The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2018

Volume 10, Pages 68-76

ICRES 2018: International Conference on Research in Education and Science

A Critical Analysis on Internet of Things: Features and Vulnerabilities

Naciye Guliz UGUR
Sakarya University

Merve TURKMEN BARUTCU
Sakarya University

Abstract: Smart devices have completely changed how society functions both outside and inside the home. A major concern is the Internet of Things (IoT), and the lack of awareness by the public of the limited data security built around IoT devices (Raggett, 2016). The purpose of this research is to investigate how a reliance on IoT devices within the home can come at the expense of personal privacy. There has been limited research conducted on how much, and what data is transmitted by IoT devices. This research focused upon data privacy and security concerns, privacy laws, law enforcement capabilities and legal precedents pertaining to personal privacy and IoT devices. The storage, transmission, sharing and retention of personal information through connected devices were found to pose substantial privacy concerns. There is a deficiency in public knowledge on the subject of IoT because people are putting a greater emphasis on functionality and design with these IoT tools that provide ease of life, but less regard for their own individual privacy. People may have reached a point where they have allowed too many other entities such as government, corporations, and data aggregators access to their personal information but limited knowledge as to what is being transmitted. Based on the research it seems that humans put a lesser value on their own privacy and personal information because the world around them is consumed by a pursuit of things like vanity, pleasure, and enjoyment. Companies should be required to provide a baseline explanation in detail exactly what, where, how, who, and anything else relating to the data transmission that contains any personal information about the consumer using the device. For anybody who doesn't have a working knowledge of what that traffic should look like, it should be explained in reasonable terms so those who are not technical can understand the data capture.

Keywords: Cybersecurity, Internet of things, IoT, Privacy, Security

Introduction

The IoT has been defined as "a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction" (Rouse, 2016). These devices can range from simple light bulbs and smart plugs that can remotely turn on a coffee machine or crockpot, to more advanced devices like the Amazon Echo, Smart TVs, home surveillance systems, and wearable technology. The list is ever expanding but the point is that these devices all communicate information back to the manufacturer. Researchers at Norton, the well-known antivirus company owned by Symantec, describes how these devices are transmitting out personal information. "The personal data collected and stored with these devices, such as your name, age, health and location can aid criminals in stealing your identity" (Symantec, 2017). Technology costs to the consumer decrease over time but people must consider that the cost savings may be due to profits companies receive from selling data.

There are many deficiencies in research around transmitted data. The average home Internet user does not take time, nor have the technical know-how to monitor their own network traffic, and even so, if the data is encrypted, he or she would not be able to read the information that is being communicated. An average home could be using more than ten home smart devices accessing the Internet simultaneously and this is a growing number. It is estimated that there will be 24 billion IoT devices connected to the Internet by 2020 (Mehta, 2017).

- This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

- Selection and peer-review under responsibility of the Organizing Committee of the Conference

© 2018 Published by ISRES Publishing: www.isres.org

Using a typical family of four as an example, some sample IoT devices found in the home of 2017 may include a Sony PlayStation 4, Microsoft Xbox One X, Samsung SmartTV, HP desktop computer, Lenovo work laptop, Apple Macbook personal laptop, spouse's Chromebook work laptop, child's Leapster tablet, Amazon Echo, Amazon Echo Dot, Amazon FireTV, a TP-Link Smart Plug, an Amazon Kindle Fire tablet, multiple Apple mobile phones, Canary app controlled home surveillance camera, Ecobee3 smart thermostat, wearable fitness trackers, the list goes on.

The purpose of this research was to investigate how a reliance on IoT devices within the home can come at the expense of personal privacy. There has been limited research conducted on how much, and what data is transmitted by IoT devices. This research focused upon data privacy and security concerns, privacy laws, law enforcement capabilities and legal precedents pertaining to personal privacy and IoT devices. The storage, transmission, sharing and retention of personal information through connected devices were found to pose substantial privacy concerns.

Literature Review

The scope of this literature review investigates how using IoT devices within the home forces users to make tradeoffs for increased quality of life at the expense of personal privacy and security.

