Security and Privacy Issues with Smart Thermostats – A First Look

The five basic human senses – sight, hearing, taste, smell, and touch have all been reproduced to a certain capacity using technology. Technological devices that reproduce the senses are commonly referred to as sensors. IoT is a concept defined by the interaction of one or more sensing device with the internet. There has been a massive adoption rate of IoT devices since its applicability in our daily lives are endless, however like most technological advancements security and privacy are afterthoughts for device manufacturers. IoT manufacturers in a move to lure more users focus on a seamless user experience of the devices, which comes at a detriment of security. The consumers of the IoT devices also favor convenience above security and privacy.

Four key security and privacy guidelines were analyzed. The paper will align the core focus of smart IoT devices using the People, Technology, and Information model. We use Brenda Dervin sense making model to explain human behavior and way of reasoning with making purchasing decisions of smart thermostats. Recommendations will be provided to highlight the importance of security and privacy by using OWASP (OWASP, 2017).

Introduction

The term “Internet of Things” was first used by Kevin Ashton in a presentation in 1999 (Gubbi, Buyya, Marusic & Palaniswami, 2013). At that time, the term was used in the context of the supply chain. It is not surprising how the term has metamorphized into something larger and with the potential to be one of the biggest technological disruptors over the next decade. One way of explaining the IoT phenomenon is by tracing its emergence to the enabler, which is the Internet. The Internet created a world of interconnectivity between computers across networks with no boundaries. The Internet serves as a backbone for extending the capabilities of both old and modern technologies. Sensors and other forms of monitors have been around for decades. A motion detector is an example of a sensor and it can be used as a security device when wired to an alarm system or an energy conservation device when connected to electric bulbs. (Atzori, Iera & Morabito, 2010) believes sensors like the motion detector devices, Radio Frequency Identification Devices (RFID) are “things”. RFID is another technology which has been around for many years. One of RFID’s main uniqueness is in the fact that they only require a low voltage and also, they are relatively inexpensive.

One of the modern-day issues faced by information security professionals is with the emergence IoT and its increasingly wide adoption rate. Today, there are a lot of mobile devices and stationary home and enterprise devices that are interconnected. Devices like our wireless thermostat, wireless garage door opener, remote-start applications for our cars that live on our smartphones, wireless microwave, IP cameras, wireless refrigerator, wireless door locks, etc. In an IoT infrastructure, these devices are connected to the internet in one form or the other. In many cases, they have an always-on connection to the internet. Their connection to the internet could be through a home or office wireless or wired connection, which implies that they all in most cases live on the same network. Driving the conversation further, IoT devices need to communicate with their host server through a medium, for example, a network port. Some IoT devices require an IP address since they need to be part of the network before they can be controlled by a remote device such as a smartphone. Getting IoT devices to coexist seamlessly may involve leaving a few security loopholes. A potential attacker could listen to the network connection stream through a tool like
Wireshark and sniff passwords, commands sent by one of the IoT devices. The vulnerability on one of the IoT devices can potentially lead to the compromise of the other connected devices which could lead to potential loss of life or property. This is a serious problem that requires extensive and continuous research.

Literature Review

IoT research publications in the areas of smart thermostats is still in its infancy. Accessing validated data within the smart thermostat field is expensive. There is a clear need for research in this area because of the growth and adoption rate of smart thermostats in both the consumer and enterprise market. A study by RnR market research stated that the adoption of smart thermostats is at a Compound Annual Growth Rate (CAGR) of 31.82% between 2015 to year 2020. (Research, 2015). The attraction to smart thermostats especially in the European markets has been attributed to the energy cost saving benefits that smart thermostats offer. The ease of use and installation is another reason why smart thermostats have gained popularity in Europe and in North America (Haney, Jamsab, Pollitt, 2009). Haney, Jamsab, and Pollitt analyzed the various energy sources and how smart thermostats have been able to mesh a usage pattern for the devices, which makes a good case for building intelligence into smart devices.

