Fall 2023

Smart Homes and You: IOT Device Data Risks in an Ever-Changing World

Autumn Person

Columbus State University

SMART HOMES AND YOU: IOT DEVICE DATA RISKS IN AN EVER-CHANGING WORLD

A THESIS SUBMITTED TO THE TSYS SCHOOL OF COMPUTER SCIENCE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

CYBERSECURITY MANAGEMENT

BY

Autumn Person

COLUMBUS, GEORGIA

2023

SMART HOMES AND YOU: IOT DEVICE DATA RISKS IN AN EVER-CHANGING WORLD

By

Autumn Person

Committee Chair:

Dr. Lydia Ray

Committee Members:

Dr. Lixin Wang

Dr. B. Bhagyavati

Columbus State University

December 2023

ABSTRACT

Social media applications are increasingly seen as a national security threat and a cause for concern because they can be used to create user profiles on government personnel and on US citizens. These profiles could be used for big data and artificial intelligence purposes of interest to foreign governments. With the rise of big data and AI being used, foreign governments could use this data for a variety of purposes that can affect normal everyday citizens, not just high value personnel. IoT (Internet of Things) devices that the population uses everyday can also pose the same threat. These devices can collect several types of data and can pose different vulnerabilities depending on the device type and types of data that they collect. In addition to this the data can be used for multiple uses including nefarious ones. IoT devices have been researched in detail, including the types of devices, what they are capable of, the type of data that they may gather and what security measures there might be in place for these devices. Several studies regarding the use of IoT devices have been inspected as well and are included in the literature review. I have also inspected various policies and procedures that are currently in place regarding IoT devices, especially from device manufacturers. Current uses for personal data and its impact on international affairs were also analyzed to connect any potential threats from IoT device data to foreign cyber threats. In addition to this, I have compiled a list of possible safeguards to create a framework for how IoT devices should be treated moving forward.

Keywords

Consumer IoT, Big Data, Artificial Intelligence, National Security, Data Privacy, National Policy, International Security

ACKNOWLEDGEMENTS

To my mother, Tammy, father, Audie, and my brother, AJ for believing in me, pushing me to continue my education, and encouraging me to be the best me that I can be. To God, who through prayer strengthens me every day. As well as various personal and family friends who accompanied me on this journey. You pushed me daily to finish what I started, and now this is the result. I strive to make you proud and hopefully I continue to do just that. Thank you for all your support and encouragement to push me over the finish line.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

Currently, there is an increased usage of devices in people's everyday lives that makes mundane tasks easier. Smart fridges, Home Pods, Amazon Alexas, smart thermostats, and even smart homes themselves with multiple appliances, light fixtures and home functions interconnected within a network. While these devices are useful in many ways, they can introduce serious cybersecurity concerns into the home by widening an attack surface for attackers to potentially exploit. Various vulnerabilities in the design and policies of these devices raise concerns about data privacy, data collection and storage of that data. While cybersecurity experts can see the potential dangers with these devices, can consumers? Manufacturers of these devices and developers of these technologies often cite the tradeoff between security and usability. Better security in a device may sometimes lead to lower convenience for consumers while lower security leads to higher inconvenience. Consumers may prefer to have a device that is easier to use with lower security measures than one that is harder to use with higher security measures i.e., they may not pay as much attention to the security of the device if it is easier to use [3]. As government officials have begun to show concerns about certain applications being present on government devices (i.e., TikTok) and the impact that they may have on national security, there may be similar rising concerns about IoT (Internet of Things) devices [12, 13, 14]. These worries over TikTok have been raised over the possibility that the social media app can be used to track user activities and create user profiles that could harm national security [5]. If those apps can perform those functions, can IoT devices that assist users in everyday tasks be used for the same purpose? This may very well be the case. As the US government has become more interested in IoT device security within the past couple of years there must be reason to believe there is a link between IoT device security and National Security, particularly regarding National Infrastructure

Security. National Infrastructure Security includes systems and processes vital to providing services necessary for governments to function and can include things like energy, roads, sanitation and Internet provision and connectivity. IoT devices are included among the topics of internet connectivity and should be considered when discussing National Infrastructure Security. If IoT devices do perform similar functions to everyday applications like TikTok and Facebook (data collecting and aggregation), they can also be used to create a routine profile for users and this functionality could be considered a serious national security concern specifically regarding Artificial Intelligence and big data. More specifically we will explore the question of how can artificial intelligence and big data gathered from consumer IoT devices be used together to create attacks in cyber warfare? In this paper, we will research the links between IoT devices, data collection, and how foreign entities can use this data in big data sets and AI enhancement to pose national security threats that the US must begin to consider. We will specifically focus on consumer IoT devices within the home excluding wearables (Apple Watches, Fitbits, medical devices, etc.). While wearable technology *can* be researched regarding privacy data collection and cybersecurity concerns, we are not sure if there is currently enough data to explore the link between these devices and national security (outside of location services). Other consumer IoT devices within the home (smart speakers, home security systems, interconnected smart homes, etc.) have more data available and legitimate concerns have been made by governments about how these devices can affect national security regarding cybersecurity concerns about infrastructure.

