consumer’s private property by targeting IoT home security products. Information and private property are not the only internet connected things hackers can attack. Some demonstrations have proven that some applications of IoT, if hacked, could mean physical, bodily harm or even death for the victim. Certain computerized cars have been proven to be vulnerable to cyberattacks. In 2015 a writer for Wired magazine, Andy Greenberg volunteered to let two security researchers named Charlie Miller, and Chris Valasek, hack his smart car as he drove it. The following quote is extracted from an article written by Greenberg about this experience.

“Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass. As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display… As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission. Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape.”[[18]](#footnote-18)

It is not difficult to see how a cyber-attack like that tested on Greenberg’s Jeep could prove deadly to a driver as well as passersby. This is an important point: mere abstinence from IoT devices cannot adequately protect a person from the dangers posed by IoT hacking. In Stephen Riga’s article, “Two Breaches, Two Enforcement Actions, and a DDoS Attack: Data Security and the Rise of the Internet of Things”, Riga pointed out that businesses can only expect IoT to appear in their facilities.

“Whether or not employers use this technology themselves, however, they must prepare for its introduction into their offices, factories, and conference rooms. Because, over the next few years, their employees will be adopting these technologies in their personal lives (many already have), and bringing these objects to work as they go about their daily routines”[[19]](#footnote-19)

Three Siemens employees I interviewed in January 2016 commented that the amount of time and money needed for a novice computer hacker to become a serious threat is very light.[[20]](#footnote-20) The ease of aquiring the needed skills for hackers, combined with the minimalistic security measures used by some IoT developers and the potential disasters that can arise from compromised security put IoT in an urgent need of improved security. A lawyer, with experience in issues of data security, Stephen Riga, has commented that implementing security in IoT devices often comes with some difficulty for developers.[[21]](#footnote-21) The incentive of profit can then easily outweigh concerns for user privacy, and security. Thus, developers lack sufficient motivation to secure their IoT products.

**Alternatives to Government Regulation**

It is unlikely that the proposed alternatives to government regulation alone will give IoT a successful level of security. Some critics of IoT regulation have argued that the government should not intervene in the IoT market because, that intervention would delay American technological progress, and resist innovation. Adam Theier, in response to an essay by Bruce Scheiner, made a case for this very argument, citing a difficulty for American Pharmaceutical companies caused by the Food and Drug Administration.

“with creating such a federal bureaucracy is that we could expect the rate of new innovation to slow considerably. Subjecting businesses to expensive pre-market approval introduces compliance costs and uncertainty that many small firms simply can't bear. This has been the case with Food and Drug Administration regulation, where most new pharmaceuticals are introduced by a handful of huge companies that can withstand the years-long, multi-million dollar regulatory process.”[[22]](#footnote-22)

Authors such as Theier have argued in support of “self-regulation” as a preferable option to government regulation. The idea of self-regulating the Internet of Things is the idea that the demands of consumers will provide the profit motive developers need to promote an acceptable level of security. Self-regulation would be a preferable option to government regulation because of its simple dependence on the free market to allow consumers. There would be no loss of freedom with a successful effort to self-regulate IoT. Customers would choose by their own volition to buy, or not buy a product, allowing the free market to pressure developers into implementing an expectable level of security in their products. it may be technically possible for IoT to be regulated without any government intervention, it is extremely unlikely that self-regulation alone can provide adequate security. Bruce Scheiner has also argued that the free market does not adequately motivate companies to provide an appropriate amount of security for sensitive information. In a testimony given by at a hearing regarding the 2017 Equifax security breach, Scheiner testified that companies such as Equifax collect information on people with whom they are not affiliated, and sell this information to clients.

“Equifax is more than a credit reporting agency. It's a [data broker](https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf). It collects information about all of us, analyzes it all, and then sells those insights. It might be one of the biggest, but there are 2,500 to 4,000 other data brokers that are collecting, storing, and selling information about us -- almost all of them companies you've never heard of and have no business relationship with.”[[23]](#footnote-23)

Scheiner argued that government regulation of some kind was warranted by the breaches of privacy, caused by this “data broking”. Scheiner further explained how a person whose sensitive information has been collected by such corporations has no power to improve the security that information.

