Human Factors in the Privacy and Security of the Internet of Things

Although attempts have been made to increase IoT security, the role users can play in protecting their information has been overlooked. This paper explores the necessity of taking a user-centered approach to privacy/security when designing/developing IoT technologies.

By Isis Chong, Aiping Xiong, & Robert W. Proctor

FEATURE AT A GLANCE:
The "Internet of things" (IoT) refers to Internet-enabled technologies designed to increase the efficiency of users' lives by communicating with other objects and elements in a system. The growth in these interconnected devices has been matched with increases in the use and aggregation of data collected by vendors or third parties. The number of hackers attempting to access users' private information also has grown. Although attempts have been made to increase IoT security, the role users can play in protecting their information has been overlooked. We illustrate the necessity of taking a user-centered approach to privacy and security when designing and developing IoT technologies.

KEYWORDS:
cybersecurity, user-centered design, smart devices, hacking, training, warnings

The nighttime monsters under your child's bed might be imaginary, but other monsters in her room might not be. Recently, hackers have infiltrated baby monitors not only to watch others' children but also to talk with them in lewd ways (Flannigan, 2016). As isolated as one might wish this incident to be, the devices many users have trusted to ensure their well-being and safety have been compromised by hackers with nefarious motives. Unlike the proverbial monster under the bed, however, hackers and the security violations they bring forth in their wake are far from imaginary.

Humans are increasingly incorporating Internet-enabled technologies into their everyday lives. For example, smart refrigerators allow individuals to use smartphones to schedule hot water to be dispensed, and a smart office building can adjust lighting and temperature to suit workers' preferences based on input received from them or from sensors.

The number of actions that can be automated by different devices with distinct user populations is substantial. These devices can be referred to as being part of the "Internet of things" (IoT), a network in which objects share and communicate information with other elements (Gubbi, Buyya, Marusic, & Palaniswami, 2013). Most recently, for example, a company in the United States began offering its employees the opportunity to implant a radio frequency identification (RFID) microchip that allows them to open doors, log onto computers, and purchase food items by a simple wave of the hand (Baenen, 2017). Although the IoT allows for the transfer of data between devices and many other components, the interconnected nature of the IoT embeds security blind spots that can ultimately leave the devices in IoT susceptible to hacking.

Researchers have suggested that security issues related to the IoT can be addressed by taking several countermeasures focused on securing accurate data and transferring these data with protection (Aleisa & Renaud, 2017). Such methods include, but are not limited to, performing a more thorough analysis of home router network traffic (Sivaraman, Chan, Earl, & Boreli, 2016) and increasing device encryption efforts (Hernandez, Arias, Buentello, & Jin, 2014).

Unfortunately, most researchers fail to consider that users are regarded as the weakest link in the cybersecurity chain (Sasse, Brostoff, & Weirich, 2001), and very few researchers have commented on the value of designing IoT devices with the user as an integral security component (Aleisa & Renaud, 2017; Zhao & Ge, 2013). This oversight can prove to be dangerous, as failing to consider the ever-present human component of the system has the potential to render any state-of-the-art security mechanism useless. As such, we argue that to ensure users' safety, researchers and designers must take a human factors approach to cybersecurity in which the human in the loop (Cranor, 2008) is considered throughout the design and implementation process.

We summarize current trends in Internet-enabled technologies that need to be considered during the design process to ensure users' privacy and security. If designers and developers will not be advocates for securing their users' information to begin with, how can we expect humans to protect themselves from the threats posed by hackers?

Table 1. The Five Primary Technologies Used for IoT Devices

Technology	Description	Example
Radio frequency identification (RFID)	Radio waves, a tag, and a reader are used to automatically identify and track physical items.	Packages can be tracked when transported from location to location.
Wireless sensor networks (WSN)	Spatially distributed sensors are used to monitor physical or environmental conditions.	A smart thermostat can use these sensors to adjust temperature settings.
Middleware	Software that serves as a bridge between a database or operating system and applications.	Middleware can be used to allow communication between different smart devices.
Cloud computing	Model for accessing a shared pool of configurable resources.	Smart surveillance systems can access hours of security footage saved in the cloud.
IoT applications	Applications that allow for human-to-human and device-to-device communication.	Homeowners can use mobile applications to control their smart devices.