IoT has drawn a lot of interests in the scholarly community for its technological features, usage potential, applicability to our daily lives, and most importantly, its security and privacy risks. Pticek, Podobnik, & Jezic, (2016) explains that the IoT and other technologies that intersect with it like the Wireless sensor networks, cyber-physical systems are all part of the Machine-to-Machine (M2M) communications. The authors describe the M2M paradigm as the communication between machines. The idea is to allow devices exchange information bidirectionally over a communication network. For a communication path to be referred to as M2M, the communication can only be between two or more devices and not a device talking to an application highlights the opportunities for automation within the smart home space. Dahmen et al. (2017) took a scenario based approach to analyze smart home technologies with a focus on home and resident security. The authors stated that a smart home technology must be able to take the steps, sense, assess, and act to be able to function in the security scenarios covered. The scenarios covered include: intruder detection, health event detection, building system failure detection. The three scenarios highlighted bases the premise on the fact that smart home technology is a combination of multiple sensory and interconnected devices, that share information as in the M2M format as illustrated by (Pticek, Podobnik, & Jezic, 2016). The possibility of system anomalies with the IoT devices posing a bigger threat of false alarm, and the fact that smart devices not having a standardized setup platform increases the risk of hacking was highlighted.

Pticek, Podobnik, & Jezic, (2016) put forward the concept of machine communication, with examples as Facebook machine and Twitter machine. M2M is defined as a “communication that takes place between machines with minimal or no human intervention.” (Pticek, Podobnik, & Jezic, 2016, p. 2); smart machine refers to “an electronic device that connects to other devices and networks via wireless” (Pticek, Podobnik, & Jezic, 2016, p. 3). A definition for IoT was stated as a term used to describe “technologies, systems, and design principles associated with the emerging wave of Internet connected things that are based on the physical environment”. The paper used models to analyze and propose a model that marries M2M, IoT and other modern technological communication platforms framework and expressed that the Machine social network built on web 2.0 is the future. This means that the network of devices can create social connections and offer services. The authors believe that advancement in technology will only mean that social IoT (SIoT) becomes the trend.

Hossain, Fotouhi, & Hasan (2015) defined IoT at a conceptual level as the “interconnectivity among our everyday devices, along with device autonomy, sensing capability, and contextual awareness”. The authors showed a prototype of an interconnected smart home, which consisted of interlinked devices like ovens, refrigerators, door lock, thermostat, smoke detectors, etc. The paper presented a scenario where a vulnerability from one of the devices in the smart home circle can be exploited to breach the security of the other interconnected device. As highlighted in the paper, they mainly proposed the three-dimensional framework to indicate the intricacy of IoT security domain, which can serve a good framework for considering security issues in the context of IoT.

Hossain, Fotouhi, & Hasan (2015) emphasized the need to focus on securing IoT devices as previous research and studies has shown the relative ease at which a security attack can be carried – out. Impersonation of a compromised device was stated as a common security attack carried – out by the device. The authors proposed that the IoT
ecosystem with which the smart thermostats are inclusive consists of five major components, which are: IoT devices, Coordinator, sensor bridge, IoT services, and controller. The authors put forward a list of IoT device security constraints, requirements, and recommendations. (Nurse, Atamli, & Martin 2016) identified smart homes as homes with deployed. The authors outlined a framework that can help with modeling the security and privacy risks with IoT deployments. The key goal of the framework design is to allow users model risks, the second goal is to promote risk awareness with IoT devices across board. The authors defined smart cities as a concept that is closely aligned with government and cities while smart home is to domains where the consumers have more choice and flexibility. The model proposed by the authors is a linearized feedback model that consist of: Use case definitions, Assets and network analysis, Threat and attack analysis, Risk definition and prioritization, and control definition and alignment. Executing the framework constructs involves asking a series of questions and collecting data from the end user and the device in question to start modeling what the possible privacy and security risks can be. The framework was tested by conducting informal interviews with a small subset of users with smart home technology. The framework is a work in progress and would continue to evolve through usage and end user feedback.