“Right now, there is no way for consumers to protect themselves. Their data has been harvested and analyzed by these companies without their knowledge or consent. They cannot improve the security of their personal data, and have no control over how vulnerable it is. They only learn about data breaches when the companies announce them -- which can be months after the breaches occur.”

Schneier discussed the lack of sufficient motivations for developers to provide ample security for their devices. “Any company that spends more on security than absolutely necessary is immediately penalized by shareholders when its profits decrease.”[[24]](#footnote-24). He later added nearing the conclusion of his initial testimony, “Unless Congress acts to protect consumer information in the digital age, these breaches will continue.”[[25]](#footnote-25).

While Equifax is not a developer of IoT products, it is easy to imagine how the development of IoT could contribute to the same kind data collection. IoT is by default is a data collector. Not only, could a company like Equifax obtain information about a person’s credit ratings, in IoT, such a company could discover how many steps that person takes in a day, when they leave their residence, the places they go during the day and when they return home, just to name a few.

WhielEither method of regulating the Internet of Things will increase the costs of those devices. If legislation indirectly requires a developer to spend more money to improve the security of his products, that developer will likely not hesitate to raise the prices of the products to compensate. This outcome is no different in the event of successful self-regulation: either way the developer would most likely raise the price of the product to compensate for the money spent on security. The following quote from a summary of a workshop held by the FTC in 2013 to discuss Internet of Things devices sold to consumers comes from the paper’s conclusion that the Internet of Things ought to be increasingly self-regulated, as well as regulated, to some extent, by the government.

“The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.”[[26]](#footnote-26)

At least for the time being the FTC is encouraging IoT to be in part regulated by the government and in part self regulated. The FTC is right to thing that consumers and developers can make the Internet of Things more secure without the government’s intervention, however customers and developers lack sufficient motivation to do so. Developers have several motivations to create IoT related features in their products while not strengthening security to an appropriate level.

**Precedents for Government Regulation**

There is a long history of precedence for government regulation of dangerous products. As far back as the code of Hammurabi, producers of goods have been held accountable by law for flaws in their designs that cause customers bodily harm.

“If a builder build a house for some one, and does not construct it properly, and the house which he built fall in and kill its owner, then that builder shall be put to death… If it ruin goods, he shall make compensation for all that has been ruined, and inasmuch as he did not construct properly this house which he built and it fell, he shall re-erect the house from his own means. If a builder build a house for some one, even though he has not yet completed it; if then the walls seem toppling, the builder must make the walls solid from his own means… If a shipbuilder build a boat for some one, and do not make it tight, if during that same year that boat is sent away and suffers injury, the shipbuilder shall take the boat apart and put it together tight at his own expense. The tight boat he shall give to the boat owner.”[[27]](#footnote-27)

In the United States, government regulation on an industry that threatens public infrastructure is nothing new. Driver’s licenses and other government issued licenses have long since added regulation for the sake of civilian safety. Regulation for the sake of security of information relayed wirelessly has long since been a major concern for consumers and developers. An early example of electronic tampering, chronicled in “Hacking at the Royal Institution” by Charolette New, describes a demonstration of Guglielmo Marconi’s wireless telegraph.[[28]](#footnote-28) Marconi had argued that his telegraph system could not be breached by a third party, because the machine required both sender and receiver to tune to the correct frequencies. Competitors of Marconi’s hired Neville Maskelyne, a telegraph enthusiast and professional magician to discredit the system’s fortitude. Maskelyne successfully transmitted an insulting message to Marconi’s telegraph before Marconi’s scheduled transmission, humiliating the inventor and proving to the world that the telegraph could be breached. In the United States, the 1927 Radio Act and the following 1934 communications act were made in-part to ensure that the traffic of amateur radio operators would not interfere with the U.S. military’s radio equipment.[[29]](#footnote-29) Government regulations such as the National Highway Traffic Safety Administration pass regulation that ensures the safety of American automobiles and drivers[[30]](#footnote-30) In researching this topic, I corresponded with Thomas Eorgan, a security manager at Bank of Tennessee who told me that currently any program that transmits currency is subject to government laws and regulations.[[31]](#footnote-31)