2. PROBLEM STATEMENT

The main question that will be asked over this paper will be: How can artificial intelligence and big data gathered from consumer IoT devices affect national security infrastructure? And do these two have any effect on national security at all? As an increasing amount of data is being processed and collected every day and can be transmitted across international boundaries, data privacy has been put into government focus [7]. There is a fear that data collected from these consumer IoT devices can be collated into big data sets and used to train AI [6, 8] to become more humanlike. In training AI, it allows foreign governments to learn more about the everyday lives of citizens in adversarial countries and can even use the data to learn the thought patterns/routines of citizens. In turn, the big data sets and AI can be used to create psychological profiles that can be influenced by information warfare (as we have seen with the success of information warfare for Russia). There has been increased evidence to suggest that this fact is why China has become increasingly interested in user data within the past few years. The US must investigate the potential national security risks that these consumer IoT devices could pose regarding the collection and use of data from foreign governments and entities.

3. BACKGROUND

In this section, I will provide context as to why this topic is important and should be considered in a security context. For this paper, IoT devices will be split into three main categories: industrial, enterprise and consumer. Most of the population do not interact regularly with industrial or enterprise IoT in their personal lives and even though these devices also have national security importance and implications, the focus of this paper will specifically be on consumer IoT devices. There is also a myriad of medical devices that are considered a part of the consumer IoT category (heart monitors, blood sugar regulators, etc.) but to gather a broader

range of data and information we will center on devices that can be utilized without medical needs. Consumer IoT is used by people every day and spans a wide variety of devices that can be found in a person's home. Some of the most common IoT devices that consumers experience in everyday life have become so ingrained into society that they are used without much of a second thought. Devices such as smart watches, smart TVs, smart appliances (refrigerators, thermostats, etc.) and smart speakers are just a small sample of what can be done with consumer IoT.

Of consumer IoT devices there has been an upsurge in usage of machines that span three broad classifications: wearable technology, smart speakers, and home security systems. Of these three broad classifications we can extract a top ten of some of the most popular IoT used by consumers. In wearable technology, there are devices such as Apple Watches, Samsung Galaxy Watches, Fitbits, and Garmin Watches. A lot of these machines provide similar services such as tracking movement, counting steps, providing time and date, phone connectivity and features and a list of other functions. Smart Speakers can include tools such as Google Nest, Apple Home Pods, and Amazon Echo/Echo Dot (Alexa line products). These can have functionality that range from playing music to controlling lights and thermostats to even buying products, all using voice commands. Smart Speakers can be particularly interesting in this case because they can connect to and control other devices which leads into the next category: Home Security Systems. Home Security Systems include brands like Ring Cameras, SimpliSafe and Vivint machines. These brands provide services like alarms and cameras that connect to various devices within a home to make it more secure. IoT Home Security Systems can be accessed from mobile phones, tablets, and smart watches and in some instances can even connect to smart speakers to control when doors lock/unlock and when clips from cameras are saved to a user's account. This interconnectivity between IoT devices is what makes them so appealing to use but is also an area

of concern. Though wearables are listed here for reference, we will be focusing on IoT devices within the home such as Smart Speakers and Home Security System. However, they are mentioned because a lot of wearable devices also interact and interconnect with home IoT devices so they may share some vulnerabilities, but they will not be examined alone.

3.1 Privacy Policies of IoT Devices

In this subsection, manufacturer's privacy policies are investigated in depth. As these machines are in use, they collect and store a good amount of personal data on users. Analyzing the privacy policies of devices reveals that location data, health data, financial information, voice data, facial recognition data, environmental data, browser data (search history, order history, websites visited, etc.) and a variety of other data is collected by this equipment [17]. The companies behind these machines also retain and store the data for various uses from creating user profiles and adding suggestions as some policies say that data collected from devices may be used to provide personalized experiences for customers (to make inferences and suggestions) or retention for legal and compliance purposes [17]. The privacy policies state that the data can be stored for a certain amount of time (though this is not specified) and may be used for other purposes outside of the basic functioning of the device. Almost always these privacy policies are hidden away by another webpage, are at the bottom of the manufacturer's website and are full of technical and legal jargon. They are often only available to fulfill legal requirements for companies than to inform consumers of possible data collection and usage. This is compounded by the fact that most of these policies state that the manufacturer may use the information collected to comply with legal requirements and standards. Many of the privacy policies listed for common IoT devices list that data is collected to promote safety and security (to protect against fraud and abuse) but this statement is left vague and is not explained in detail as to *how*

the data is used for security purposes. As stated in these privacy policies, data from these devices is also collected from third parties which means that data is collected from outside sources as to what websites may be visited on the device, if there were any products searched for or ordered with the device and location data detailing where a device is being used. This may also go the other way with tracking data habits and information being given to other third parties for advertising purposes.