The paper, “Framework for communicating with consumers using an expectation interface in smart thermostats”, identified that the design of smart thermostats lacks the user expectation consideration, hence user satisfaction and usage pattern is not being included during the design phase, as a result less of customers’ requirements are captured. (Ponce, Peffer, & Molina, 2017) defined smart thermostats as devices that can show controllers and indicators using interfaces that run on mobile devices such as cell phones and tablets. The paper identified five areas where consumers show sentiments and poses an opportunity for customer expectations to be met as the closely align with energy saving behaviors. The authors presented design models and tested the models for response to consumer expectations. Based on the proposed model and the test results consumer expectation and usability will be improved with the new design. The issue of end user expectations as it relates to smart thermostats were examined in the paper A Systematic Study for Smart Residential Thermostats: User Needs for the Input, Output, and Intelligence Level. Usage optimization issues were examined using input, output and the level of intelligence through data collected from interviews and surveys. The research questions were based on the usage variables: input, output and level of intelligence. The questions are:

1. “Input: via what platform? With buttons, touchscreen, speech, or gesture? Should it be set-based or satisfaction-based?”
2. “Output: What to display? How to display? Where to display?”
3. “Level of intelligence: How do users like automation indoor environment controls? What type of automation is preferred?”

The authors conducted three studies, collecting user data in all the studies. Study one explored user needs through interview and survey. Study two examined user needs through surveys. A survey of 200 people was in fact conducted. The authors focused on the popular smart thermostats at the time of the survey, which included the nest learning thermostat and the Honey well smart thermostat. As part of the results obtained, the paper identified that convenience was a very important factor for end users in choosing a smart thermostat. This was evident in the control behavior of the devices as shown by the users. The authors concluded that “an improved traditional thermostat may better fit the needs of elderly users, and the high tech with convenience as a major usability factor can be tailored to male users of 30 years old and above.”

Snow, & Auffenberg (2017) conducted on a research specific to smart thermostats to better understand the idea of an optimized and efficient human interaction with the thermostats. The authors stated that a smart thermostat is “one which better accounts for these messy social invitabilities” (Snow, & Auffenberg, 2017, p. 1595). The authors defined a smart thermostat as “A smart thermostat is a computer based agent to control temperature via HVAC systems in the home or office”, (Snow, & Auffenberg, 2017, p. 1596). Series of surveys and interviews were conducted to determine people’s definition of an acceptable temperature. The paper through the interview and survey results made a case for smart thermostats to be more intelligent. The paper focused more on feature improvement of the smart thermostats and collection of data to improve the overall smart thermostat experience. No emphasis was placed on building a secured platform that is mindful of user’s security and privacy. While it is true according to the author that “smart thermostat aims to augment intelligence, not absolve responsibility.” (Snow, & Auffenberg, 2017, p. 1603)
Manufacturers of smart thermostats have always aimed to set themselves apart by offering differentiating components and features with the IoT device. Some smart thermostats manufacturers like EcoBee offer additional sensors with their EcoBee3 thermostat, which allows for the temperatures of the other rooms within the proximity of which the main thermostat is installed to be sensed and recorded. The Nest smart learning thermostat has an intuitive smart dial and click functionality (Burrough, & Gill, 2015). The underlying focus of this paper is security and privacy with the smart thermostats. In terms of identifying who the market leader for smart thermostat is, the data available over the internet for the past 5 years shows a pattern of key players in the smart thermostat market. “Nest Labs (U.S.), Honeywell International (U.S.), Ecobee (Canada), Schneider Electric SE (France), Emerson Electric Co. (U.S.), Tado (Germany), Control4 Corporation (U.S.), Ingersoll Rand (Ireland), Carrier Corporation (U.S.) and Nortek, Inc. (France)” (Research, 2015) are some of the names of the market players. Upon surveying over 6 articles with the ranking of companies that are regarded as market leaders in this industry, and reviewing the article by Hill, (Hill, 2016) we conclude that the market leader is in fact EcoBee.

Rotondo, Johnson, Gonzalez, Waranowski, Badger, Lange, & Foster (2017) paper giving an overview of the existing and future use cases for connected thermostats gave a good account of the current state of smart thermostats, identified the big players and articulated the possible future dimensions. The paper defined a connected thermostat as “an internet connected device that enables consumers to set and modify a setpoint schedule for HVAC control and incorporates remote communication to other devices in the home or via the web.” (Rotondo, Johnson, Gonzalez, Waranowski, Badger, Lange, & Foster, 2017, p. 1). The authors identified 3 markets leader’s manufacturers in the smart thermostat space. Nest, Honeywell and Ecobee are the top three most used smart thermostats for residential homes. The paper will however focus on EcoBee and the Nest thermostat.