Source. Lee and Lee (2015).
Note. IoT = Internet of things.

WHAT IS THE CURRENT STATE OF IOT?

To understand the importance of adopting a human-centered approach to IoT security and privacy, one must first focus on the current state of interconnected devices and how users interact with them.

IoT technologies. The successful deployment and implementation of IoT-based products and services rely primarily on five technologies:

a. RFID,
b. wireless sensor networks (WSN),
c. middleware,
d. cloud computing, and
e. IoT application software (Lee & Lee, 2015; see Table 1 for detailed descriptions).

Consideration of the range of technologies that make up the IoT is key to understanding how users can come to interact with IoT devices. In the case of devices utilizing RFID, for example, identifying information can be shared in a manner similar to, but more sophisticated than, reading a bar code. Other IoT devices, however, may require users to program their IoT devices using a mobile application. Although the interaction complexity of one device can differ greatly from that of another IoT device, these devices promise to streamline users' day-to-day lives.

Nest devices. To exemplify both the benefits and potential drawbacks of the IoT, we turn toward an increasingly popular IoT device, the Nest Learning Thermostat (see Figure 1). The Nest Learning Thermostat utilizes cloud computing to learn and adapt to each unique household. Consider a particularly cold winter morning, when even the best of us have struggled to get out of bed and begin our day. The idea of getting out from under our covers seems like a Herculean task designed for only those with an iron will. There are those among us who might even begin to wonder if calling in sick to work is an option.

Figure 1. Example of a third-generation Nest Learning Thermostat. This product was chosen as a sample representation of Internet-of-things devices and is not endorsed by the authors. Photo courtesy of Nest Labs.

The Nest Learning Thermostat promises to make these mornings a bit less daunting by warming up your home before you wake up. By learning from your typical behaviors and inputs, it can prepare your home for your day ahead even though you might not be. What might once have been a cold morning is instead a morning like any other. Before heading out the door, remembering to turn down your thermostat to avoid a costly heating bill is no longer an issue. This smart device knows when you leave your home and can begin to warm the house based on your expected time of arrival.

The Nest Learning Thermostat and similar smart home devices are considered to be at the forefront of IoT innovation (Lee & Lee, 2015). With access to information from sensors, past user inputs, and users' smartphones, the Nest Learning Thermostat also has the ability to change a wide number of settings in users' homes to increase energy efficiency and inform users of potentially harmful situations. A malfunctioning furnace, for instance, triggers a notification to be sent to the app designed for all of a user's Nest devices. The user is then informed of the problem and told that maintenance may be required. Another of the Nest Thermostat's features, Airwave, controls air in the home so that cool air from the air conditioner is dispersed by the fan without further taxing the cooling unit and wasting energy in the process.

From an economic standpoint, users may save on their utility bills and even be rewarded by energy companies for saving during peak use hours. The potential for energy savings is so alluring that energy and security companies offer rebates or provide the Nest Learning Thermostat at no additional cost. Like other IoT devices, this thermostat's automation promises to increase efficiency while minimizing time and cost.

Despite the number of benefits of this device, The Nest Learning Thermostat has been shown to have a number of security issues. Vulnerabilities have allowed individuals to hack the device to access users' personal information (Hernandez et al., 2014). Hernandez and colleagues (2014) found a "back door" whereby simply holding down the thermostat's Home button for 10 seconds and plugging in a USB device with custom firmware gave them full control over the device.

Hacking into a home thermostat may seem innocuous, but this device is essentially a computer that stores information about when users are home, when they sleep, and even when they walk by the device. This information can be used to ultimately track individuals and, in the case of similar smart devices in business settings, potentially can be used to determine when proprietary information can be stolen. Additionally, although successful attacks on the Nest Learning Thermostat have been local and not conducted remotely, hacking attempts made into many other smart device systems have demonstrated that hackers do not have to be physically present to wreak havoc. Although Nest recently made upgrades to its software to increase the security of its devices (King, 2017), system susceptibility to hacking still lingers.