While most privacy policies can have broad similarities some manufacturers may choose to add specific wording about how data is collected, handled, and stored for their use. Samsung specifically states that information stored on the device, such as face clustering data or biometric data, is not accessible to them [17]. This is interesting because it shows how companies are aware that this consumer information is valuable and how important it is to assure customers that their data on the device is secure. Amazon states that they collect voice recordings of conversations that customers have with their Alexa devices. They state that these recordings can be reviewed and deleted by consumers or that voice recording can be turned off and recordings never saved; however, they state that doing this might result in a lowered user experience and that certain features such as voice ID may not work [17] which will incentivize consumers to allow this data collection method to happen for ease of use. This voice data can be important in the creation of AI software that can mimic human voices or in the use of deepfakes used to create an AI duplicate of a real human being. Apple uses a worldwide approach as opposed to tailoring data handling procedures to specific countries or territories [17]. They specifically mention this because it creates uniformity among their different departments regarding privacy data. This can be vital in determining how to store, utilize and transport data across national boundaries. If there is uniform rule, then there are not rules in one country that would allow access to certain types of

data while another country prohibits it thus closing any loopholes that may create discrepancies to allow for access to data. These are just some interesting points between different companies' privacy policies and what they choose to focus on can say a lot about why data in these devices must be protected. Highlighting some of the similarities and differences is important to show also how vague and convoluted these terms can be and that they sometimes exist not for the benefit of users but for manufacturers. Nonetheless, privacy policies stating uses for this data along with storage terms proves that the data within IoT devices is valuable and can have many different uses outside of what many may typically think of.

Though consumer IoT has a variety of benefits and can make tasks seem easier and more efficient in the eyes of consumers, they are not without risks. As with any Internet connected device there are vulnerabilities present in these machines that carry dangerous risks. Vulnerabilities such as unsecure patch management, insecure network usage, easily guessable passwords, and potential use of outdated components/legacy software [15] are all some general vulnerabilities present in IoT devices that would also be present in “regular” devices. Even further, there are some vulnerabilities that are unique to consumer IoT devices. Continuously recording voice/health data, continuously recording video, monitoring of location data, cloud uploads, and interconnectedness with other devices on a network. Along with this, portability, and the need to be low powered can introduce more complications like not using proper encryption (because of higher power consumption) [16] and the potential spreading of viruses/malware. Listed in the chart below is a list of IoT vulnerabilities and whether these vulnerabilities are policy, coding, privacy, or process/design related.

Table 1: List of IoT Device Vulnerabilities Categorized

IoT devices topics	**Vulnerabilities**	**Coding-related**	**Process/design related**	**Policy related**	**Privacy related**
Smart Watches	Continuously recording health data	No	Yes	Yes	Yes
Smart Watches	Location data	No	Yes	Yes	Yes
Smart Watches	Voice data	No	Yes	Yes	Yes
Smart Watches	Portability	No	Yes	Yes	No
Home Security Systems	Continuously recording video	No	Yes	Yes	Yes
Home Security Systems	Cloud uploads for video clips	Yes	Yes	Yes	No
Home Security Systems	Attacker can control locks and alarms	Yes	Yes	Yes	Yes
Smart Speakers	Voice recognition features (voice data)	No	Yes	Yes	Yes
Smart Speakers	Voice commands	Yes	Yes	Yes	No
Smart Speakers	Integration with other smart devices/home network	Yes	Yes	Yes	No
Smart Speakers	Continuously recording user conversation	No	Yes	Yes	Yes

All 3 IoT Types	Storage of financial data	Yes	Yes	Yes	Yes
All 3 IoT Types	User passwords being easily guessed	Yes	No	No	Yes
All 3 IoT Types	Insecure networks being used	Yes	No	No	Yes
All 3 IoT Types	Unsecure patch management	Yes	No	Yes	No
All 3 IoT Types	Outdated components or use of legacy software that is no longer supported	Yes	No	No	No
All 3 IoT Types	Always on Functionality	Yes	Yes	Yes	No

These vulnerabilities can be taken advantage of by many threat actors ranging from people hacking for fun to hacktivists, organized crime units and terrorists and lastly, other foreign governments. There have been numerous studies suggesting that China's interest in foreign user data has increased dramatically in recent years. These studies also seem to suggest that there is a clear and present reason as to why user data would be of interest to foreign governments- big data and artificial intelligence [4, 6, 9]. Data collected from IoT devices can be collated into vast storages of data that can be stored away for future use, sold or in this case, used for differing purposes. Artificial Intelligence (AI) has gained more traction in our everyday society within the past few years and is evolving rapidly. From various software such as ChatGPT to botnets and