*What the Government Should Do and Not Do*

Too much regulation on the IoT development process could easily harm the industry and violate the rights of developers. The freedom of industries to experiment with IoT within their own facilities without the watching eye of government agencies should be seen as an extension of the Bill of Rights’s promise of freedom from unreasonable searches. Furthermore, by ensuring the government has little to no effect on the early development of and IoT product it can be assured that the government will have no ability to interfere with a product’s development and the product’s developer. One possibility lies with the distribution of patents. The U.S. patent office could hire penetration testers to test the software of IoT products. This testing would come at no expense to the taxpayer, because the U.S. patent office is supported solely on fees payed by the inventors of products.[[32]](#footnote-32) Although cost will translate to an increase in the cost of the product, self-regulation or any other alternative to government regulation would likely result in the same conclusion. A product not passing the standard test for IoT security must not be allowed to be sold in the United States. As, such the government must test foreign IoT devices for related security flaws. Testing foreign devices would help to ensure that IoT regulation does not harm the United State’s ability to compete in the global technology market. Foreign developers would most likely recognize the loss in profits their products would suffer for being unable to export to the U.S. Thus, as a consequence of proper IoT regulation, the United States would encourage a global effort to make IoT a safer place for everyone. In a time when electronic information is growing in worth; even becoming integral to public infrastructure, it is important that we consider the appropriate actions of the government toward IoT in the United States. The United States government should regulate the implementation of the Internet of Things on American soil, perhaps by requiring developers to include security and data encryption features in all Internet connected devices they submit for U.S. patent review. IoT devices add impermissible risks to user privacy.

**Conclusion**

The internet has yet more to offer to the citizens of the United States and to the world at large. However, the internet, by nature, is a work-in progress. It has had both good and bad days. The efforts made thus far to make the Internet of Things more secure have been inadequate. The current development of the Internet of Things endangers the safety and privacy of American citizens. The danger grows by the day, and if public utilities and infrastructure in the United States is to be sustained, adequate action must be made. As such, the United States government should regulate the Internet of Things.

End Notes

Samsung.com. “Family Hub”. Online Advertisement. Accessed 14 November 2017. Web.

Federal Trade Commission. *FTC Staff Report: internet of things: Privacy and Security in a Connected World.* January 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Accessed 3 October 2017. Web.

Ngo, Fawn. and Jaishankar, K. “Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime” International Journal of Cyber Criminology. June 2017. <http://cybercrimejournal.com>. Web. Accessed 16 November 2017.

Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017).

Greenberg, Andy, and Kim Zetter. “How the Internet of Things Got Hacked.” *Wired.com*. 28 December 2015. Web. 29 February 2016.

Schneier, Bruce. “Worst-Case Thinking” www.CNN.com. 12 May 2010. Web.

Gilchrist, Alasdair. A Concise Guide to the Internet of Things for Executives (Kindle Locations 129-131). RG Consulting. Kindle Edition.

Balamurugan, S.,Divyabharathi, N., Jayashruthi, K., Bowiya, M., Shermy, R.P., Gokul, Shanker, R. *Internet of Agriculture: Applying IoT to Improve Food and Farming Technology*. International Research Journal of Engineering and Technology. October 2016. [www.irjet.net](http://www.irjet.net). Web. Accessed 9 November 2017.

Balamurugan, S.,Divyabharathi, N., Jayashruthi, K., Bowiya, M., Shermy, R.P., Gokul, Shanker, R. Internet of Agriculture: Applying IoT to Improve Food and Farming Technology. International Research Journal of Engineering and Technology. October 2016. [www.irjet.net](http://www.irjet.net). Web. Accessed 9 November 2017.

