IoT Privacy and Security: Necessary Changes For a More Interconnected World

Timothy Kang

Tkang6@hawk.iit.edu

IoT Privacy and Security: Necessary Changes For a More Interconnected World

Computers come in all shapes and sizes with uses that many would have never expected in the past. The devices that can be classified as a computer range from portable devices such as a phone or watch, to household appliances such as a television or refrigerator. Even a car or simple doorbell is no exception to this seemingly limitless list. These devices are now able to connect to the Internet to make up what is known as the Internet of Things (IoT). With the IoT, the world is connected right from our home, but this does not come risk-free in terms of privacy and security. Changes are needed by all parties involved to ensure that this interconnected world is capable of coping with this technology and not end up in a disastrous situation.

Before delving into the shortcomings of the IoT, it is necessary to fully understand the definition of this growing digital system and what it entails. As stated earlier, many of the devices that we see at home, work, school, and other surroundings can be categorized as a computer. When these objects are connected to the Internet and communicating with each other without human involvement, they are now a part of the IoT (Mäkinen, 2015, p.265). This interconnection by means of the Internet allows for the devices to send and receive data and do their programmed tasks. The term IoT can be broadly broken down into the following three components: the Internet, things, and semantic-oriented part (Mäkinen, 2015, p.265-266). The "Internet" is the network framework that is in place, the "things" are the objects within this framework, and the "semantic-oriented part" is "where the things communicate with each other" (Mäkinen, 2015, p.265-266). These three components make up the IoT with the purpose of allowing communication between physical devices to benefit people across the globe. This functionality and the implementation of these components are made possible by the parts of an IoT device.

Many of these devices are not full-blown personal computers with the ability to run high level applications and have multiple functions. However, they all share many parts that lead to their classification as a computer. This includes “sensors that collect data, computing power to figure out what to do with the collected data, and actuators that effect the real world” (Kerner, 2017). These parts allow for these devices to be fully functional once connected to the Internet. This is neither a new nor unpopular technology. The number of devices connected to the Internet are already in the billions and still growing with no signs of stopping. It is expected that there will be “as many as 30 billion devices connected to the Internet by 2020” (“Senators,” 2017, p.6).

There are many different examples of IoT devices out on the market today. One example would be a coffee maker connected to your home Wi-Fi. There is no longer a need to wake up, force oneself to go to the kitchen, and go through the tedious procedures of brewing coffee; simply having an app on your phone that is linked to the coffee maker can allow the person to schedule automated brews to match their morning schedule. Another example would be the Nest’s Thermostat which can help visualize how the parts of an IoT device work together. This thermostat allows for the user to remotely regulate indoor temperatures with a click of a button on their smartphone. It has sensors to find the current temperature or detect if a person is nearby, machine learning to learn habits and automate temperature settings, and actuators to light up the panel to display temperature and time when someone walks by (Poudel, 2016, p.997-998). Clearly, there are many benefits to the user by making things convenient and allowing efficient use of their time.

The IoT architectural model and enabling technologies are important aspects of the IoT that should be considered in order to understand why the IoT risks exist. One model is by an

organization called oneM2M and is split into three layers. The layers consist of the application layer which contains the programs and operational logic, the common services layer which deals with how data is being stored and processed, and the network services layer which deals with functions revolving around connectivity, transport, and service (Poudel, 2016, p.1001). By understanding which part of the model deals with the transit of data, one can pinpoint possible risks of the device. Another thing to take note of is the IoT's enabling technologies and how it makes all of this possible.

Many advancements have been made in the world of information technology and the convergence of these improved technologies allow for the constant growth of the IoT. Hardware improvements are a given such as a sensors, microprocessors, and communications hardware. However, hardware is not the only factor to be considered; these other factors include advancements in big data analytics, the cloud, algorithms for automation, network technologies, IPv6, and accurate GPS technology (Poudel, 2016, p.1003). There are other additional factors such as parts becoming cheaper and Internet connectivity being more accessible, reliable, and faster. The combination of all these factors make up the building blocks of the IoT and has allowed for the IoT to expand and improve over time.