even AI that can generate lifelike art and pictures, these programs have seen increased usage. It is common for a social media user to scroll down their Instagram, Facebook, or X (formerly known as Twitter) feeds and encounter some form of AI generated text, art, or message. AI has been utilized to write messages, papers, create art, visual assets, and more. For AI to perform these things they must be trained. Many AI programs are created with the end goal being to make them seem more humanlike; so much so that the text and pictures they create or actions that they perform would be indistinguishable from actual human behavior. Training AI can take different forms ranging from algorithms and mathematical equations to using models of actual human behavior to be replicated by programs. Large swaths of data can come from many sources; social media, website traffic data, emails, but especially devices that the populace use every day that are so integrated into our lives. As they can be such large sources of human data and store personal information of millions of people, these IoT devices that we have within our homes should be guarded for safekeeping to protect the data within (as with all devices and systems). Personal data privacy has become increasingly a topic of debate regarding data that is gathered across websites and particularly social media but what about data gathered by IoT devices within the home? We will look more in depth into the topic and see if personal data collected on users by IoT devices in a household can be a cause for concern when discussing national security here in the United States.

4. LITERATURE REVIEW

In this section, we have searched for existing literature on the topic of consumer IoT devices and national security concerns to see if there has been any extensive research on the topic at hand; however, it seems there has not been much research done on the topic of home consumer IoT devices specifically. We will need to combine different subject matter from diverse literature to

form our argument as to why this topic is important and should be studied more and we will use this to propose our own viable solutions. Many of these papers have focuses that are outside of the US, but the same ideas and concepts can be applied here. Using various sources, we will evaluate the security of consumer IoT devices, what threats the data that they collect can pose on national security and propose potential solutions to help mitigate possible threats from IoT devices.

As National Security and Cybersecurity have become more intertwined, many topics such as data privacy, personal data privacy and device security have come to the forefront. Cybersecurity has been steadily becoming more of a focal point within the national infrastructure of various countries. Ranging from topics such as energy grids/systems to manufacturing and logistics, cybersecurity is considered vital to ensuring the systems that oversee daily operations integral to government functionality are protected and the data within them is secure. While cybersecurity within the sphere of protecting government systems is more well known, there is less research done about IoT device security and how their security can impact national security infrastructure here in the United States. However, nation-states are becoming more interested in these topics and with good reason. In the article named Privacy Concerns in the Smart Home Context, Guhr et al. outline some of the existing concerns about IoT device security regarding smart home devices. Although smart home devices enable user activity tracking and recording like never before, there seems to be a distinct lack of privacy concerns regarding these devices in opposition to social media [2]. This lack of privacy concerns could come from the fact that smart home IoT devices can have higher usability and can make everyday tasks easier for users so not much attention is paid to the gap in data privacy concerns with home IoT devices. Higher usability and easier convenience for consumers can sometimes lead to lower security within

devices. There is also the fact that consumers may not care as much about IoT device security as some may think [3]. While consumers do expect devices to be secure when they buy and use them, not much care is given to what happens to data after it is collected and how it is stored [3]. Some concerns exist for IoT smart home devices regarding hackers and the like but not much attention is paid in general to data privacy [3]. With these two points in mind, there is no wonder as to why there is a gap in the literature and national focus on IoT device security within the home.

Even though these devices form infrastructure that should be protected and can gather and store a sizable amount of data about citizens, they have not been given much of the focus that they should be. Recently, we have seen how this has been changing over the past few years. In 2021, the Biden Administration published an Executive Order highlighting recent concerns with IoT device cybersecurity and explaining how it is considered a vital piece to the future of US national security [14]. It outlines some major recommendations that must be made to improve IoT device security for national security purposes. The Executive Order Does not go into as much detail as a research paper or article would, however, it does show that there is a growing interest in the security of IoT devices to protect American consumers and that consumer IoT device security may have an international outlook. CISA (Cybersecurity and Infrastructure Security Agency) has also released various official documents displaying the various concerns about IoT devices, their security and how they could be used to affect infrastructure security in the US. In the official document titled *The Internet of Things: Impact on Public Safety Communications,* the benefits to IoT devices, concerns about IoT devices (lack of policy, extended attack surfaces, lack of standards, etc.) and how they can impact the infrastructure here in the US are discussed [13]. These concerns can impact citizens in diverse ways that must be considered by governments in

ways that they have not been until now. This paper however does not give context into how different user data may be used by adversaries in opposition to US national security. Another official US document summarizes the findings from a virtual workshop that focused on cybersecurity risks in consumer IoT devices. The report, titled *Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices* [12], is an official NIST (National Institute of Standards and Technology) document that outlines some of the cybersecurity concerns in IoT devices that are used in the consumer homes space. It details why these vulnerabilities are important and why they should be mitigated. The purpose of this paper is to promote "US economic and public welfare" (i.e., looking out for the interests of consumers with IoT devices in their homes). Also, the intended audience for this paper is "manufacturers, consumer organizations and other stakeholders within the consumer IoT device market." [12] highlighting how this concern not only provides manufacture guidelines but also affects consumers as well. Publishing documents on a federal government level highlights how the cybersecurity of IoT devices in the home can have an impact on a national level and shows how if the security of these devices were to be compromised on a meaningful scale, there could be significant national security concerns.