It should be noted that these security issues are not unique to the Nest Learning Thermostat and can be found across a number of IoT appliances (Notra, Siddiqi, Gharakheili, Sivaraman, & Boreli, 2014). For example, Nest's indoor/outdoor security camera with firmware Version 5.2.1 has been found to have vulnerabilities that allow hackers to send Wi-Fi data via Bluetooth to make the camera crash, restart, or disconnect (Estes, 2017). In a nod to Nest users who moonlight as hackers and a proposal vaguely reminiscent of the Ides of March, Hernandez and colleagues (2014) suggested that in the event that legitimate users cannot access their settings directly, they can utilize security holes to attack their own Nest device.

Widespread hacking attacks from legitimate users to take back control of their devices might leave many developers and designers proclaiming, "Et tu, user?" If users are not proficient in coding and lack the skills necessary to hack into their Nest Thermostat, they are always free to read through the more than a dozen legal items related to the device to gain a more accurate picture of the rights, obligations, and responsibilities of all parties involved with the thermostat (Noto La Diega & Walden, 2016). Unfortunately for owners of this smart thermostat, slightly scaling back functionality to increase security is not an option, as the alternative is to have the device function without any smart components at all.

In defense of the efforts of the maker of the Nest Thermostat to secure users' privacy and security, the marketing for these devices focuses on energy efficiency, not on security features. At the time of this writing, the latest Nest Thermostat device, the Nest Thermostat E, is marketed as an "easy-to-use, energy-efficient, control-it-from everywhere" device (Veron, 2017). With a lower price point than its predecessors, this thermostat is marketed primarily on its being a more accessible, yet aesthetically pleasing, device. Missing from these advertisements, however, are potentially off-putting tech buzzwords that mention the device's learning algorithms (Tilley, 2017) and, more important, the security features designed to protect this user-specific information.

In actuality, many companies rarely mention security and privacy in their marketing materials (Wilson, Hargreaves, & Hauxwell-Baldwin, 2017), and this lack of mention may be indicative of their current design efforts. Although the U.S. government has released general design principles related to IoT security, these principles have not been translated into binding human-centric regulations (Moskvitch, 2017; Ziegeldorf, Garcia-Morchon, & Wehlrle, 2014). These oversights may, in part, be due to misconceptions about the potential role that humans can play in securing IoT devices and protecting their personal information (Aleisa & Renaud, 2017). We argue, however, that if given the proper tools and information, users can take part in defending their privacy.

HOW DO WE ENABLE USERS?

Bringing users into the fold requires designers and developers to understand that users hold the potential to be capable and informed elements of a system. Considering users and the various interactions they have with the system can allow designers to have a more well-rounded approach to understanding and ensuring IoT security (Jeske & van Schaik, 2017). To highlight the role users can play in protecting their privacy and minimizing their risk, we discuss steps that can be taken long before a cyberattack actually happens and what can be done when a hacking attempt occurs.

Equipping the user. Working toward ensuring users' privacy and security should begin by considering what users are like before they begin to use an IoT device. When users begin using a smart device for the first time, are they considering their safety and security? Or, perhaps, are they more concerned with a particular function of the device? The answers to these questions can differ from one user to the next.

Designers and developers should evaluate, among other factors, how users think about their safety, their motivation to be proactive in securing their information, and the trust they have in interconnected devices, as these factors will affect how users interact with their devices. For instance, the average user lacks an adequate understanding of the number and type of Internet-related risks to which he or she might be exposing him or herself (Harbach, Fahl, & Smith, 2014) and the role he or she can play in securing his or her information (Furman, Theofanos, Choong, & Stanton, 2012). This situation can be improved; an increased awareness of privacy threats and risks is correlated with the number of protective actions users report having taken (Kang, Dabbish, Fruchter, & Kiesler, 2015).

Given the protective role that information about safety and security may have, designers of IoT systems should aim to cultivate knowledge among their users. In other words, how can we give users a base-level understanding of what security issues they might encounter, and how can we teach them how to avoid those issues?

Training, for instance, can be used to disseminate knowledge about the importance of protecting one's personal information and the actions that can be taken to prevent third parties from accessing that information. The format that training takes can be highly variable, given the large number of environments in which IoT devices can be used and the different roles various users might assume.

In an attempt to address this variability, intelligent training systems that adapt to a user's specific profile and instructional requirements have been proposed (Mangold, 2012). These training systems would involve activities and assessments catered specifically to an individual or an organization and the respective needs of either. An employee, for example, might receive less technical training than an administrator within the same organization. Alternatively, embedding training in a typical use setting can increase security knowledge of general users (e.g., Kumaraguru et al., 2007). For instance, a prompt on a smart baby monitor can occasionally remind the user that changing the password often can better protect his or her information.

