Human Factors in Smart Home Technologies Workshop

September 24, 2019
Workshop Summary

Authors:
Susanne Furman
Julie Haney

Information Technology Laboratory
National Institute of Standards and Technology

Report Date: November 5, 2019

Abstract

On September 24, 2019, the National Institute of Standards and Technology (NIST) hosted a one-day workshop entitled "Human Factors in Smart Home Technologies." The workshop addressed human considerations for smart home devices, including usability, user perceptions, and end-user privacy and security considerations. Invited speakers from industry and academia provided their perspectives via presentations and a moderated panel. In addition to becoming more aware of human aspects of smart home technologies, the attendees from industry, government, and academia had the opportunity to influence NIST's future research direction in this area by voicing their opinions, challenges, and ideas during afternoon breakout sessions. This report provides a summary of the workshop, including presentations, panel discussion, and breakout session overviews.

Keywords

Smart homes, internet of things, IoT, usability, cybersecurity, privacy

Disclaimer

Throughout this summary report, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose. In addition, the opinions of speakers and attendees summarized in this report do not necessarily represent NIST's official stance on these topics.

Background

The Internet of Things (IoT) market is rapidly expanding, with the number of IoT devices worldwide expected to grow from 20 billion in 2017 to 75 billion in 2025 [1]. With this growth, IoT technology is becoming more pervasive in the home environment. While early adopters of smart home technologies have typically been more technically savvy, these devices are increasingly being used by non-technical users who may have little understanding of the technology or awareness of the implications of use. In addition to well-known usability factors (e.g., error recovery, feedback, context), consumers may be impacted by other contributing factors, such as security, privacy, trust, accountability, and device transparency.

To provide a forum to explore these issues, on September 24, 2019, the National Institute of Standards and Technology (NIST) hosted a one-day workshop entitled "Human Factors in Smart Home Technologies." The workshop addressed human considerations for smart home devices, including usability, user perceptions, and end-user privacy and security considerations. Invited speakers from industry and academia provided their perspectives via presentations and a moderated panel. In addition to becoming more aware of human aspects of smart home technologies, the attendees from industry, government, and academia had the opportunity to influence NIST's future research direction in this area by voicing their opinions, challenges, and ideas during afternoon breakout sessions. Dr. Susanne Furman, a cognitive scientist in NIST's Information Technology Laboratory (ITL) Visualization and Usability Group (VUG), served as the workshop's master of ceremonies. She was joined in conference co-chair duties by Julie Haney, a computer scientist in VUG.

This report provides a summary of the workshop, including presentations, panel discussion, and breakout session overviews.

Presentations

This section summarizes presentations given during the workshop's morning session.

Opening Remarks

Jim St. Pierre, the Deputy Directory of the NIST Information Technology Laboratory (ITL), provided opening remarks. Mr. St. Pierre welcomed the attendees to the workshop and summarized NIST's previous and current IoT work, for example, NIST's core cybersecurity baseline for IoT [2] and guidance on mitigating IoT network-based attacks using the Internet Engineering Task Force (IETF) Manufacturer Usage Description (MUD) standard [3]. He emphasized the importance of considering human factors in both IoT smart home design and the development of IoT guidance.

Keynotes

Invited keynote speakers were:

1. Rob Martens, President of Allegion Ventures & Allegion Futurist, and Bobby Prostko, Allegion, Principal, Allegion Ventures
2. Dr. L Jean Camp, Professor, Indiana University School of Informatics and Computing
3. Jason Mathew, Sr. Director, Global Connected Strategy at Whirlpool Corporation
4. Julie Haney, VUG, NIST Usable Cybersecurity project lead

Rob Martens & Bobby Prostko, Allegion
What the Intersection of New Technology, Cybersecurity, and Privacy Means to Allegion and Our Customers

Allegion views their products as life safety devices that need to work all the time without exception. Their belief is that when they partner with other vendors, if that vendor's product has a security problem, it becomes Allegion's problem.

With their products, you own your identity and data, which is in contrast with that of the majority of startups whose business models are based on owning your identity. They believe there has been a consumer backlash with privacy because of high-profile data breaches.

Allegion's privacy approach has been influenced by:

- European Union's General Data Protection Regulation (GDPR) – privacy-by-design and privacy-by-default. Rob and Bobby see similar laws coming to the U.S. in the future.
- California Consumer Privacy Act – GDPR-like requirements; "do not sell my personal data" provision
- California IoT law – requires "reasonable" security features; passwords must be unique or require change on first use
- Australia Assistance and Access Act – developers must be able to disable encryption or create backdoors for government; however, Allegion is concerned about this because doing so defeats the security architecture.