IoT devices can have significant impact on national security especially in the realms of infrastructure and defense [8] and while many different IoT devices can be included in that, consumer IoT is worthy of deeper analysis. Different literature on the topic of how consumer IoT devices can affect national security (especially regarding infrastructure) contend that data from these devices can be of especial importance to foreign governments and adversaries. An example of the Equifax data breach and the cyberattack on the Office of Personnel Management (OPM) demonstrates how foreign governments may benefit from accessing personal data/information of citizens as there is reason to believe that access to this personal information of citizens can be

useful for counterintelligence operations of other foreign nations [4]. There is also the recurring topic of Artificial Intelligence and "big data" when discussing what foreign adversaries may want with consumer IoT device data [4,6,8]. There are many articles that reference these two issues when mentioning why foreign governments may want to access smart devices that may be present in the home to gain access to profile data stored on those devices. Others say that data transfers can and should be regulated on an international scale, outlines why they must be regulated and provides reasoning for why data on citizenry must be regulated on international terms while others believe better regulation will not solve the issue and allow for more government overhead regarding citizens' personal data [7]. These factors will be useful to remember when discussing consumer IoT device data and how it concerns national security. The articles listed here do not directly reference or explain why home consumer IoT devices may have a direct effect on cybersecurity infrastructure and why the data within them must be protected.

5. METHODS OF AUTHORIZED AND UNAUTHORIZED ACCESS TO IOT DATA

There are multiple ways that attackers can access IoT data of private citizens through differing means. In this section, I offer some ways that attackers or other users may gain access to devices (and their data) through various means: authorized or unauthorized.

With these devices designed to be portable and small enough that they can be snuck into secure locations they can be used with relative ease, however this can introduce other problems. The small and portable nature of these devices means that they can be used to move viruses or other malware easily from network to network. As with other internet connected devices, weak encryption and unsecure communications are an area of concern for IoT devices as well. If weak encryption methods are used for these devices and there is unsecure communication between the

devices and a network, this could lead to data being compromised and locations being guessed as well as passwords that allow for authorized access to these devices. The usage of voice commands on these devices allows for ease of use for consumers and permits anyone to use one. This can introduce unwanted use of a device without proper authentication for those who might be using the device for a specific purpose. A benign example being that anyone can use voice features to order items with a stored credit card linked to the account. If this were to be used for something more sinister (like using voice commands to change authorizations or get restricted access to a device), the consequences could be disastrous. Along with these methods listed before, some privacy policies of these IoT devices state that the device must be connected to a network to work or perform any basic functions. On one hand, this can be good for authorization of users, devices, and servers, and some may ask the question: why any consumers would want to use a device that would not work without internet functionality. On the other hand, this can allow for the IoT device to be used be used as a "backdoor" into a larger network or other connected devices. As most IoT devices within a home are designed to be interconnected with other devices, this means that an attacker can use one device to connect to others that may control other functions such as using a smart speaker to control air conditioning temperatures or allow for remote access to control locks and alarms. This interconnectedness of devices is very convenient for consumers and users but means that if one device is compromised, others can be as well with minimal effort. Lastly, the always on functionality design of these devices means that they are always powered on and collecting data. This can lead to connections at almost any time and give time for an attack to be covertly established such as using the device to funnel data out of a network without raising alarm. As the device is always on and always connected, there would be no alarm raised if internet connectivity happened at odd hours.

Aside from attackers trying to gain unauthorized access to IoT devices for malicious purposes, there are also users who can access IoT data through authorized means and then can use the data for malicious purposes. These devices' privacy policies often cite the need to save and store various amounts of data for a given period. Whether that be location data, voice data, financial data, or video clips from cameras they are collected and stored for a certain amount of time in the cloud [17]. This means a lot of data is stored somewhere on a server that someone could access if they have the right credentials to do so. Some IoT device manufacturers state in their privacy policies that they reserve the right to keep data collected from these devices for a certain amount of time and what they do with it is almost never mentioned. Another way that this IoT data can be obtained through authorized means is by receiving the data from device manufacturers. Along with the right to store and use data mentioned earlier, device privacy policies also mention that users' data may be given to third parties willingly [17]. Most consumers think this means that data is given away to help with targeted advertising but there are no specifics mentioned as to who or what these "third parties" are. If a "third party" is posing as an ad company and obtaining IoT device data through legitimate means, that data can then be used for malicious purposes if necessary. It can then be sold to other entities or even used by those malicious "third parties" themselves to access personal information of users. Whether the data is being accessed by authorized means by using legitimate passwords or obtaining data from third party brokers or by unauthorized means from using sneaky cyber-attacks and interacting with IoT devices directly, the data is still being accessed. Privacy data is becoming more valuable as the world moves towards an all-digital future and different threat actors want access to users' personal data. With most consumer IoT devices working within the home, this makes them more appealing as they are more likely to have access to users' personal spaces and record what they do on a device in

the comfort of their own home. This closeness means that the data they gather can have a significant impact if found in the hands of others and there can be power in obtaining that personal data and information that is invaluable to some.