The building block of the IoT is known as a smart object and can be categorized as wearable computing, quantified self, or domotics. Just like what the name implies, wearable computing objects are everyday devices that you wear and these objects "incorporate sensors that can record and transfer data to the device manufacturer" (Mäkinen, 2015, p.266). Smart watches would fall under this category. Quantified self-objects deal with recording information about the individual such as their lifestyles (Mäkinen, 2015, p.266). An example of this are trackers that are put on one's wrist to measure things like heart rate and progress in terms of fitness. The last

category is domotics which is another way of referring to devices used for automation at home or other locations (Mäkinen, 2015, p.266). Having a Google Home alongside a smart television would be an example of this. A majority of IoT devices are encompassed by this category. One important thing to note is that the IoT is not limited to just one device being connected to the Internet. Many devices on the same network are able to interact with one another based on its capabilities which can be a blessing or an issue that cannot be ignored.

There are two major threats stemming from the IoT that must be addressed; the first being threats to the privacy of the user. Smart objects and the device manufacturers collect and use a colossal amount of data. Unfortunately, sensitive information is no exception to the data being collected and used. The collection of sensitive data can be done directly through sensors or done indirectly through inferences (Poudel, 2016, p.1013). Information that is collected directly would include data that is quantified such as one's weight, heartbeat, or the speed that you are traveling at. These examples can be directly observed, calculated, and recorded. On the other hand, inferences can be made based on the data that the device is collecting. This includes driving habits, personality type, and user demographics. For example, an IoT device used for exercising would directly track heart rate per minute, numbers of miles ran, how long it took to run a mile, and how often the user exercises. Based on the data that is collected directly, inferences can be made about the user's overall well-being in terms of health, their age, their gender, their eating habits, and even their personality type. If someone has a high resting heart rate and is incapable of slowly jogging short distances, inferences such as a possible heart condition, high stress levels, and poor diet could be made. This is merely a simple example, and manufacturers that have access to this information with a large sample pool and the computing power to properly analyze this data can make much more accurate and intrusive inferences.

With such personal data being collected, there are obvious consequences that can come as a result. Understanding the amount of data being collected and processed helps with visualizing why these privacy threats exist and how they can negatively impact its users. The FTC had revealed that "fewer than 10,000 households using IoT home-automation products can 'generate 150 million discrete data points a day or approximately one data point every six seconds for each household'" (Tran, 2017, p.268). This is not a statistic that can be taken lightly. One can only imagine the total amount of data being generated by all the IoT devices in use today which will continue to grow every year.

Scholars that specialize in privacy have suggested that this volume of data brings forth issues such as data aggregation and cross-contextual inferences (Tran, 2017, p.268). Data aggregation is when data from multiple sources are combined to create a digital profile for a person. This becomes dangerous in the hands of an organization that uses this information for their own services. It is difficult to paint a complete picture of someone with only sensor data which results in inaccuracies and could be disadvantageous for the person in certain scenarios. For example, if your fitness IoT device determines that you are unhealthy and incapable of following a workout schedule, a health insurance company with this information might change their rates to be higher for that specific user. This is a clear breach of privacy since the user would not have realized that this information is being used to negatively impact them. A digital profile is made and this profile, despite possibly being inaccurate and incomplete, could lead to a very unfortunate situation which brings up the next issue of cross-contextual analysis leading "to unforeseen discrimination problems" (Tran, 2017, p.271).

Inferences regarding one's health or habits based on sensor data could change how an insurance or loan company views their client. An example of this in the corporate world is Target

which provided FitBits to their employees as part of their corporate wellness program. The data collected by the devices were monitored by Fitbit and inferences were made based on data collected outside of work hours such as "sleep patterns or dietary habits" (Tran, 2017, p.273). This information would be used for making corporate decisions such as giving benefits or compensation to the employees. Theoretically, this information could potentially be used in litigation; if the FitBit recorded your location and speed at which you were driving, this could be a determining factor of a car crash claim and be used to determine liability if this evidence is admissible (Mighell, 2014, p.29). Without a doubt, the employees' privacy was being violated for discriminatory reasons despite it being based on data that was collected outside the confines of normal workday hours.