Allegion S^3 principles are:

- Security
- Simplicity
- Scalability

Dr. L Jean Camp
Security: What is the Problem and Why

Dr. Camp presented research about people's security and privacy attitudes. Research has found that people don't care about privacy, don't know the risks, or they know the risk but just can't do anything about it.

The consumer typically cannot distinguish between low risk and high risk. Risk communication can help users make better decisions about their privacy. But how?

- People do not care about the risk: they need incentives and economics
- People do not know about the risk: better risk communication is required
- People do know and care: they require usable technology

To solve the problem, Dr. Camp's research shows that creating useful, timely, and actionable risk communication is important. The goal of risk communication is to change behavior and create a partnership. But warnings designed for the "typical" user do not necessarily resonate with populations that are not typical. She offered the following recommendations:

- Make the risks clear and create benefits.
- Solve the problem by empowering people to protect themselves.
- There are well-established methods we can use such as known research on risk communication and rewards and usability design guidelines and evaluations.
- We need to treat people as participants.
- Do not look at averages; rather design for the most vulnerable communities.

- Build the interface for busy people by: respecting cognitive limits; saying why, not just how; creating good defaults; and respecting and learning from failures.
- Give people controls that they can understand and trust, for the privacy and security they choose.

Jason Mathew – Whirlpool
Technology can be very powerful but also very destructive. Technological and societal changes have led to the most demanding consumer they have ever experienced. Power has shifted from companies to consumers. Consumers no longer have to make a commitment to a company. The challenge is how to make technology *for* humanity instead of technology *vs.* humanity.

Most consumers are hopelessly confused. Early adopters (i.e., enthusiasts and visionaries) want technology and solutions. Pragmatists and conservatives want solutions and convenience. But we are a decade away from getting to mass market in IoT/smart home technology. Technology should fulfill human needs for connection (belonging), power, achievement, freedom, efficiency, and pleasure. Artificial Intelligence (AI) is powerful but it has its limitations. For example, AI cannot determine a context, lacks common sense, cannot make inferences, and cannot make analogies.

The basis for competition is STILL about trust, not just data, devices, or footprint. Rather it is about winning the war for the heart and mind of the consumer by building trust. Whirlpool wants to provide great brands with a clear purpose and not just sell consumers a product but also service it for years. But the question may be: will technology advances shorten the life cycle of products?

Julie Haney
Consumer Perceptions of Smart Home Privacy and Security
Ms. Haney presented the preliminary results from a NIST study of consumers of smart home devices. She presented data analysis focused on user perceptions of smart home privacy and security and answering the following research questions:

- What are smart home users' privacy and security concerns, if any?
- What privacy/security mitigation actions do users take, if any?
- Who do users believe is responsible for the privacy and security of their smart home devices?
- What is the relationship, if any, between perception of responsibility, concern, and taking mitigative action?

Forty smart home device consumers participated in the study. They were highly educated with 95% having a BS/BA or MS/MA. There were 22 males and 18 females with the almost half (18) in the 30-39 age category.

Results show that the participants had a mixed level of concern about privacy and security; the mitigations to address their privacy and security concerns were often simplistic; and their perceptions of responsibility for the privacy and security of their smart home devices did not necessarily correspond to their concern level or mitigative actions.

Implemented mitigations included authentication (e.g., setting passwords), limiting audio and video exposure (e.g., turning the camera away from the room); having a secure Wi-Fi; configuring device options; and choosing devices they thought were secure or that protected their privacy.

Participants were uncertain about what information or data was being collected. With regards to privacy, they expressed the desire to be able to control what happens with their data but did not know what, if any, options were available. Their security threat models were often incomplete, they felt they had little or no control over device vulnerabilities, and they lacked the knowledge to implement security mitigations.

To assist consumers, manufacturers can do the following:

- Be transparent – inform the consumer about what data is being collected, when updates are available, and what options are available.
- Provide privacy and security (some) options and include them at installations:
    - Provide opt-in and opt-out options for data collection and usage.
    - Make the device secure by default as much as possible.
    - Include better instructions or wizards to help consumers make informed decisions.
    - Provide granular controls for advanced users.