In an earlier study, (Burrough, & Gill, 2015) conducted a security analysis of both smart thermostats including the Honeywell smart thermostats as well. The paper offered recommendations to the manufacturers based on the vulnerabilities and weaknesses detected during the research. The paper did not however, use models or support the research with academic theories that explain the manufacturer and consumer behavioral pattern.

The table below (key IoT and smart thermostat definitions) illustrates a summary of the definitions of terms in IoT.

Table 1 – key IoT and smart thermostat definitions

<table>
<thead>
<tr>
<th>Context</th>
<th>IoT Definition</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Things</td>
<td>Interconnectivity among our everyday devices, along with device autonomy, sensing capability, and contextual awareness</td>
<td>(Hossain, Fotouhi, &amp; Hasan, 2015, p. 21)</td>
</tr>
<tr>
<td>Smart Thermostats</td>
<td>IoT ecosystem with which the smart thermostats are inclusive consists of five major components, which are: IoT devices, Coordinator, sensor bridge, IoT services, and controller.</td>
<td>(Hossain, Fotouhi, &amp; Hasan, 2015, p. 22)</td>
</tr>
<tr>
<td>Smart Homes</td>
<td>Homes deployed with IoT devices.</td>
<td>(Nurse, Atamli, &amp; Martin 2016, p. 256)</td>
</tr>
<tr>
<td>Smart Thermostats</td>
<td>Smart thermostats as devices that can show controllers and indicators using interfaces that run on mobile devices such as cell phones and tablets.</td>
<td>(Ponce, Peffer, &amp; Molina, 2017, p. 44)</td>
</tr>
<tr>
<td>Smart device</td>
<td>A smart device is described as an electronic device that connects to other devices and networks via wireless</td>
<td>(Pticek, Podobnik, &amp; Jezic, 2016, p. 2)</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>IoT is a term used to describe technologies, systems, and design principles associated with the emerging wave of Internet connected things that are based on the physical environment</td>
<td>(Pticek, Podobnik, &amp; Jezic, 2016, p. 3)</td>
</tr>
</tbody>
</table>
A smart thermostat is a computer based agent to control temperature via HVAC systems in the home or office (Snow, & Auffenberg, 2017, p. 1596).

an internet connected device that enables consumers to set and modify a setpoint schedule for HVAC control and incorporates remote communication to other devices in the home or via the web.” (Rotondo, Johnson, Gonzalez, Waranowski, Badger, Lange, & Foster, 2017, p. 1).

Analyzing the People Technology and Information (PTI) model with smart thermostats
Understanding the human behavioral and purchasing thought process with devices such as the smart thermostat can be better illustrated by positioning the verticals being considered into a model. The various unknowns in the models can then be suggested based on facts and other research elements. One model that fits this mold is the People, Technology and Information (PTI) model as shown below. Information literacy and information behavior are some of the core focus areas of information science, hence the PTI model can help build a better reasoning of the information behavior pattern of consumers of smart thermostats.

Fig 1. People Technology and Information (PTI) Model

One of the enticing facts about smart thermostats that has led to the high adoption rate and technological adoption is in the fact that they are data generators. A smart thermostat with the aid of its sensors and the connectivity to the internet reveal geographic, usage, and life pattern information about an end user. The People component of the PTI model with reference to smart thermostats, can be viewed from the perspective of the consumer and the IoT device manufacturer. With regards to security and privacy, humans are the most vulnerable to any security posture of an environment. When users of the smart thermostats operate the devices, the behavioral pattern like the temperature the user likes, the time the user spends in each room that the IoT device covers, the time the individual is at the house and the time the user leaves the house is collected. There are very many dimensions of metadata that is collected. An example of a targeted attack with the data collected from the IoT device will be breaking into a house when the sensor reports that the occupant of a house is away or through patterned occupant availability.

Information, which can be referred to as data in the context of the information generated from the smart IoT devices is the main driver of the smart thermostats manufacturers making the devices easy to install and use at the risk of higher security. Information can also be assessed from the perspective of what smart thermostat manufacturers decide to disclose to their customers as possible risks to their privacy and security. Manufacturers can hold back information that may be risk consumer confidence in their product.

Much of the advancement in technology has been fueled by the collection of the consumer big data which is then used to improve the technology. Many technology manufacturers use logging and usage data collected from
consumers to improve the technology. With the modern-day advancement in technology, social media data is used
to also improve technology. Information technology which stems from the merger between information and
technology combines the information and technology aspects in the PTI model. The intersection between people and
technology in the PTI model can be explained from the standpoint of people and their interaction with social media
for example. Most of the data collected from the usage of the IoT devices are stored in the cloud, this also brings an
interesting perspective to the model, especially with social media.