Many consumers know that their privacy is at stake but continue to buy and support the IoT devices because of the features and convenience that comes with utilizing the IoT. Why do these consumers trade away their privacy for convenience? One minor reason revolves around an IoT device's privacy terms and disclosures. Not only can this be difficult to find, but it can also be tedious to read and difficult to fully understand. A Hello Barbie doll by Mattel has a microphone and cloud-based machine learning system to record conversations, transmit it to the manufacturer for research purposes, and evoke different interactions depending on the child. The downside to this data collection and possible intrusion of privacy is that the only way to find out about this function was to read the Privacy Policy and Terms of Use (Schultz, 2016, p.38). However, this reason cannot be used to justify these actions since even if it were easy to find and understand, majority of consumers skip over such terms. A bigger reason for this tradeoff is none other than the lack of federal and state regulations for the IoT.

Unfortunately, the rate at which technology changes is far too fast for the legal framework to catch up with; hence laws and regulations are frequently out-of-date especially in terms of privacy and even security. There are many privacy-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), but these laws "are often too narrowly drafted to cover all implementations of new technologies" such as the IoT (McMeley, 2014, p.71). Simply put, there are no regulations to protect the consumer from privacy-related practices that an organization has in place and there is no reason for there to be any form of transparency as to what is being collected and what is being done with this information.

In addition to the reasons listed above, two behavioral law and economics (BLE) theories can also explain the reasoning behind a user neglecting their privacy. The first behavioral bias is known as unrealistic optimism and the second is hyperbolic discounting. Unrealistic optimism is when an average person believes that he is better than the average denizen and believes, in the case of using an IoT device, that he is "less likely than the average person to experience harm from data loss" (Bailey, 2016, p.1036). This mentality allows for the consumer to underestimate the possible outcomes and take risky actions since they are assuming that they are safe. Hyperbolic discounting is quite different from unrealistic optimism since this is based on how the consumer views the pros and cons depending on how far off a possible outcome is. Since the benefits of using an IoT device is instant and the consequences of giving up privacy could be far off in the future or possibly nonexistent, many prioritize consumption over privacy (Bailey, 2016, p.1036). While these reasons are not applicable to all consumers, it still explains the possible thought process behind a consumer and why privacy is being neglected by many. This thought process could be dangerous as corporations continue to collect data through these

devices. To prevent these digital profiles from being created, companies de-identify the data so the datasets are just information with no face or name behind it. However, this does not mean that the consumer's privacy is safe. Re-identification is possible so the sensitive information could be linked back to the owner (Bailey, 2016, p.1029). Privacy is evidently at risk and this is further enabled by the second major IoT threat which are security threats.

Many news outlets have daily headlines about data breaches, security vulnerabilities, and malware. The IoT is also at risk to this especially as more people rely on such devices. Despite being considered computers, they "usually have minimal computing power" which results in making them "more vulnerable to security breaches than their more familiar cousins: laptops, tablets, and mobile phones" (Ashton, 2017, p.805). There are many security risks with the IoT that should be acknowledged. A data breach is a detrimental risk to both the consumer and seller. Sensors collect a lot of information about the user and this information could be labeled as sensitive. If a hacker gets a hold of this sensitive information due to a security flaw, our privacy is at stake. The seller would also be affected since their reputation would be ruined by having such a flaw in their products. The Federal Trade Commission (FTC) created a report on the IoT security risks and the three forms that it can take.

The three forms are that these risks can enable access for an unauthorized user, allow attacks onto other systems on the network, and create physical risk (Tran, 2017, p.267). Data breaches would fall under the first form which can ultimately lead to the attacker using this elevated access and information to engage in theft, fraud, or other criminal acts. The second form is based on how a network operates and having a vulnerable device on the network could serve as an access point for other systems to be attacked. The third form involves IoT devices that could possible endanger a person such as a car or medical machine. An example of this security

risk would be a modern car. Many parts of a car are controlled by a computer that the manufacturer implemented for reasons such as safety. Unfortunately, this means that someone could hack this system to control the vehicle remotely. Having access to the steering wheel or brakes could result in a fatal accident for the driver (Poudel, 2016, p.1015). This example is not a theoretical scenario, but is an actual flaw that has been exploited by hackers.

There are many reasons why these seemingly simple and sought-after devices have a variety of security risks. The manufacturer's inexperience with properly securing software and hardware is one possible factor. This is amplified by the fact that different stakeholders have different visions and prioritizations when it comes to the IoT; this lack of coordination results in possible flawed or nonexistent security designs during the implementation phase (Poudel, 2016, p.1016). As stated before, lack of processing and battery power are another factor since proper encryption methods are demanding on the processors. In the case where a security vulnerability is found, it is difficult to roll out patches on an IoT device to fix these vulnerabilities. Having unpatched devices allow for the vulnerabilities to continue existing and allow malicious actors to exploit them for a variety of reasons. Before discussing solutions to privacy and security threats, it is necessary to see the current privacy regulations in place in different countries.