Space Daily. “Smart Concrete Could Improve Levees." Space Daily, 27 Sept. 2005. go.galegroup.com. Web. Accessed 15 Nov. 2017.

Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016.

Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016.

Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016.

The Washington Post. “A History of Internet Security.” Washington Post Reporting. 30 May 2015. Web.

The Washington Post. “A History of Internet Security.” Washington Post Reporting. 30 May 2015. Web. 16 February 2016.

Dingman, Shane. *Why Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity. Globe&Mail.*

Dingman, Shane. *Why Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity. Globe&Mail.*

Greenberg, Andy. ““Hackers Remotely Kill a Jeep on the Highway- With Me in It”. 21 August 2015. Wired.com. Web. Accessed 7 November 2017.

Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017).

Garrabrandt, Frank. and Harry Brian. and Sergey Chibizov. Personal interview. 8 January 2016.

Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017).

Thierer, Adam. “Leave the Internet of Things Alone: Don’t Let Government Regulators Stifle Internet Innovation”. [www.U.S.News.com](http://www.U.S.News.com). 12 June 2017. Web. Accessed 9 November 2017.

Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web.

Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web.

Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web.

Federal Trade Commission. *FTC Staff Report: internet of things: Privacy and Security in a Connected World.* January 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Accessed 3 October 2017. Web.

“The Code of Hammurabi” <http://www.constitution.org/ime/hammurabi.pdf> Accessed 15 November 2017

New, Charlotte. *Hacking at the Royal Institution. Rgib.* 11 July 2016. Web. 15 November 2017.

Moschovitis, Christos. And Poole, Hillary. And Schuyler, Tami. And Senft, Theresa. M, “History of the Internet: a Chronology 1843 to the Present”. Moschovitis Group. Santa Varvar, California. 1999. Print.

National Highway Traffic Safety Administration. “Risky Driving”. www.NHTSA.org. Accessed 16 November 2017. Web.

Eorgen, Thomas. Personal E-mail. 15 November 2017.

Intellectual Property Owners Association. “Uptso Funding”. [www.ipo.org](http://www.ipo.org). accessed 16 November 2017.

Works Cited

Balamurugan, S.,Divyabharathi, N., Jayashruthi, K., Bowiya, M., Shermy, R.P., Gokul, Shanker, R. *Internet of Agriculture: Applying IoT to Improve Food and Farming Technology*. International Research Journal of Engineering and Technology. October 2016. [www.irjet.net](http://www.irjet.net). Web. Accessed 9 November 2017.

“Building Cities of the Future.” Business Today 17 Jan. 2016. General OneFile. Web.

5 Jan. 2016.

Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes.” Wired.com. 21 November 2014. Web. 18 February 2015.

Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016.

Clarke, Zuley, James Clawson, and Maria Cordell, Maria. *A Brief History of Hacking.* Historical Approaches to Digital Media. steel.ICCgatech.edu. November 2003. Web. 9 February 2016.

Dingman, Shane. *Why Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity. Globe&Mail*

Eorgen, Thomas. Personal E-mail. 15 November 2017.

Federal Trade Commission. *FTC Staff Report: internet of things: Privacy and Security in a Connected World.* January 2015. https://www.ftc.gov/ system/files/documents/ reports/federal-trade-commission-staff-[report-november-2013-workshop-entitled- internet-things-privacy/150127iotrpt.pdf](https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-%09report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf). Accessed 3 October 2017. Web.

*Garrabrandt, Frank. and Harry Brian. and Sergey Chibizov. Personal interview. 8 January 2015.*

Gilchrist, Alasdair. A Concise Guide to the Internet of Things for Executives (Kindle Locations 129-131). RG Consulting. Kindle Edition.

Greenberg, Andy. ““Hackers Remotely Kill a Jeep on the Highway- With Me in It”. 21 August 2015. Wired.com. Web. Accessed 7 November 2017.

Greenberg, Andy, and Kim Zetter. “How the Internet of Things Got Hacked.” *Wired.com*. 28 December 2015. Web. 29 February 2016.