The decision for an individual to purchase a smart thermostat is dependent on the user’s accessibility to information.
Identifying the security and privacy risks of the decision is vastly dependent on the information literacy of the user.
When a user does not understand the security and privacy risks associated with using the device, they cannot make
informed decisions concerning their information that may be at risk. Within the PTI model, smart devices like the
smart thermostat for example fits the intersection between People, Technology, and Information.

**Brenda Dervin Sense making theory and smart thermostats**

Dervin’s sense making theory can help describe the landscape of smart thermostats and how consumers and
manufacturers make choices as to using the devices. With reference to the model below, in this scenario, the case
study, which is the security and privacy analysis of the Ecobee 3 and Nest learning thermostats represents the
situation. Consumers will be presented with the choice of either purchasing the EcoBee thermostat or the Nest
learning thermostat. The final product the consumer buys will be based on experience, past horizon, or future
horizon. The PTI model serves as the bridge that helps connect the consumer with the decision-making logic. Here
the knowledge of the consumer is tested against the ideas, thoughts, attitudes, emotions, narratives, all of which are
presented by the PTI model. The outcomes of the decision the consumer makes eventually presents an information
gap. Hypothetically, in a case where the EcoBee thermostat is the more secure product, and the nest learning
thermostat is the less secure one. The consumers decision has presented some information gaps. The choice will
affect the outcomes of the consumers perception of the product or even smart thermostats at large.

Within the Dervin’s model, there are known and unknown information gaps. This may be confusions that the
customer may have and other unknowns when making the purchase decision. The gaps are also the some of the
bridge constraints that the PTI model does not fully address.
Security and Privacy Issues

WIFI Encryption Standards
Wireless security standards have evolved over the years. Throughout the technological evolution, however, security has evolved with it as well. Wireless security is important to prevent unauthorized access to the network, which could compromise the systems within the network. The two well-known wireless securities are the Wired Equivalent Privacy (WEP) and the Wi-Fi Protected Access (WPA). Of the two listed wireless security protocols, WPA is the most secure, however, WPA has been revised to form WPA2. WPA2 is a more secure alternative.

In the analysis of the two smart thermostat products, EcoBee and the Nest thermostat both support all the WIFI security protocols. This is an example of a situation where the manufacturer puts convenience and ease of use of the consumers ahead of security. Both IoT devices get connected to the network and get assigned IP addresses within the network with which they are installed. Once an attacker can compromise a weak WIFI infrastructure, the attacker can cause damage the IoT devices as well.

Password Requirements
The EcoBee and the Nest smart home thermostats, like other IoT devices, can be accessed via the web through their web application portal or through a mobile device. The remote administration of the devices can be done through the web portal. Maintaining a high password requirement is important because of the harm that can be caused if an unauthorized user gains access to the password. An unauthorized user can heat up the house, thereby causing suffocation. For residence where pets are kept, this could be life threatening. Access to confidential usage data will be exposed if the password is compromised.

While the EcoBee and Nest smart thermostats enforce an eight-character long password requirement, upon further testing, some end-user compromises that reduced the security posture of these devices were uncovered. IoT manufacturers cannot afford to compromise on password requirements for the IoT device access. EcoBee allowed an eight all text and no number password, such passwords are very vulnerable to dictionary attacks. Nest, however, enforces an alphanumeric with special character password combination, which is far less susceptible to dictionary
attacks. While both management portals have account lockout thresholds, the EcoBee and the Nest web application allow re-use of passwords, this is a bad security practice. This leaves room for password guessing.

**Security Statement**
The security statement by an IoT manufacturer goes a long way to affirming their stance on security and privacy with regards to their devices. A security statement document is a statement that clearly defines an organization position on the safety standards, privacy and security practices. The findings from the review of EcoBee and Nest security statement on their website has been listed below.

EcoBee has page on their website titled “How do I know it’s secure?”, the company posted “ecobee is committed to protecting our customer’s privacy. ecobee supports WEP, WPA and WPA2 security for connecting to Wi-Fi networks. ecobee products and services use an SSL connection to ensure the highest level of security. The SSL protocol is commonly utilized by banks, government agencies and e-commerce sites to ensure privacy and the protection of personal information.”