Beyond training, users can be equipped with tools that help them determine the safety of an IoT device. Researchers have proposed a mobile app that supports users' privacy-related decisions (Broenick et al., 2010). A "privacy coach" in the form of a mobile app can inform users if an RFID privacy policy matches up with their preferred privacy settings. On the whole, these types of tools may make users more aware of their role in the system and what can be expected for their privacy.

In addition to encouraging risk awareness, designers of IoT devices should focus on instilling trust among users (Hoff & Bashir, 2015). All devices should be able to perform their basic functions reliably, but in the case of smart, interconnect devices, users should be assured that their information will be handled properly and that they will have the ability to revoke access to this information at any time. IoT devices are designed specifically to work with large amounts of users' data, so a reduction in access to users' information can be counterproductive to the overall goals of an IoT device. As such, it is important to reassure users about their device's safety. When considering baby monitors, for instance, it is not enough for users to know that their device is transmitting an image of their child for them to monitor remotely; users must be assured that only they have access to this feed.

Putting users at ease may involve including a certain level of transparency as to what steps are being taken to protect their personal information. Increasing overall levels of trust may lead users to be more inclined to allow IoT devices access to information they might not grant access to if there were doubts about the security capabilities of the IoT system (Lee & Lee, 2015).

The user characteristics mentioned herein are merely a select few of the many factors that can affect a user's willingness to be an active participant in securing his or her information. An IoT user in a home environment may differ significantly from an employee in an office setting, just as a novice differs from an expert user. Aside from very specific training and personalized recommendations, more general design implementations may encourage users to make more security-minded decisions.

Although users may differ in their overall motivation and their general enthusiasm toward securing their interconnected devices, implementing concise and easy-to-perform security instructions and minimizing user effort may be more effective than designing a system that defaults to allow for a high level of security customizability. Forget et al. (2016), for instance, found that some users tend to think that their computer systems are secure by default; as such, users are more likely to avoid taking action to ensure the security of their devices. These users in particular may provide benchmarks for implementation of straightforward security functionality setups, such as disabling remote-management access or other similar far-reaching network tools.

Warning the user. Roman, Najera, and Lopez (2011) argued that a key component of a fault-tolerant IoT system includes objects that are able to defend themselves not only against network failures but also from outsider attacks. Items in the IoT should be able to use intrusion detection software and other tools to hold back attackers. As sophisticated as IoT systems may be, the rate at which hackers infiltrate cybersystems might leave programmers playing a perpetual cat-and-mouse game. Any abnormal activities or situations should eventually result in the degradation and gradual cessation of service. Users, however, should be made aware of critical events as they occur.

For instance, in the case of widespread malware attacks, once an issue is identified with other devices, a user should be notified immediately of the increased likelihood of an attack occurring to them. In such cases, encouraging users to change their passwords or take other necessary precautions might alleviate headaches associated with stolen information and compromised privacy.

Although the average user does not possess the skill set necessary to combat a hacker keystroke by keystroke, as is often depicted in Hollywood dramas, information about a potential hack should allow users to take other, more plausible courses of action. Work focused on other domains, such as mobile app selection, has revealed that transparency about data collection and sharing can benefit users greatly (Van Kleek et al., 2017). Sharing information with users has been shown to leave individuals with the ability to make informed decisions that align better with their preferences and overall worldviews.

Along the same lines, although IoT users may be unaware of the large number of IoT interactions that take place behind the scenes, presenting warnings and sharing information about any potential cyberthreats may allow users to jump back into the loop to make their own decisions about their safety. A user who is warned that his refrigerator has been hacked, for instance, may opt to change his login credentials or, at the very least, remove his online account information from the grasp of the appliance. Surely, that must be what real-life users who found themselves in the possession of refrigerators sending out spam e-mails in 2014 would have done if warnings had been available (Beck, 2014). This particular instance of remote attacks reportedly sent out 750,000 malicious e-mails from everyday smart appliances (Kharpal, 2014).

For warnings to ultimately make a difference in protecting user information, users' actions must be congruent with any warnings they receive (Meyer, 2004). A warning should result in users' taking some action toward securing their information. The highest compliance rates are associated with warnings designed to contain relevant and useful information (Meyer, 2001).