6. THE THREATS OF IOT

Data from IoT devices within our homes may seem like something that is of little significance in the grand scheme of things but as these devices form an integral part of the nation's everyday infrastructure, they have been singled out as important cyber devices that must be protected. IoT device data can be used in many different scenarios, for different purposes and can have different outcomes. In this section, we will look at uses for IoT device data from common IoT devices found in the home. We will discuss the impact that breaches of these devices could have if used by opposing forces and suggest some safeguards as to how to protect these devices and therefore national security infrastructure. Listed below are some potential adversaries that might find data collected from consumer IoT devices of interest, what they might use the data for and what the possible benefits may be to gaining access to and gathering the data.

Table 2: Potential Adversaries for IoT Device Data and Data Usefulness

Adversary	**Usage of Data**	**Purpose/motivation of adversary**
Nation-states	Espionage Spying Ransom AI Destabilizing techniques	Propaganda, PsyOps, Power
Terrorist Organizations	Ransom Spying Narrative setting Recruitment (targeting specific people)	Money, Propaganda, Power
Activists (Hacktivists)	Ransom Defamatory purposes Expose wrongdoing	Propaganda, Reputation Setting

Organized Crime Units	Ransom Sell for profit to other governments/actors	Money, Blackmail, Power
Non-Affiliated Hackers	AI Data collection Just want to find vulnerabilities Want to see if they could gain access to the data	Fun, Skill testing, Research

Potential adversaries look to gain access to large swaths of data generated by users on IoT devices that they use every day. From other foreign governments to terrorist organizations, organized crime units and unaffiliated hackers, there will be a lot of separate groups on the hunt. Motivation for wanting to gain access to this information may differ as well.

6.1 Nation-States

There are other foreign governments who may want to gain access to this data for espionage and spying. They may also want to use the data to help with destabilizing techniques or more importantly and more recently, for AI usage. The IoT data can be used to create profiles of users and be used to target people with propaganda who match a certain user profile. The devices can be used to set the narrative regarding certain current events (public opinion about wars, elections, etc.) by utilizing bots or ads clogging up information/news feeds with false or misleading information. Finally, data from devices can be used to train AI using big data sets. This is one of the more pertinent reasons as to why foreign governments may now want access to IoT data. As stated before, training AI to be more human like can sometimes take vast amounts of data that must be collected from somewhere. Learning patterns and behavior can be achieved by recording human interactions and running them through software to train said software. In turn, this AI can be used to launch sophisticated attacks on other critical systems. Voice data could also be used to

create AI and deep fakes based on real people which can be used to create propaganda and other content that could be detrimental if the wrong person were to be targeted. The worry is that this AI could be used for botnets and psychological operations (PSYOPS) attacks that would harm US national security. Botnets can be used to overwhelm systems to the point that they are unusable, which in the context of government systems such as energy systems or government internet, can be vital. Psychological Operations attacks are intended to influence or motivate a group of people to take a certain action and can be a bit more nuanced. An example of this type of attack would be misinformation campaigns as was the case with suspected Russian interference into the US's elections.

6.2 Terrorist Organizations

For terrorist organizations they may want to get IoT data to hold for ransom, to spy on certain citizens or to target specific people whose target demographic may match who they want to recruit. Gathering data on users who may share the same mindset and like the same content that a group does would be beneficial in targeting certain audiences that are susceptible to recruiting. Using IoT devices to push certain advertisements that promote ideologies or to push content that can change the mindset of users would be advantageous to organizations looking to influence political outcomes or reach political goals. Terrorist Organizations can also utilize the data for monetary purposes such as holding personal data (pictures, website traffic, etc.) for ransom. Lastly, this data could be used for narrative setting. These organizations can use ads in a comparable way as stated before but instead of using them for recruitment, they use them to spread a narrative about political events that may benefit them.

6.3 Activists

Activists may want to gain access to data to use in propaganda, to hold for ransom, to expose wrongdoing, or for defamatory purposes. If IoT devices are used to create unique profiles for individual users, then accessing the data stored within them may prove useful for activists wanting to share propaganda or ads that can help spread awareness for a certain issue or event. They can also use data to aid in setting a reputation for their group (make the group seem more appealing to the public to push their goals). Another usage for activists wanting to gain access to IoT device data is to expose some form of wrongdoing on behalf of a cause or to use that data for defamatory purposes.

6.4 Organized Crime Units

Some of the reasons listed above are the same for organized crime units but they may differ in the fact that while Terrorist Organizations have a vested political goal that they are working towards, Organized Crime Units do not. Organized Crime Units are simply in it for monetary gain or for material that they can use to exert power over others. They may want to access the data to sell for profit to other actors. Data brokers, companies, or other governments are possible customers that could cooperate with these groups to obtain data without having to put in the work to hack into the devices themselves. Organized Crime Units can also be used as decoys by other actors to make it seem as if they are not accessing or obtaining IoT data, but they are using the organized crime units as an intermediary to get what they want without looking like the bad guy.