In the United States of America, the regulations that are in place differ greatly from those of European countries. The current regulations in the U.S. can be split into existing federal legislation, state legislation, and executive agency enforcements (Tran, 2017, p.273). These laws are focused on privacy and do not pertain completely to the IoT but knowing these regulations will reveal what the country currently has in their arsenal to combat privacy threats. Federal legislation includes acts such as the HIPAA, Fair Crediting Report Act (FCRA), and Children's Online Privacy Protection Act (COPPA) (Tran, 2017, p.274). HIPAA deals with privacy of

health information, FCRA deals with privacy of credit information, and COPPA deals with privacy of information from children. In terms of federal criminal statutes regarding security, the Computer Fraud and Abuse Act (CFAA) exists which deals with cybercrime and protection from unauthorized access to computers. The CFAA has its flaws since "as it currently stands, [it] theoretically doles out the same punishment for sharing one's Netflix password with a friend as it does for selling the password… on the black market" (Ashton, 2017, p.813).

State legislation, as the name implies, is dependent on the state. Some laws state that when a data breach occurs, the company is responsible for alerting all their customers. Unfortunately, these state laws are vague and do not cover the necessary aspects of the IoT. None of these laws take into account the capabilities of a sensor and the sensitive information it is capable of directly collecting or indirectly inferring. The inconsistencies and lack of proper state legislation adds a lot of confusion and gray area for the IoT.

The last type of regulations in the U.S. is executive agency enforcement which simply means regulation by the FTC. They are under the FTC Act which "states that 'unfair or deceptive acts or practices in or affecting commerce' are unlawful" (Tran, 2017, p.276). When TRENDnet provided IoT cameras that recorded live feeds of sensitive information and had gotten compromised, the FTC were able to pursue action against TRENDnet and forced them to create a comprehensive program to mitigate any existing security and privacy vulnerabilities (Tran, 2017, p.277). This instance might have been seen as a victory, but their authority to enforce this all over the country is still lacking and their regulations are seen as ambiguous. In addition, they were only able to take action when many people were affected by the vulnerability; nothing can be done if it were outside the scope of their authority.

In a report about the IoT, the FTC had proposed three recommendations to combat privacy and security risks: data security, data minimization, and notice and choice (Poudel, 2016, p.1016). The first recommendation is to have a high emphasis on security. Actions such as strong encryption, strong authentication, and regularly scheduled patching should be enforced. Data minimization is to de-identify data to ensure digital profiles cannot be created through re-identification. The notice and choice recommendation is to ensure that the consumer understands what is happening to their data and to allow them to consent if the data is being sold or used elsewhere. All organizations should take these recommendations to heart, adjust them to fit their needs, and apply them but this is much easier said than done. Without the proper regulations in place, enforcing such recommendations is extremely difficult.

Privacy and security issues are not only rampant in America. European countries also have the same risks but have a completely different take on regulations. Europe has the Article 29 Working Party (Article 29) that also created a report to address the IoT and list recommendations. The main differences between the recommendations of Article 29 and the FTC are that Article 29 had more recommendations, were "more specific, and [were] tailored to many IoT stakeholders" (Poudel, 2016, p.119-120). In addition to this advisory body, most people associate Europe and data privacy with the General Data Protection Regulation (GDPR) which has changed how the European Union deals with privacy and the protection of data. Before the GDPR, there were many international human rights treaties such as Charter, ICCPR, and ECHR that regulated privacy (Mäkinen, 2015, p.267). These rights defined how there is a right for privacy in one's family and private life but failed to consider the new digital age brought forth by the Internet. GDPR, on the other hand, which came into play on May 2018, accounts for the issues brought by the IoT. The relevant IoT standards relate to "informed

consent, notification duties, privacy by design and privacy by default, data protection impact assessment, algorithmic transparency, automated decision-making, and profiling" (Wachter, 2018a, p.3).