IoT Framework

The Internet of Things (IoT) can be referred to in its simplest form as a network of Internet connected devices. These devices have the ability to operate independently of human interaction in some capacity and have autonomous functions and features (Weber, 2016). IoT devices are able to capture data using human input, and with that input perform their own autonomous functions and execute decision-making capabilities that do not require human participation. In comparison to the Internet, IoT can be thought of as "the future Internet for the new generation, integrating sensory, communications, networking, and service and intelligent information processing" (Li & Xu, 2017).

In 1999, home computers were independently operated and were controlled physically. However, now that society has reached the age of IoT "each connected device could be a potential doorway into the IoT infrastructure or personal data" (Li & Xu, 2017). Meaning that today's world devices can be remotely controlled using other devices, either through an app, a programmed schedule, mobile phone or even another IoT device, taking much less, but not a complete absence of human interaction to operate. This leads into the main purpose of the IoT's existence and that is to improve the quality of life for the user by making manual tasks more automated.

The architecture of IoT technology must be understood to grasp the privacy and security implications inherent in its use. What was once a networked way to locate and inventory items within a warehouse using RFID (Radio-Frequency Identification) has evolved into what is now the IoT, connecting billions of devices through a layered architecture with each layer associated with a specific function. Connectivity, and subsequent security and privacy are impacted by the various layers of this access. This is important to understand because the IoT currently suffers from poorly designed and implemented IoT systems, a lack of standards for authentication, no best practices, no established methods for achieving situational awareness of security posture, and numerous other shortcomings (Li, S., & Xu, L., 2017).

The many methods, layers, applications, etc. used by these devices, including the various acronyms and functions are technically challenging to understand for a basic user with no working knowledge of network protocols. However, that same user is relying on these processes for their devices to function. Within some of these layers, the data collected and stored by the device might be used by a specific protocol that transmits personal data back to the manufacturer. Additionally, a vulnerability might exist that can be exploited to hack the device.

With all of the various layers used in IoT devices, security authentication is a big concern. It is generally agreed that IoT devices require secure authentication, secure bootstrapping and data transmission, security of IoT data, and secure access to data by authorized persons (Borgia, 2014). IoT device hacking has already occurred in baby monitors, refrigerators, thermostats, cameras, and firearms to name a few (Banafa, 2014). Now, consider that there are not just billions, but tens of billions of devices, each with their own IPv6 address (Borgia, 2014).

IoT has expanded into today's society in a number of ways. A simple look at industries most heavily invested in IoT include manufacturing (highest), then transportation and utilities, followed by healthcare, and consumer electronics and cars (DeNisco, 2017). Questions remain unanswered about how the growing infrastructure will handle the simultaneous communication of tens of billions of devices. Questions to be answered include what happens when the devices are weaponized, which has occurred in cases like the Mirai malware. First, in order to effectively demonstrate the trade-offs of privacy and security, this research reviewed how these devices have improved our lives in many ways.

IoT as Ease of Life

When humans create tools, it is due to a drive to accomplish a task in a more efficient way. Televisions, computers, pedometers, security systems, plugs, home thermostats, refrigerators, and much more have emerged from a necessity to make processes or information gathering simpler, more efficient, or more convenient. As of 2017, all of the devices listed above now have autonomous and remotely controllable variants that allow consumers to access and manage these devices in new and unique ways. A concern is how fast these devices are being added to our surroundings, both in number and in scope. The IoT is changing the way people work, live, and play, and societies around the globe are gaining a greater ability to control their environments to suit their personal needs and preferences (Mehta, 2017).

A Federal Trade Commission (FTC) report (2015) states that 2009 was the year that the number of 'things' connected to the Internet surpassed the number of people. These devices are specifically IoT devices that capture and transmit information back to a third party. In addition to Mehta's report that over 24 billion devices would be installed throughout the world in 2020, today, in 2017 it is predicted that 5.5 million new IoT devices are being added to the Internet every day (Mehta, 2017).