A hacking warning presented without useful information may be less effective than a warning presented with some insight on the state of the IoT system. For instance, a very basic warning may be ignored, whereas a warning about someone requesting remote access to a user's information may be more effective at eliciting action. If a simple software bug is identified, this proposed warning system may be as straightforward as presenting a text prompt urging users to install the latest software version in addition to a rationale for this update. Compared with a simple text prompt that simply suggests a software update, users will probably be more likely to oblige in the latter case when they are provided with additional information.

CONCLUSION

In August 2017, members of the U.S. Congress introduced the Internet of Things Cybersecurity Improvement Act of 2017, a bill with the intention of securing IoT-enabled federal devices (Warner, 2017). Cybersecurity, however, is a complex issue, and maintaining privacy and security requires a concerted effort on the part of all designers and developers across different sectors and beyond any narrow standards that might come to be established by legislation. Users should be able to use their interconnected devices with confidence, where even programming a smart thermostat leaves them free from fear for the security of information or, in more severe cases, physical safety.

In this article, we raise the need to take a human factors approach to security and privacy when designing IoT devices. This work, of course, is far from a prescription on how to address hacking attempts. We highlighted the importance of considering the human user as yet another defense against ever-present cyberattackers. Work must go from creating simple coding patches to taking users into account at the earliest stages of the design process. Designers and developers should consider who the users are and how they can be called to action when facing privacy and risk issues.

If researchers and designers truly wish to fight the cyberattackers encroaching on privacy and security in the IoT, a well-rounded approach that includes users must be taken.

REFERENCES

Aleisa, N., & Renaud, K. (2017). Privacy of the Internet of things: A systematic literature review. In *Proceedings of the 50th Hawaii International Conference on System Sciences*. Retrieved from http://hdl.handle.net/10125/41881

Baenen, J. (2017, August 2). Wisconsin company holds "chip party" to microchip workers. *Chicago Tribune*. Retrieved from http://www.chicagotribune.com/bluesky/technology/ct-wisconsin-company-microchips-workers-20170801-story.html

Beck, R. (2014, January 18). Smart refrigerators hacked to send out spam. *NBC News*. Retrieved from http://www.nbcnews.com/tech/internet/smart-refrigerators-hacked-send-out-spam-report-n11946

Broenink, G., Hoepman, J. H., Hof, C. V. T., Van Kranenburg, R., Smits, D., & Wisman, T. (2010, May). *The privacy coach: Supporting customer privacy in the Internet of things*. Paper presented at Pervasive 2010, Helsinki, Finland. Retrieved from https://arxiv.org/pdf/1001.4459.pdf

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. In *UPSEC'08 Proceedings of the 1st Conference on Usability, Psychology, and Security* (pp. 1–15). New York, NY: ACM.

Estes, A. C. (2017, March 22). This Nest security flaw is remarkably dumb. *Gizmodo*. Retrieved from http://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264

Flannigan, J. (2016). Parental warning: Baby monitors can be hacked. *Healthline*. Retrieved from http://www.healthline.com/health-news/baby-monitors-can-be-hacked#1

Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., & …Telang, R. (2016). Do or do not, there is no try: User engagement may not improve security outcomes. In *Proceedings of Twelfth Symposium on Usable Privacy and Security (SOUPS)* (pp. 97–111). Denver, CO: USENIX Association.

Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, *10*, 40–49.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*, 1645–1660.

Harbach, M., Fahl, S., & Smith, M. (2014). Who's afraid of which bad wolf? A survey of IT security risk awareness. In *Proceedings of IEEE 27th*

Computer Security Foundations Symposium (CSF) (pp. 97–110). Piscataway, NJ: IEEE.

Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2014, August). *Smart Nest thermostat: A smart spy in your home*. Paper presented at Black Hat, USA, Las Vegas, NV. Retrieved from https://pdfs.semanticscholar.org/f1aa/f326c8b2cb6a94fa105b9910125e61920714.pdf

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*, 407–434.

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, *66*, 129–141.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). “My data just goes everywhere:” User mental models of the Internet and implications for privacy and security. In *Proceedings of Symposium on Usable Privacy and Security* (pp. 39–52). Berkeley, CA: USENIX Association.