6.5 Non-Affiliated Hackers

Non-Affiliated Hackers may also want to gain access to IoT device data, though these purposes can either be malicious, neutral, or beneficial. Non-affiliated hackers can be hackers trying to acquire the data through authorized or unauthorized means. Their motives may overlap with some groups listed earlier or they may have unique cases that do not fit any of the other groups. For example, a person or a group of people in this category may try to gain access to IoT device data for research purposes or to collect valuable data that can be used in statistical analysis. They may also be trying to hack into these devices to test their skill or to find vulnerabilities within the devices as part of a bounty program. These hackers' motivations can also be monetary gain (again to hold information for ransom or to sell).

The adversaries listed above have a personal stake in accessing IoT device data. Whether it be for money, power, influence, reputation, or research, each group has its own motivations and reason for wanting to obtain IoT device data. An area of increasing concern is the data's potential in usage of AI mentioned in the Nations-States subsection or usage of the data for botnets and coordinated cyber-attacks. Whatever these groups may want it for, IoT data has proven to be a digital commodity that can no longer be ignored. Safeguards and protections must be considered to protect the data within the devices used in millions of homes every day.

7. SUGGESTED SAFEGUARDS

To protect against these threats, we propose that multiple avenues should be looked at and combined to create a comprehensive defense against IoT data threats. In this section, I offer some safeguards and suggested protections that would aid in making IoT devices more secure with users' data. More accessible privacy policies (user awareness), international data

regulations, a more open approach to hacking of IoT devices and improving the use of techniques that are already in place are some suggestions that we believe would lead to a safer digital environment for IoT device data. Better accessibility and ease of use regarding privacy policies [1] should be considered as many consumers are not attentive to or know how, why, where or for what purpose their data is being used for. Long documents listing the privacy policies of IoT devices are available, but they are written in technical jargon that many may not understand. Making these documents easier to understand and easier to find is beneficial to users by allowing them to have more control over their data and would lead to a better understanding of how, why, and what data is collected.

Regulating data trades on an international scale [7] as mentioned before would mean that user data would be more secure. Having laws and regulations that mandate where data is stored, how it should be stored and how it should be used would lead to better protection for the data as opposed to if the data were unregulated. Implementing these rules would also allow for more repercussions if the data were to be used unlawfully or against an international agreement (such as a treaty restricting AI usage and so on). In addition to this, having a common international framework for the transportation, storage, and usage of data across different countries would be beneficial in data privacy and protection. A mismatch in laws allows for certain loopholes that benefit attackers and malicious organizations that could be fixed if there are uniform regulations in place. Allowing for more openness regarding researcher's ability to hack into IoT devices to discover vulnerabilities [9] would allow for faster response regarding remediation of potential vulnerabilities.

With more openness about the ability to hack, more research can be done concerning how these IoT devices can be accessed and what data can be collected from them on a larger scale. Also, as

most data from these devices can be stored remotely, it would have an impact on researching and learning about remote data access and remote data extraction. And lastly, making use of and improving upon different techniques already in place (data anonymization) [11] would allow for a flawed system that is already in use to be upgraded to allow for better ways to obscure personal data from being traced back to a certain device or person. IoT devices currently can anonymize data which could be useful, but it is flawed, and that data can be deanonymized through the right techniques [11]. This would allow for less personal tracking and block the potential of user profiles being created for consumers that could then be used for targeted campaigns. Combined these factors can be used to construct a framework that will create a plan of action to protect IoT device data. The figure below illustrates how these four components are important and can be implemented in the future.

Mandate International

for setting standards and making sure they are followed

Initiate a bug bounty program to

Figure 1: IoT Device Data Protection Components and Possible Implementations

The four components we have listed above (along with some ideas about how to implement them) can all be integral elements that will contribute to the defense of IoT data.

Increasing consumer awareness through privacy policies can create a populace that can be aware of how their data is being used, collected, and stored and would be beneficial to them knowing the potential risks associated with IoT devices. They may then start to interact with devices

differently and may contribute to making sure their data is more secure. For example, if a consumer knew that their data would be used to create AI profiles specifically for them (that look and act how they would act) they may then start to become wary of what information is stored within these devices thus lowering the chance that another person may access this data (they cannot access what is not stored on the device).

International regulations and standards that are enforced by a common ruling body would be helpful in making sure that IoT device data is uniformly regulated and that there are less legal loopholes that can be exploited to gain access to personal IoT data (similar to the reason why Apple has a global privacy policy instead of tailoring it to different countries). Allowing for more extensive research on IoT devices outside of what manufacturers do can open these devices to be scrutinized by external actors. Sometimes companies may miss vulnerabilities or leave unintentional exploits from development in devices' code or design.