Industry leaders and IT professionals have much to say about investing in IoT in 2017. Gartner, a leading research and advisory company, claims by 2020 more than half of new businesses will incorporate elements of IoT. They also estimate that the black market will comprise more than $5 billion in fake video and sensor data to consumers, and addressing compromises with IoT security will require a 20% increase in annual security budgets (Panetta, 2016). However, when digging deeper into these figures, although it is estimated that more than 25% of identified enterprise attacks involve IoT devices in 2020, IoT will only account for 10% of the total IT security budget (Gartner, 2016).

Privacy Concerns

One of the examples of a device that has had significant impact on the way people think, influenced opinions and has increased American materialism through advertising, is the television, and what better window into how the average human spends his or her time than to target personal information about television usage. Sarah Perez, (2017) a writer for Tech Crunch, quotes a December 2016 analysis by Flurry that the average person spends up to five hours per day on mobile devices, and John Koblin of the NY Times writes that Americans watch "on average 19 fewer minutes of TV a day, than they did two years ago" (Koblin, 2016). Possible reasons for this could be because of the streaming services and absence of commercials, therefore less time required to finish a TV show. Breaking this down, 20% of the average human's daily practices can be digitized and analyzed for some type of further analysis. A more compelling question to answer is what information IoT devices such as SmartTVs are transmitting and how that information is used.

The factor that makes organizing this data less cumbersome is that we no longer live in a world where people are required to sit back and flip through endless channels to find something to watch. SmartTVs and other media devices come loaded with video streaming apps like Hulu, Netflix, Amazon Video, and many others. This makes analyzing what someone watches and making a clear determination such as "x" person spends an above average time watching horror, suspense, mystery, crime, politics, or comedy, etc. much easier. For example, "a Vizio [SmartTV] records the date, time, and channel watched. Vizio takes all that data and connects it to the IP address. With that much data, any big data analyst can know more about you than your family does" (Vaughan-Nichols, 2017). Vizio is a known media product for most consumers. However, consumers should be aware of the potential risk of purchasing devices and products from venues not associated with trusted manufacturers such as Apple, Microsoft, Dell, etc. Thousands of such items are available on eBay and other Internet sources, generally from unknown vendors and in some instances, vendors from outside the United States. Elizabeth Montalbano, of The Security Ledger, explains that IoT devices are like any other computer, yet include limited protections against malware, and sometimes contain no or limited ability to change the default password (Montalbano, 2017).

One situation regarding exfiltrated data using IoT technology was the Mirai botnet, which successfully hijacked devices by scanning the Internet for IoT systems protected by factory default or hard-coded usernames and passwords (Massive Media, 2017). The malware was able to install itself and create a backdoor directly on a home router, which is the hub that transmits all of the information from all of the devices connected on a home network out to the Internet. This malware proved that IoT devices can be infected, reprogrammed, and used in tandem to create one of the biggest distributed denial of service attacks (DDoS) ever recorded. Hackers were able to control a botnet army of IoT devices due to lacking security measures implemented on these devices. Twitter, PayPal and Verizon were some of the targets and experienced site outages due to this DDoS botnet attack (Newman, 2017).

This was a global attack, targeting both the east and west coast United States as well as Europe (Thielman & Hunt, 2016) and worked by creating a command and control center containing a MySQL database of all of the infected IoT devices. Furthermore, unless a person was analyzing the traffic from his or her specific IoT device, the botnet attack coordinated from the person's home network was almost undetectable.

Danny Palmer (2017), a writer for ZDNet explains how the default username and password can be a challenge to change on IoT devices such as wireless toasters, smart plugs, and thermostats. "Users might not have any idea how to change them, and, vendors are hard-coding usernames and passwords into devices without giving users the ability to change them" (Palmer, 2017). The password prompt is not displayed in a way that is shown with each use, as it is when a person logs into their email, mobile phone, and personal computer, or maybe it was only accessed once, when the device was originally set up.