Intellectual Property Owners Association. “Uptso Funding”. [www.ipo.org](http://www.ipo.org). accessed 16 November 2017.

Moschovitis, Christos. And Poole, Hillary. And Schuyler, Tami. And Senft, Theresa. M, “History of the Internet: a Chronology 1843 to the Present”. Moschovitis Group. Santa Varvar, California. 1999. Print.

National Highway Traffic Safety Administration. “Risky Driving”. www.NHTSA.org. Accessed 16 November 2017. Web.

New, Charlotte. *Hacking at the Royal Institution. Rgib.* 11 July 2016. Web. 9 February 2016.

Ngo, Fawn. and Jaishankar, K. “Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime” International Journal of Cyber Criminology. June 2017. <http://cybercrimejournal.com>. Web. Accessed 16 November 2017.

Samsung.com. “Family Hub”. Online Advertisement. Accessed 14 November 2017. Web.

Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web.

Schneier, Bruce. “Worst-Case Thinking” www.CNN.com. 12 May 2010. Web. Accessed 9 November 2017.

Sterling, Bruce. “The Epic Struggle of the Internet of Things.” Strealka Press, 2014. Kindle.

The Washington Post. “A History of Internet Security.”Washington Post Reporting. 30 May 2015. Web. 16 February 2016.

Space Daily. “Smart Concrete Could Improve Levees." Space Daily, 27 Sept. 2005. go.galegroup.com. Web. Accessed 15 Nov. 2017.

"Researchers Submit Patent Application, 'Enhanced DNS-Based Service Discovery in an Internet of Things (IoT) Environment', for Approval (USPTO 20150341446)." Computers, Networks & Communications 17 Dec. 2015: 1995. Computer Database. Web. 18 Dec. 2015.

Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017).

Thierer, Adam. “Leave the Internet of Things Alone: Don’t Let Government Regulators Stifle Internet Innovation”. [www.U.S.News.com](http://www.U.S.News.com). 12 June 2017. Web. Accessed 9 November 2017.

Wenzel, Scott, L. *Not Even Remotely Liable: Smart Car Hacking Liability.* 2017. University of Illinois Journal of Law, Technology, and Policy. Accessed 7 November 2017. Web.

Zetter, Kim. “How to Hack the Power Grid Through Home Air Conditioners.” Wired. 9 February 2016. Web. 9 February 2016.