The security statement page on EcoBee’s site as of the time this paper is being written hasn’t been updated since September 9th, 2014. For an evolving topic like security, the expectation is that the IoT manufacturer should continue to add more security features and publish the new additions on the security page. This shows the level of attention that is being paid to security by the manufacturer as compared to consumer usability of the products.

The Nest thermostat does not have a page dedicated to security, however, the company has a page that covers issues with regards to security and data protection. In 2015, it was reported that a vulnerability was found with the Nest smart thermostat that allowed an attacker to infiltrate the WIFI infrastructure (Hernandez, Arias, Buentello & Jin, 2014). This is a huge security risk. Though the vulnerability has been fixed, it is an example of an unpatched IoT device introducing a vulnerability to a secured environment. On the Nest website, there were more details provided to address how the Nest team handles security and data privacy. While direct reference was not made to the OWASP top 10 vulnerabilities, most of the security interests listed were top on the OWASP top 10 web application vulnerability list.

**OWASP Top IoT Vulnerabilities**
The Open Web Application Security Project (OWASP) a non-profit organization popular for the OWASP Top 10 Web application vulnerabilities publication saw a need for a similar publication on IoT. The OWASP Top 10 web application vulnerabilities list hasn’t changed much since 2013, however many web application security scanning tools use the metric to prioritize scanning and reporting of their penetration testing. OWASP analyzed the IoT security and privacy trends and published a top 10 list of IoT vulnerabilities. The list is to help raise awareness of security vulnerabilities inherent in IoT devices. This helps start a conversation regarding design priorities for IoT manufacturers. The UI development for the web applications and mobile applications should prioritize design based on the OWASP guidelines.

The top 3 lists on the OWASP IoT vulnerabilities list is Insecure Web Interface, Insufficient Authentication/Authorization, and Insecure Network Services. Both the EcoBee and Nest thermostat fall short of this requirement. Insecure Web Interface does not only refer to the communication between the consumers’ web interface to the manufacturer's server, the chain of trust of the transaction that happens after the initial sign-in is even more important. Security and privacy are always evolving, hence the IoT manufacturers should continue to revisit the guidance and test continually for holes.
Conclusion

IoT devices should not be allowed to connect to less secure wireless infrastructure. The amount of data that can be stolen and the damage that can be caused by compromising the wireless network hence gaining access to confidential information is not worth the risk. This calls for a need for an IoT security model. ZigBee wireless infrastructure devices serve as a low powered wireless backbone for IoT devices. ZigBee typically connects to wireless infrastructure as a mesh network. This sets the precedence for higher security for the IoT devices connected to the ZigBee network.

Reducing best practices standards for passwords cannot be allowed. The IoT manufacturers are putting the consumers and their information at risk. It is unethical to allow exposure to consumers of the IoT devices hacks that have proven to be effective, without helping the end users ensure that this does not happen. This is clearly negligence on the part of the IoT manufacturers. With the data generated from the IoT devices stored in the cloud, it is imperative that the IoT manufacturers provide the consumers with a 2-factor authentication to their management portal as against relying on the mobile application to provide this feature.

The need for a standardized IoT model that hones security and privacy of consumer data cannot be emphasized. The following guidance as provided by OWASP and data protection laws should be a requirement for IoT manufacturers. Consumers should have ownership of the data the devices they purchase generate. Only consumers should have the right to how the data generated can be shared or the retention of the data. EcoBee and Nest thermostats do not provide easily accessible options to customers at a granular level to control their privacy and data retention.

IoT is fast growing. The opportunities and possibilities are endless, so are the threats and dangers that consumers face if IoT manufacturers are negligent towards security and privacy issues. With IoT, security and privacy are not a question of due diligence or due care, they both should be the primary focus. The goal is not to slow down the pace of innovation, it more about integrating security and privacy by design practices as IoT devices evolve.

Even with the PTI model, the Dervin’s sense making model help us identify the gaps within the model and areas of confusion that a consumer might have. Collecting real life data of consumers of smart thermostats in the form of interviews and survey can help answer some behavioral questions and also the gaps in the research.
References
https://nest.com/privacy/data/