Other means to assist consumers may be best practice guidance and consumer ratings for device security and privacy to help in the consumer's purchase decisions.

Panel

Keynote speakers (Dr. Camp, Mr. Mathew, Mr. Martens, and Mr. Prostko) fielded audience questions in a panel format. Ms. Haney from NIST moderated. The questions as written below were paraphrased from the originals.

Question: How are considerations for your target population inserted into your company's process for moving a product to market, for example, from idea generation to identification of user requirements to design and testing? For Dr. Camp, what should this process look like?

Allegion tries to solve specific jobs and problems for their consumers. Some products are built for purpose, some are mass market products. They often ask themselves "Is it frivolous or is it fabulous?" when considering what features/functionality to include. Whirlpool focuses on identifying consumer attitudes and needs. Dr. Camp emphasized that there needs to be a process in discovering people's needs and expectations that should be followed as part of any human-centered design process.

There was also a short discussion about how technology can mediate aging in place. For example, a connected teakettle sensor could automatically notify a family member that an elderly person living alone had used and turned off the teakettle (an indicator that all is well) and alleviate the need for the family member to check in every day.

Question: How do you see the product lifecycle changing because of IoT? What about upgrades?

Mr. Mathew stated that Whirlpool's products will be in service for many years. Therefore, they feel they have a duty to keeping improving the product over time. This longevity is in contrast to laptops and cellphones, which consumers expect to upgrade every few years.

However, since it is difficult to predict where technology will be in 10 years, they cannot future-proof a product with a 10-15 year lifespan. Allegion believes that keeping up with the latest in security will be especially challenging, for example, current encryption algorithms may be deemed obsolete in a few years. Hardware lasts much longer than software. Therefore, they see the need for thoughtful, flexible modular design of IoT technology. Modularization allows for modules being able to be swapped out more easily as the technology changes and less in landfills if only some parts need to be replaced.

Dr. Camp provided examples of long-lived technology that has been able to be updated (e.g., Xbox and OnStar). However, Mr. Mathew sees a difference between the ability to do over-the-air updates (as in the case of OnStar) and the ability for the technology to be updated. Mr. Marten agreed, saying that the hardware may have processing or memory limitations, for example, that may preclude being updated with future technology advances. He also said that eventually connected devices will have to be aged out, and manufacturers must ask how long is too long to keep a device in the field.

Question: How do you deal with global and regional privacy regulations?

Mr. Prostko said that Allegion has a program in which they think globally about privacy from the beginning. This includes privacy impact assessments and including GDPR requirements into their design processes. They also carefully choose partners to engage with and consider how much data they can keep locally. To accommodate regional regulations, Allegion has local implementations and adaptations. There is always a balance between functionality and protection. Mr. Mathew said that Whirlpool has connected devices in only a portion of their global markets because they do not want to do local implementations and have a privacy standard that they do not wish to go below.

Question: How can potential physical hazards of IoT be addressed?

Mr. Martens said that, because Allegion views many of their products as life-safety devices, there are some features they are not willing to implement. For example, they do not do auto unlock because it is impossible to know the intent. He also discussed the "If This Then That" (IFTTT) [4] software platform that connects apps, devices, and services from different vendors in order to trigger automations. IFTTT is often used by smart home do-it-yourselfers but can result in "dangerous recipes" when consumers do not fully understand the implementations and potential consequences. For example, an automation might prohibit the connected garage door from opening if a connected fire alarm triggers because of the danger of an inrush of oxygen from the door opening worsening the fire. However, the garage door not opening might pose a safety risk for inhabitants trying to get out of the house.

Mr. Mathew also saw his company's products as having to protect consumer safety. In some cases, consumers must be in physical proximity to an appliance to start it; remote activation may not be possible. For example, with a connected dishwasher, there may be a child entrapment issue, so a consumer must push a physical button to start the dishwasher even though they can configure settings via an app.

Question: What do you expect product developers to do with respect to product security? How do you help the developers?

Allegion sees an inherent value in security because they produce life-safety products. They use open standards, which they feel are more secure than proprietary implementations. They also perform security risk assessments, use various tools to identify potential security issues during development, and do third-party penetration testing. There is always a tension between security and convenience. Mr. Mathew said that product development is more complex today than it was five years ago. Whirlpool has internal and external security teams that perform security quality checks on their products. There is a security person who has the authority to stop the launch of a product if there is a security problem.