1. Samsung.com. “Family Hub”. Online Advertisement. Accessed 14 November 2017. Web. [↑](#footnote-ref-1)
2. Federal Trade Commission. *FTC Staff Report: internet of things: Privacy and Security in a Connected World.* January 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Accessed 3 October 2017. Web. [↑](#footnote-ref-2)
3. Ngo, Fawn. and Jaishankar, K. “Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime” International Journal of Cyber Criminology. June 2017. <http://cybercrimejournal.com>. Web. Accessed 16 November 2017. [↑](#footnote-ref-3)
4. Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017). [↑](#footnote-ref-4)
5. Greenberg, Andy, and Kim Zetter. “How the Internet of Things Got Hacked.” *Wired.com*. 28 December 2015. Web. 29 February 2016. [↑](#footnote-ref-5)
6. Schneier, Bruce. “Worst-Case Thinking” www.CNN.com. 12 May 2010. Web. [↑](#footnote-ref-6)
7. Gilchrist, Alasdair. A Concise Guide to the Internet of Things for Executives (Kindle Locations 129-131). RG Consulting. Kindle Edition. [↑](#footnote-ref-7)
8. Balamurugan, S.,Divyabharathi, N., Jayashruthi, K., Bowiya, M., Shermy, R.P., Gokul, Shanker, R. *Internet of Agriculture: Applying IoT to Improve Food and Farming Technology*. International Research Journal of Engineering and Technology. October 2016. [www.irjet.net](http://www.irjet.net). Web. Accessed 9 November 2017. [↑](#footnote-ref-8)
9. Balamurugan, S.,Divyabharathi, N., Jayashruthi, K., Bowiya, M., Shermy, R.P., Gokul, Shanker, R. Internet of Agriculture: Applying IoT to Improve Food and Farming Technology. International Research Journal of Engineering and Technology. October 2016. [www.irjet.net](http://www.irjet.net). Web. Accessed 9 November 2017. [↑](#footnote-ref-9)
10. Space Daily. “Smart Concrete Could Improve Levees." Space Daily, 27 Sept. 2005. go.galegroup.com. Web. Accessed 15 Nov. 2017. [↑](#footnote-ref-10)
11. Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016. [↑](#footnote-ref-11)
12. Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016. [↑](#footnote-ref-12)
13. Burrus, Daniel. “The Internet of Things is Far Bigger Than Anyone Realizes Part II.” Wired.com. 26 November 2014. Web. 28 March 2016. [↑](#footnote-ref-13)
14. The Washington Post. “A History of Internet Security.” Washington Post Reporting. 30 May 2015. Web. [↑](#footnote-ref-14)
15. The Washington Post. “A History of Internet Security.” Washington Post Reporting. 30 May 2015. Web. 16 February 2016. [↑](#footnote-ref-15)
16. Dingman, Shane. *Why Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity. Globe&Mail.* [↑](#footnote-ref-16)
17. Dingman, Shane. *Why Cybersecurity Matters; Researchers Have Found That Hacking Connected Devices Could Lead to Potentially Stealing One’s Identity. Globe&Mail.* [↑](#footnote-ref-17)
18. Greenberg, Andy. ““Hackers Remotely Kill a Jeep on the Highway- With Me in It”. 21 August 2015. Wired.com. Web. Accessed 7 November 2017. [↑](#footnote-ref-18)
19. Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017). [↑](#footnote-ref-19)
20. Garrabrandt, Frank. and Harry Brian. and Sergey Chibizov. Personal interview. 8 January 2016. [↑](#footnote-ref-20)
21. Riga, Stephen, A. March 2017. *Two Breaches, Two Enforcement Actions, and a DDOS Attack: Data Security and the Rise of The Internet of Things*. *Journal of Internet Law, 2017.Aspen Publishers Inc.* 3. *Academic OneFile*, EBSCO*host* (accessed September 26, 2017). [↑](#footnote-ref-21)
22. Thierer, Adam. “Leave the Internet of Things Alone: Don’t Let Government Regulators Stifle Internet Innovation”. [www.U.S.News.com](http://www.U.S.News.com). 12 June 2017. Web. Accessed 9 November 2017. [↑](#footnote-ref-22)
23. Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web. [↑](#footnote-ref-23)
24. Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web. [↑](#footnote-ref-24)
25. Schneier, Bruce. “Me on the Equifax Breach” 1 November 2017. [www.schneier.com](http://www.schneier.com). Accessed 15 November 2017. Web. [↑](#footnote-ref-25)
26. Federal Trade Commission. *FTC Staff Report: internet of things: Privacy and Security in a Connected World.* January 2015. <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Accessed 3 October 2017. Web. [↑](#footnote-ref-26)
27. “The Code of Hammurabi” <http://www.constitution.org/ime/hammurabi.pdf> Accessed 15 November 2017 [↑](#footnote-ref-27)
28. New, Charlotte. *Hacking at the Royal Institution. Rgib.* 11 July 2016. Web. 15 November 2017. [↑](#footnote-ref-28)
29. Moschovitis, Christos. And Poole, Hillary. And Schuyler, Tami. And Senft, Theresa. M, “History of the Internet: a Chronology 1843 to the Present”. Moschovitis Group. Santa Varvar, California. 1999. Print. [↑](#footnote-ref-29)
30. National Highway Traffic Safety Administration. “Risky Driving”. www.NHTSA.org. Accessed 16 November 2017. Web. [↑](#footnote-ref-30)
31. Eorgen, Thomas. Personal E-mail. 15 November 2017. [↑](#footnote-ref-31)
32. Intellectual Property Owners Association. “Uptso Funding”. [www.ipo.org](http://www.ipo.org). accessed 16 November 2017. [↑](#footnote-ref-32)