Kharpal, A. (2014, February 24). Can your fridge be hacked in the “Internet of things”? *CNBC*. Retrieved from https://www.cnbc.com/2014/02/21/can-your-fridge-be-hacked-in-the-internet-of-things.html

King, R. (2017, March 7). Nest is turning up the security on its thermostats. *Fortune*. Retrieved from http://fortune.com/2017/03/07/nest-thermostat-security/

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 905–914). New York, NY: ACM.

Lee, I., & Lee, K. (2015). The Internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*, 431–440.

Mangold, L. V. (2012). Using ontologies for adaptive information security training. In *Proceedings of Seventh International Conference on Availability, Reliability and Security (ARES*; pp. 522–524). Piscataway, NJ: IEEE.

Meyer, J. (2001). Effects of warning validity and proximity on responses to warnings. *Human Factors*, *43*, 563–572.

Meyer, J. (2004). Conceptual issues in the study of dynamic hazard warnings. *Human Factors*, *46*, 196–204.

Moskvich, K. (2017). Securing the IoT in your smart home and your connected enterprise. *Engineering and Technology*. Retrieved from https://eandt.theiet.org/content/articles/2017/03/securing-the-iot-in-your-smart-home-and-your-connected-enterprise/

Noto La Diega, G., & Walden, I. (2016). Contracting for the “Internet of things”: Looking into the Nest. *European Journal of Law and Technology*, *7*, 1–38.

Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014). An experimental study of security and privacy risks with emerging household appliances. In *Proceedings of 2014 IEEE Conference on Communications and Network Security (CNS*; pp. 79–84). Piscataway, NJ: IEEE.

Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of things. *Computer*, *44*, 51–58.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the “weakest link”: A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*, 122–131.

Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016). Smart-phones attacking smart-homes. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (pp. 195–200). New York, NY: ACM.

Tilley, A. (2017, August 31). Nest launches a cheaper thermostat to bring the smart home to the masses. *Forbes*. Retrieved from https://www.forbes.com/sites/aarontilley/2017/08/31/nest-cheap-thermostat-e/#7e9a0cfe2b48

Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., & Shadbolt, N. (2017). Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 5208–5220). New York, NY: ACM.

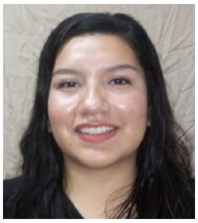
Veron, M. (2017, August 30). *E is for everyone*. Retrieved from https://nest.com/ca/blog/2017/08/30/e-is-for-everyone/

Warner, M. R. (2017, August 1). *Senators introduce bipartisan legislation to improve cybersecurity of “Internet-of-things” (IoT) devices*. Retrieved from https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy*, *103*, 72–83.

Zhao, K., & Ge, L. (2013). A survey on the Internet of things security. In *Proceedings of 9th International Conference on Computational Intelligence and Security* (*CIS*; pp. 663–667). Piscataway, NJ: IEEE.

Ziegeldorf, J. H., Garcia-Morchon, O., & Wehrle, K. (2014). Privacy in the Internet of things: Threats and challenges. *Security and Communication Networks*, *7*, 2728–2742.



Isis Chong *is a doctoral student at Purdue University in the Department of Psychological Sciences. She received her master’s degree in human factors psychology from California State University, Long Beach. Her research deals with investigating cybersecurity issues with a focus on human information processing. She is co-president of the Human Factors and Ergonomics Society Purdue University Student Chapter.*

Aiping Xiong *is a postdoctoral fellow in cognitive psychology and human factors at Purdue University. She received her master’s degree in industrial engineering in 2014 and PhD in cognitive psychology in 2017 at Purdue University. Her research focuses on applying basic cognitive principles and theories to understand human action selection and decision making within various cybersecurity and privacy settings.*

Robert W. Proctor *is Distinguished Professor of the Department of Psychological Sciences at Purdue University, with a courtesy appointment in the School of Industrial Engineering. He is a fellow of Purdue’s Center for Education and Research in Information Assurance and Security. He received his PhD from the University of Texas at Arlington in 1975 and specializes in basic and applied human performance. He may be reached at rproctor@purdue.edu.*

This work was supported in part by the National Science Foundation under Grant Numbers 1314688 and 1539527.

DOI: 10.1177/1064804617750321