On the other hand, companies such as Apple and Google want to learn all they can about their users to market products and services and sell that data to others (Wadhwa, 2015). Many are embracing the IoT but very few understand how to secure the billions of devices of varying types, sizes and functions. Many cannot fathom the ramifications that could present themselves now that autonomous IoT devices are being integrated into critical infrastructures such as utilities and communications. An example of this can be found by using advanced Google searching to locate unsecured critical infrastructure devices available for public viewing and potential modification (Talamantes, 2016). Connecting exponentially vulnerable devices opens these devices up to a swarm of potential cyberattacks, or vulnerable devices could be added to a zombie army or botnet, exfiltrating personal data from well-known and trusted companies.

Every day, IoT devices are passively collecting data, which can fall into the wrong hands. These devices are talking to each other while interacting with the environment, unbeknownst to the owner. Individuals are now beginning to comprehend the serious privacy threats, and society as a whole is realizing that the technology is not fully transparent. March 11, 2017 was the 28th anniversary of the Tim Berners-Lee proposal for the World Wide Web. Berners-Lee originally imagined the web as an open platform to share and collaborate across geographic boundaries, however, one of the major trends that has worried him in recent times is that people have lost control of their personal data (Berners-Lee, 2017).

Humans have little problem with some personal information being collected in exchange for free services. The problem is that the data being captured by devices is out of human sight and control. Thereby, people are giving up the benefits of being able to choose when and where that data is shared (Berners-Lee 2017). People may not know who the third parties are that companies are selling the data to, and it is impossible to accept only part of the terms and agreements, leaving consumers with little choice other than to not use the product at all, even if that product is considered a killer-app or life optimizing technology. Humans understand that privacy is valuable, but on an individual basis they may not attempt to quantify it against the value of services received by an IoT device (Turgut & Bölöni, 2017).Therefore, the users of IoT products may make the wrong choices when faced with an excellent product yet declining to use it because that particular company may freely give data to third-parties. While on the opposite end of the spectrum, people may be willing to give up too much privacy for a product that serves little purpose (Turgut & Bölöni, 2017).

Security Concerns

Over the past decade, people have more frequently fallen victim to security breaches across the financial, retail, healthcare, technological, and industrial sectors as well as many others. These security breaches occur by way of malicious attack, human error, or system glitch (Ponemon Institute, 2017). IoT has opened up a wide door, and the variety of new devices and processes to target a victim compound the difficulties of understanding the how, why, and who questions of remediation. These devices that contain personal data may be controlled by proprietary operating systems, unavailable to view by the consumer, but for the hacker, a particular device or flawed code makes for a tempting target to study. For example, the article Computer Security and the Modern Home by Denning, Kohono, & Levy, describes how burglars can target a connected door lock to plant hidden access codes, and arsonists can target a smart oven to cause a fire at the victim's home (as cited in Fernandes, Jung, & Prakash, 2016). Additional IoT security shortcomings are evident in the hacking that has also occurred in newer IoT devices such as baby monitors, refrigerators, thermostats, cameras, and even assault rifles (Banafa, 2017).

Privacy Agreements

Privacy agreements are important yet humans tend to click quickly through them when installing an exciting new app, opening a technology gift or testing out a digital service offering in order to get to use the device faster. According to a Fairer Finance survey "the small print for some companies now runs more than 30,000 words and [out of a sample of 2000 people] 73% admit to not reading the fine print. Of those who do, only 17% say they understand it" (Glancy, 2014). This study was followed up by another in 2017 where it was calculated that reading an average American's digital contracts would take almost 250 hours a year (Berreby, 2017). Teena Maddox (2015), a cybersecurity writer for TechRepublic explains that agreeing to share your data with one company doesn't mean that company will be in business next year, or new laws could be passed that change who has access to the data a person willingly gave up his or her privacy rights to share. This opens up a number of additional questions regarding all of the privacy agreements the average American has signed over the course of the past twenty years such as what happens to personal data when a business closes its doors permanently or is purchased by another company.