While many privacy and security issues are addressed by the GDPR, it is still lacking in certain aspects due to a conflict between GDPR provisions and how IoT devices and their data controllers work. For example, a sensor is designed to collect an excessive amount information so that the manufacturer could use for numerous possible reasons. This goes against Article 5, 7, and 25 of GDPR. These articles call for data minimalism, informed consent for well-defined purposes, and privacy by design, respectively (Wachter, 2018b, p.271). There are clear benefits of GDPR, but it is also evident that when it comes to the IoT, conflicts between the consumer and manufacturer exist. For a system as big as the IoT, this is one step in the right direction but still lacking and requires more.

Based on the current regulations set by the U.S. and European Union, changes are needed to ensure that our privacy is securely protected. Technology is increasing at a frightening rate and the realm of the IoT is only growing bigger and collecting more private data. With this in mind, the first necessary action that the U.S. must take is for the government to act in order to "have a counter-balancing force for corporate power" (Kerner, 2017). Drafting legislation that pertains specifically to the dangers of IoT should be a given. For example, a bill was drafted in the U.S. to prevent manufacturers from not prioritizing security and selling products that either are not compliant to industry security standards or have known vulnerabilities that should be addressed before it hits the market ("Senators," 2017, p.6). This bill does not take into consideration all of the security and privacy issues, but it is one step in the right direction. Additional government action is needed to protect our data and privacy. One way to remedy

harm to a consumer specifically is to have IoT private tort laws which can be divided into public disclosure of private facts tort and intrusion upon seclusion tort (Tran, 2017, p.263). The private facts tort flexibly applies to the IoT when sensitive data that is collected is distributed elsewhere. Data aggregation and discrimination problems can be remedied using this tort in a scenario where the consumer experiences a negative effect from utilizing the IoT. The seclusion tort is applied when one's seclusion is intruded on. For example, a consumer assumes privacy and seclusion in their home and does not wish to "worry about social and economic consequences" (Tran, 2017, p.295). Intruding into such a private place by collecting data for an inappropriate purpose would allow for this tort to be held in court. These torts, without a doubt, are beneficial in remedying privacy issues even though the torts were not designed strictly for the IoT.

Similarly to other laws, a proper enforcement system should be implemented. It cannot be stressed enough that this enforcement system should be properly adapted to cover criminal and civil wrongs of the IoT. "Cybercrimes raise unique issues not commonly seen in other areas of the law" and appropriate personnel is a necessity to cover such unique issues, which is why specialized enforcement units should be established that consist of jobs like policemen and prosecutors (Ashton, 2017, p.822). The members of the unit should be trained in cybercrime so that they fit the requirements for engaging in cyber-related cases. For example, searching someone's house for physical evidence is a completely different story in a legal sense than searching a hard drive for digital proof. Only those that specialize in this line of work and have the authority to do so should be dealing with anything related to the legality of IoT issues. A civil enforcement regime is also required to make sure companies are keeping up with all of the technological changes and implementing security protocols that could be considered adequate at the very least (Ashton, 2017, p.805). These laws and entities can help deal with cyber-related

crimes and civil cases before and after it happens. In addition, what America needs is to have a GDPR of our own with additional guidelines to fill the lacking areas of this relatively new data privacy regulation.

As with most things, there are pros and cons to GDPR. A three-step transparency model should be applied and added on as additional guidelines to combat weaknesses within GDPR provisions, its governing principles, and known IoT privacy risks (Wachter, 2017b, p.268). The first step is to be transparent with the possible privacy and security risks that come with using the IoT (Wachter, 2017b, p.278). The public should know what they are signing up for by utilizing the IoT and its devices. Then the consumer can make decisions they will not regret in the near future, since they understand and consent to what the devices will do and the possible risks. The second step involves have transparent procedures for mitigating risks regarding identification, profiling, and discrimination (Wachter, 2017b, p.281-282). Users should know the data that is being collected, the inferences that are made, and who has access to such data. Having transparent tools that allow direct access to data collected from the user could have an adverse effect on the company in terms of commercial interests but also allows for a higher ethical standard in which customers can trust in the data controllers (Wachter, 2018b, p.283). The third step is to have transparent contingency plans for when security measures fail and systems become compromised (Wachter, 2017b, p.285). Data breaches and exploitation of security vulnerabilities are common occurrences and our privacy is compromised if this were to happen. There is no guarantee that privacy can be protected completely, which is why transparency regarding realistic expectations is needed. These additional steps and guidelines can be used in conjunction with GDPR to benefit both the consumer and the seller. This solution can also mitigate the BLE biases that causes the prioritization of convenience rather than privacy and

security. After all, understanding the privacy dangers through transparent and mandatory disclosures will prevent people from underestimating the potential threats of using IoT devices and make them think carefully before purchasing an item and connecting it to the Internet. Furthermore, limiting sellers through such regulatory actions will "limit how private data could be used by third parties" and protect consumers without forcing them to consent or take any other actions (Bailey, 2016, p.1052-1053). Without question, government intervention is required to making the IoT sphere a safer place for everyone.