Calling upon external actors to try to hack into these machines through a bug bounty program can pay dividends. This would also allow for more extensive research regarding how these machines work and how they can evolve in the future. Lastly, improving on techniques already in use can allow for better research to develop newer techniques and can incentivize and reward innovation in tandem with research. These can all be factors that can help regulate how IoT device data is accessed and used, thus making the devices more secure. Together, these elements will help create a comprehensive environment that can protect IoT user device data collected from smart home devices and can be useful when defending against national security attacks using the data collected from those devices.

8. CONCLUSION

Home consumer IoT devices have allowed for unprecedented access to personal data collection and storage. As these devices are within the home, they allow for personal tracking on a scale that has never been seen before. Financial data, location data, and more can be stored in these devices making them an attractive target for intrusion. In addition to that home IoT devices can control security, electricity, appliances, and other home features through the interconnectedness of IoT devices. Therefore, these devices should be considered a vital part of the modern infrastructure and should be looked at regarding cybersecurity infrastructure within the US. Adversaries might seek to gain access to personal data on these devices for a variety of reasons: ransoms, blackmail, spying/espionage, etc. But a large reason a foreign nation state may want to gain access to this data has become clearer and clearer: AI. AI can be used to form different attacks against another nation and can be an especially useful tool. In this paper, it was shown why differing groups may show interest in home IoT data and why others gaining access to said data can be harmful to consumers and the populace. In home IoT devices should be treated as a part of the US national security regarding infrastructure and should be offered protections as such. It increasingly seems as if others are seeing the impact that this data could have, good or bad, and it looks as if the US government has started to pay attention to the issue on a national scale within the past few years. While some may think the time to pay attention to this topic may have passed, many think that this is just the beginning.

9. REFERENCES

[1] Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., & Cranor, L. F. (2021). Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices? *2021 IEEE Symposium on Security and Privacy (SP), Security and Privacy (SP), 2021 IEEE Symposium on, SP*, 519–536. https://doi.org/10.1109/SP40001.2021.00112

[2] Guhr, Nadine, et al. "Privacy concerns in the smart home context." (2020) *SN Applied Sciences*, vol. 2, no. 2, https://doi.org/10.1007/s42452-020-2025-8.

[3] Lili Nemec Zlatolas, Nataša Feher, & Marko Hölbl. (2022). Security Perception of IoT Devices in Smart Homes. *Journal of Cybersecurity and Privacy*, *2*(1), 65–73. https://doi.org/10.3390/jcp2010005

[4] Doss, A. F. (2021). Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That Are Inextricably Linked. *Duquesne Law Review*, 59(2), 231–268.

[5] Clausius, M. (2022). The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes. *Washington University Global Studies Law Review*, 21(2), 273–292.

[6] Lasso Cardona, L. A. (2021). Technological trends: a focus on citizen security. *Ingeniería Solidaria,* 17(1), 1–28.

[7] Marengo, F. (2020). Regulating Data Transfers through the International Trade Regime. *Manchester Journal of International Economic Law*, 17(2), 266–297.

[8] Pătrașcu, P. (2021). EMERGING TECHNOLOGIES AND NATIONAL SECURITY: THE IMPACT OF IoT IN CRITICAL INFRASTRUCTURES PROTECTION AND DEFENCE SECTOR. *Revista Academiei Fortelor Terestre*, *26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

[9] KILOVATY, I. (2019). Freedom to Hack. *Ohio State Law Journal*, *80*(3), 455–520.

[10] Zubiaga, A., Procter, R., & Maple, C. (2018). A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things. *PLoS ONE*, *13*(12), 1–18. https://doi.org/10.1371/journal.pone.0209472

[11] Park, S., Kim, R., Yoon, H., & Lee, K. (2021). Data Privacy in Wearable IoT Devices: Anonymization and Deanonymization. *Security & Communication Networks*, 1–9. https://doi.org/10.1155/2021/4973404

[12] Megas, K. N., Fagan, M., Cuthill, B., Raguso, M., Wiltberger, J. Workshop Summary Report for "*Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices*" Virtual Workshop. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8333.pdf

[13] CISA *The Internet of Things: Impact on Public Safety Communications*. https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper_3.6.19%20-%20FINAL.pdf

[14] *Executive Order on Improving the Nation's Cybersecurity*. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[15] Hameed, A., & Alomary, A. (2019). Security Issues in IoT: A Survey. *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2019 International Conference On*, 1–5. https://doi.org/10.1109/3ICT.2019.8910320

[16] Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). An overview: Security issue in IOT Network. *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference On*. https://doi.org/10.1109/i-smac.2018.8653728

[17] *Various Privacy Policies for IoT devices*.

Samsung: https://www.samsung.com/us/account/privacy-policy/

Apple: https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf

Amazon Alexa: https://www.amazon.com/gp/help/customer/display.htmlnodeId=GVP69FUJ48X9DK8V

Google Nest: https://nest.com/legal/privacy-statement-for-nest-products-and-services/

Ring: https://ring.com/privacy-notice

SimpliSafe: https://simplisafe.com/privacy-policy

Vivint: https://www.vivint.com/legal/privacy-notice