Consumers are giving up privacy bit by bit because consumers are unaware of what they are signing over when they agree to a company's terms and privacy agreements. When users first started accessing the Internet, information collection practices were simpler. Companies would accept purchase forms that included information for payment and address to accomplish reasonable tasks such as order processing and customer service. If a consumer received subsequent marketing information that was unwanted, he or she could opt out or have themselves added to a do-not-call list (Brill, 2017).

Today, social media companies may provide what is referred to as a privacy notification when a user posts content, like a picture or a post, which is a second prompt that notifies the user that what he or she is about to share will be public. There are little to no privacy notifications with IoT devices. "As the boundaries defining privacy are challenged, it creates uncertainty for businesses and consumers that are part of the economy of IoT" (Brill, 2017). The problem is compounded when a company's privacy agreement is not extensively examined nor fully understood by a user. Referencing the Fairer Finance survey, the small print for some companies runs more than 30,000 words. Additionally, 73% of 2000 people surveyed admitted to not reading the fine print. Of those that did read the contracts, it was found that only 17% said they understood the details (Glancy, 2014). Another study in 2017 calculated that in total, the average American is skipping over 250 hours' worth of digital contract reading every year (Berreby, 2017).

Data Breaches

The average person uses a mobile phone, personal computer, and now, through the linking of smart devices such as the Amazon Echo and other home IoT products, he or she can access financial data, transactions, and credit scores through voice and home mobile connectivity. With the increasing number of IoT devices comes a greater capability for data leakage. There exists a lengthy history of data breaches involving major corporations in the United States such as Anthem, BlueCross, Yahoo, JP Morgan, Target and many more (Lord, 2017). Heidi Daitch (2017), a data breach analyst for IdentityForce states that in 2017 alone there have been more than thirty data breaches considered to be major breaches. One of the worst in history occurred on September 7, 2017: Equifax Inc. announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017 (Equifax, 2017).

As of September 2017, Equifax has offered over 143 million customers complimentary credit reporting when signing up through TrustedID Premier. This service provides the affected consumers with the following: Equifax Credit Report; Equifax Credit Report Lock, which allows consumers to prevent access to their Equifax credit report by third parties; three bureau credit file monitoring, which alerts users to changes in Experian, TransUnion, and Equifax reports; social security monitoring, which searches suspicious web sites for their social security numbers; and also $1 million in identity theft insurance (Equifax, 2017). One key point to note is that with this service, like other technical services, it requires personally identifiable information to register. More importantly, each of the users signing up for this complementary service must agree to a brand new set of privacy agreements.

Law Enforcement Considerations

Law enforcement IoT concerns can be isolated to the technical problems of investigating crimes and the legal problems dealing with warrant scope. Jurisdictional issues arise as to where Internet crimes are to be prosecuted, and also become far more complicated due to the anonymity and global nature of these crimes. Many different areas come into play such as infringement on constitutional rights of consumers using IoT devices. Topics include prior lower court decisions as well as past and pending U.S. Supreme court decisions, such as United States v Jones (2012) and United States v Carpenter (2017), evidence gathering associated with Third-Party Doctrine issues, and other complex IoT legalities.

Wearable IoT devices can be used as evidence in court, especially insurance fraud cases. In the article The Dark Side of Wearables, Teena Maddox quotes Karhrman Ziegenbein, CEO of Toonari Corp "Once it's known that the defendant uses a wearable device, it's considered transactional data. You can subpoena this data or get it through discovery" (as cited in Maddox, 2015). For example, a person could claim to be on disability or disabled due to an automobile crash, yet data obtained from a victim's IoT device such as a fitness tracker, which indicated daily or extended use, would bring such disability claims into question.