But what should organizations that manufacturer IoT devices and act as data controllers do to protect their company and their clients? The first two steps would be to create a comprehensive privacy and security program that takes the IoT issues into account. Steps that can be taken for the privacy program include identifying legal requirements, assessing risks, incorporating Privacy by Design, limiting the amount of personally identifiable data, giving choices to a consumer related to what information is being collected and shared, placing restrictions when dealing with third-party vendors, educating employees, and regularly reviewing this program to keep it up to date (McMeley, 2014). An information security program is similar but would include the design and implementation of security safeguards and regular testing of these safeguards to test effectiveness (McMeley, 2014). These programs would be meaningless if no actions are taken after designing them. The organization must take proper steps to properly audit these programs and have the employees understand policy violations to keep the company safe from the outside and inside. These organizational programs and practices alongside government regulations are not a fool proof method that will eliminate the privacy and security related issues that plague the IoT. They serve as a starting point that will continue to evolve as time passes and technology changes. Every organization is different, and programs should be

catered to that specific company. All parties involved are at risk if no action is taken which is why regardless of what threat is lingering, appropriate solutions must be implemented. Only by doing so, can the IoT prosper and continue to bring convenience without the need to sacrifice our privacy and security.

We are living in a time where "internet security is now becoming 'everything' security" (Kerner, 2017). Many appliances and devices that we are accustomed to are now able to connect to the Internet where sensors collect data indiscriminately. It can be scary to many of how our homes contain objects that are designed to make our lives easier, but also invade our privacy. The IoT has flaws dealing with privacy and security, but this does not mean it is a failing system that should be removed from existence. For the unforeseeable future, it will continue to grow which is why immediate action is needed. It will not be a wasted effort to try and protect our private data by passing government enforced regulations and implementing strong security and privacy programs in an organization. This will allow everyone to overcome the shortcomings of the IoT and continue to enjoy this interconnected world.

References

Ashton, M. (2017). Debugging the Real World: Robust Criminal Prosecution in the Internet of Things. *Arizona Law Review*, *59*(3), 805–835.

Bailey, M. W. (2016). Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things. *Texas Law Review*, *94*(5), 1023–1054.

Kerner, S. M. (2017). IBM's Schneier: It's Time to Regulate IoT to Improve Cyber-Security. *EWeek*, 1.

McMeley, C. S. (2014). Protecting Consumer Privacy and Information in the Age of the Internet of Things. (Cover story). *Antitrust Magazine*, *29*(1), 71–77.

Mäkinen, J. (2015). Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things. *Information & Communications Technology Law*, *24*(3), 262–277. https://doi-org.ezproxy.gl.iit.edu/10.1080/13600834.2015.1091128

Mighell, T. (2014). The "Internet of Things" in Law Practice. *Law Practice: The Business of Practicing Law*, *40*(3), 28–29.

Poudel, S. (2016). Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security. *Berkeley Technology Law Journal*, *31*, 997–1021. https://doi-org.ezproxy.gl.iit.edu/10.15779/Z38PK26

Schultz, J. (2016). Law and Technology The Internet of Things We Don't Own? *Communications of the ACM*, *59*(5), 36–38. https://doi-org.ezproxy.gl.iit.edu/10.1145/2903749

Senators to Introduce Bill to Secure Internet of Things. (2017). *Information Management Journal*, *51*(5), 6.

Tran, A. H. (2017). The Internet of Things and Potential Remedies in Privacy Tort Law. *Columbia Journal of Law & Social Problems*, *50*(2), 263–298.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, *34*(3), 1-22. https://doi-org.ezproxy.gl.iit.edu/10.1016/j.clsr.2018.02.002

Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation & Technology*, *10*(2), 266–294. https://doi-org.ezproxy.gl.iit.edu/10.1080/17579961.2018.1527479