Previous Cases And Precedents

IoT devices have recently been used as evidence in both civil and criminal cases by both prosecution and defense. Although IoT has proven successful in cracking many different types of cases, its use has also brought to light many constitutional and privacy concerns (Zatz, Meadows, Aradi, Mathis, 2017). With IoT devices such as smart speakers, fitness wearables, pacemakers, and biometric devices, courts in Illinois have sustained claims and approved settlements of consumer cases brought against technology companies for violating privacy laws due to using and sharing personal identifiers like fingerprints, facial and retinal scans as well as voiceprints (Zatz et al., 2017). Some acts such as the IoT Cybersecurity Improvement Act of 2017 established minimum security standards for IoT devices sold to the U.S. government (Martin, Meade, & Nusraty, 2017). However, these acts are specifically written to protect the U.S. government and not the consumer.

Conclusion and Recommendations

The purpose of this research was to investigate how a reliance on IoT devices within the home can come at the expense of personal privacy. There has been limited research conducted on how much, and what data is transmitted by IoT devices. This research focused upon data privacy and security concerns, privacy laws, law enforcement capabilities and legal precedents pertaining to personal privacy and IoT devices. The storage, transmission, sharing and retention of personal information through connected devices were found to pose substantial privacy concerns.

The importance of researching privacy issues relating to IoT devices serves the following purpose. It provides knowledge and actual analysis of privacy issues relating to IoT devices and sheds light on the actual information some of these IoT devices are transmitting. Furthermore, privacy agreements glanced over by the average consumer results in confusion, unawareness, and potential legal issues. This topic is extremely important to consider because there appears to be a deficiency in public knowledge on the subject of IoT because people are putting a greater emphasis on functionality and design with these IoT tools that provide ease of life, but less regard for their own individual privacy. People may have reached a point where they have allowed too many other entities such as government, corporations, and data aggregators access to their personal information but limited knowledge as to what is being transmitted. This information being transmitted may have been approved by a person quickly skipping over a privacy agreement, however, if the person knew the specifics they might conclude the information is too personal. Additional justification includes providing the public a better understanding of the government and law enforcement's reach regarding admissible evidence from IoT devices, and how their Fourth Amendment rights are affected. What makes this more significant is in cases where the interests of the nation supersede the respect to privacy for an individual.

IoT is a new age of computing and has effectively changed how people interact with technology across many areas of life such as work, play, and sleep. However, even though people place such a strong reliance on these devices, they don't treat them with the same scrutiny as typical computer systems, and both users and manufacturers have neglected to place the priority on securing them from malware and hackers. One of the critical failures that was mentioned by Elizabeth Montalbano was that IoT devices include limited protections against malware, and sometimes contain no or limited ability to change the default password (2017). This prevents the ability to lock IoT devices down with a first line of defense, and results in a more vulnerable product. With typical computers it is common for even a non-technical user to navigate a slow PC system and state that it's bogged down with a potential virus or spyware. However, it is highly unlikely for a user to even notice one of their many IoT devices being hacked. A user might simply state something like "Alexa is just working slow today." Meaning, the home assistant response slowness may in fact be a successful hack where a user's prompts are being distributed to an unauthorized location, but it is not realized by the user.

Taking the time to analyze the summary of personal information captured across IoT devices discovered in this research should cause alarm for anyone using these products. Kevin Curran stated that now that there are millions of home IoT devices connected, and analyzing and monetizing consumer data is both possible and lucrative. This is especially true when combining this data with predictive modelling (Kevin Curran, as cited by Maddox, 2017). With more time, comes more data, and with more data comes more accurate analysis, which essentially makes the data more valuable. Can it be speculated that trend analysis, say five years' worth of combined fitness data, could paint a picture that society as a whole is exercising more? Or, when purchasing multiple data sets across multiple manufacturers, a single company with unlimited resources could have a firm grasp on where, when, and what people are doing with all of their time.

Based on the research it seems that humans put a lesser value on their own privacy and personal information because the world around them is consumed by a pursuit of things like vanity, pleasure, and enjoyment. In this world, the privacy breaches that have become so prevalent in recent years won't matter. "Customers are persuaded that the IoT devices provide a value that exceeds their physical and privacy costs" (Turgut & Bölöni, 2017). In fact, breaches will simply become a routine way of life, and if the information is already out there, does it make a difference what additional parties have access to it? Who cares as long as the product still functions and a new model is coming soon.

It has been researched how serious the privacy and security implications are and below list a few recommendations for improving the IoT privacy and security landscape. One of the first recommendations is that companies should be required to provide a baseline generic John Smith packet capture that explains in detail exactly what, where, how, who, and anything else relating to the data transmission that contains any personal information about the consumer using the device. For anybody who doesn't have a working knowledge of what that traffic should look like, it should be explained in reasonable terms so those who are not technical can understand the data capture. Recommendations include muting the devices when not in use, and when setting up a device use fake personal information. This may seem excessive, but each person could essentially create a masked profile. By using different credentials, it will add an additional layer of protection for the true information. Also, historical data used by a manufacturer must be limited in duration held.

References

Banafa, A. (2014). IoT Standardization and Implementation Challenges. IEEE. org Newsletter.

Berners-Lee, T. (2017). I invented the web. Here are three things we need to change to save it. Retrieved March 11, 2017. from https://www.theguardian.com/technology/2017/mar/11/tim- berners-lee-web-inventor-save-internet

Berreby, D. (2017). Click To Agree With What? No One Reads Terms Of Service, Studies Confirm. Retrieved March 03, 2017. from https://www.theguardian.com/technology/2017/mar/03/terms-of- service-online-contracts-fine-print

Borgia, E. (2014). The Internet of Things Vision: Key Features. *Applications And Open Issues Computer Communications*, 54, 1–31.

Brill, H. (2017). What Rules Apply to Information Privacy and the Internet of Things?. *The Santa Clara High Technology Law Journal.* Retrieved 29 October, 2017. from https://techlawquestions.com/home/2017/7/17/what-rules-apply-to-information-privacy- and-the-internet-of-things.

Daitch, H. (2017). 2017 Data Breaches - The Worst Breaches, So Far. *IdentityForce*. Retrieved September 29, 2017. from https://www.identityforce.com/blog/2017-data-breaches

DeNisco, A. (2017). The Five Industries Leading The Iot Revolution. Retrieved June 23, 2017. from http://www.zdnet.com/article/the-five-industries-leading-the-iot-revolution/

Equifax Inc. (2017). Equifax Announces Cybersecurity Incident Involving Consumer Information. Retrieved December 29, 2017. from https://investor.equifax.com/news-and-events/news/2017/09- 07-2017-213000628

Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security Analysis Of Emerging Smart Home Applications. *In Security and Privacy (SP*), 2016 IEEE Symposium on (pp. 636-654). IEEE.

FTC (2015). The Internet of Things: Privacy and Security in a Connected World. Retrşeved 01 March 2018. from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Gartner (2016). Gartner Says By 2020, More Than Half Of Major New Business Processes And Systems Will Incorporate Some Element Of The Internet Of Things [Press release]. Retrieved 23 June, 2017. from https://www.gartner.com/newsroom/id/3185623

Glancy, R. (2014). Will You Read This Article About Terms And Conditions? You Really Should. Retrieved April 24, 2018. from https://www.theguardian.com/commentisfree/2014/apr/24/terms- and-conditions-online-small-print-information

Koblin, J. (2016). How Much Do We Love TV? Let Us Count the Ways. Retrieved 22 October, 2017. from https://www.nytimes.com/2016/07/01/business/media/nielsen-survey-media-viewing.html

Li, S., & Xu, L. (2017). Securing The Internet Of Things. Cambridge, MA: Syngress.

Lord, N. (2017). The History Of Data Breaches. Retrieved July 27, 2017. from https://digitalguardian.com/blog/history-data-breaches

Mehta, R. (2017). How The Iot Will Explode At 2020. Retrieved August 19, 2017. from http://customerthink.com/how-the-iot-will-explode-at-2020/

Maddox, T. (2015). The dark side of wearables: How they're secretly jeopardizing your security and privacy. Retrieved January 19, 2018. from http://www.techrepublic.com/article/the-dark-side-of- wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/

Martin, J., Meade, C., & Nusraty, W. (2017). A Summary Of The Recently Introduced Internet Of Things (Iot) Cybersecurity Improvement Act Of 2017. Retrieved October 04, 2017, from https://www.insideprivacy.com/data-security/cybersecurity/a-summary-of- the-recently-introduced-internet-of-things-iot-cybersecurity-improvement-act-of-2017/

Massive Media. (2016). Mirai Malware: How To Protect Yourself From The Internet Of Things (Iot Exploit). Retrieved October 31, 2017. from https://www.massivealliance.com/2016/10/31/mirai-malware-protect-internet-things-iot- exploit/

Montalbano, E. (2017). 300 Billion Passwords? Internet Of Things Growth Poses Unprecedented Threat By 2020. Retrieved February 01, 2018. from https://securityledger.com/2017/02/300- billion-passwords-internet-of-things-growth-poses-unprecedented-threat-by-2020/

Newman, S. (2017). Service Providers: The Gatekeepers Of Internet Security. *Network Security*, 5, 5-7. doi:10.1016/s1353-4858(17)30048-x

Palmer, D. (2017). Is 'Admin' Password Leaving Your Iot Device Vulnerable To Cyberattacks? Retrieved April 26, 2018. from http://www.zdnet.com/article/is-admin-password-leaving- your-iot-device-vulnerable-to-cyberattacks/

Perez, S. (2017). U.S. Consumers Now Spend 5 Hours Per Day On Mobile Devices. Retrieved March 3, 2018. from https://techcrunch.com/2017/03/03/u-s-consumers-now-spend-5-hours- per-day-on-mobile-devices

Ponemon Institute (2017). 2017 Cost of Data Breach Study: United States. 12, 4-5, Retrieved October 09, 2017. from https://www- 01.ibm.com/marketing/iwm/dre/signup?source=urx-15764&S_PKG=ov58458

Rouse, M. (2016). What is Internet of Things (IoT)? Retrieved March 12, 2018. from http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Symantec (2017). Securing the Internet of Thing. Retrieved January 6, 2018. from https://sg.norton.com/internetsecurity-iot-securing-the-internet-of-things.html

Talamantes, J. (2016). Google Dorking And Shodan. Retrieved from November 9, 2017. http://www.elp.com/articles/powergrid_international/print/volume-21/issue- 11/features/google-dorking-and-shodan.html

Thielman, S., Hunt, E. (2016). Cyber Attack: Hackers 'Weaponised' Everyday Devices With Malware. Retrieved October 22, 2017. from https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised- everyday-devices-with-malware-to-mount-assault

Turgut, D., Bölöni, L. (2017). Value Of Information And Cost Of Privacy In The Internet Of Things. *IEEE Communications Magazine*, 55(9), 62-66.

Vaughan-Nichols, S. J. (2017). How To Keep Your Smart TV From Spying On You. Retrieved March 8, 2017. from http://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying- on-you/

Wadhwa, V. (2015). When Your Scale And Fridge Conspire To Make You Lose Weight, The Internet Of Things Will Have Gone Too Far. Retrieved June 29, 2017. from https://www.washingtonpost.com/news/innovations/wp/2015/06/29/when-your-scale- and-fridge-conspire-to-make-you-lose-weight-the-internet-of-things-will-have-gone-too-far/?utm_term=.6ffbbfc4131c

Weber, R. H. (2016). Governance Of The Internet Of Things—From Infancy To First Attempts Of Implementation?. *Laws*, 5(3), 28.

Zatz, C. J., Aradi, L. O., Meadows, J. L., & Mathis, P. (2017). Recent Iot Device Cases. Lexology. Retrieved July 29, 2017. from https://www.lexology.com/library/detail.aspx?g=97b70db8- b67d-4e8b-b9bf-d4beaf12eddd

Author Information

Naciye Guliz Ugur
Sakarya University
Sakarya Business School, Sakarya/Turkey
Contact e-mail: ngugur@sakarya.edu.tr

Merve Turkmen Barutcu
Sakarya University
Sakarya Business School, Sakarya/Turkey