Breakout Sessions

As the last activity of the workshop, attendees had the opportunity to choose between two breakout sessions: Smart Home Usability and User Experience and Human Aspects of Smart Home Privacy and Security. During these discussions, attendees were able to voice their thoughts about challenges and solutions facing smart home consumers and provide input to guide NIST's future research direction in this area.

Usability and User Experience

Moderator: Dr. Susanne Furman, NIST

Question: What do you think are the highest priority usability/user experience consumer issues that need to be addressed?

1. Initial setup is too hard – need to connect to WiFi; is the application (app) understandable?
2. Discovering all the features is difficult for consumers.
3. Confusion about what you are controlling – make it clear what your actions are doing.
4. Trust in knowing your information is secure, what you expect is happening, and getting feedback.
5. Users have to be convinced of the usefulness. What is the value proposition?
6. Interoperability - you may have 5 different IoT apps from 5 different manufacturers; need industry standards for interoperability. Users don't want to download another app (too many to manage). How can you integrate all the apps? There may be a need for a control app.
7. Current IoT seems to cater to the nuclear family – the upper middle class. There is a mismatch between functionality and needs that can be exacerbated by socioeconomic status issues or structural issues in society.
8. Accessibility issues – e.g., voice control won't work for deaf person.
9. Changes in how the consumer uses the product - are they using it in a way that is unsafe?

Question: How can we address/solve the challenges?

- Accessibility – can have multi-modal access.
- Need to have device provide feedback that the action was completed. For example, Alexa makes a two-tone confirmatory tone; when lights are glowing and moving in a circle that means Alexa is trying to tell the user something.
- NavCog navigation for people who are blind in buildings - it also provides two-tone feedback after a turn is made (in addition to spoken direction before the turn).
- Price point may be a challenge along with rapidly changing technology and competition between manufacturers – may prevent making a common interface control.

- As generations change, consumers need change – e.g., kids in elementary school do not understand how a regular phone works and what a dial tone is.

Question: What are manufacturers doing right/wrong with respect to usability and user experience?

- Wrong - Monetizing data and owning data
- Wrong - Nobody on the panel mentioned user testing of their devices
- Right - Use of security software libraries – liked that the panelist referred to open standards; they appear to have well-defined/developed software/security lifecycles (don’t get that from immature companies).
- Right - Sophisticated understanding of how long it takes to be successful for a product (around 15 years).

Question: From a research perspective, where do you think we should go from here? What areas need immediate investigation?

- Need usability testing
- Business models – Who owns data and what are they selling? Which class of business model is more user friendly?
- Consumer models of free for information - you provide information and what you want is free. Example – how to make it more like a library which is free.
- Should there be standards?
- Should there be labels about privacy?
- How do we replace end user license agreements (EULAs)?
- Study non-adopters – value proposition – convenience vs. complexity.
- Accessibility features
- Convenience so risk is accepted
- Multi-functionality – fine grained control

Human Aspects of Privacy and Security

Moderator: Julie Haney, NIST

Question: What do you think are the highest priority privacy/security consumer issues that need to be addressed? What more needs to be done?

- Little information sharing about security vulnerabilities- security might be better if companies shared more and worked together
- Consumers often say they want transparency
- Smart home device updates - transparency
    - Manufacturers should notify consumers of vulnerabilities instead of hiding or minimizing their existence
    - Manufacturers use term software, not security, update - consumers may think updates are just adding new features or fixing generic bugs; may not realize the importance from a security perspective
    - NIST smart home user study - participants rarely talked about updates in the context of security

  - Consumers may have had negative experiences with updates breaking some functionality, so they might be hesitant to apply them
  - If manufacturers were to be transparent about the reasons for an update and security fixes issued too often, consumers might lose trust in the product

Question: What type of privacy and security information do consumers need or want? What is the best way to communicate this information?

- Consumers should be given pertinent privacy and security information
- Some users may not understand or be overwhelmed with privacy and security information if too much is provided or at too technical a level – for example, EULAs
- Manufacturers may face a tradeoff between keeping customers and helping them make informed security/privacy decisions
- Consumers should not just be provided information that scares them; should also be given actionable guidance they can follow
- Accommodating consumers with different risk profiles can be difficult - for example, an attendee analogized different consumer risk profiles with traveling risks at her institution. There is a distinct risk difference between bringing a work laptop to China versus traveling with it within the continental United States.

Question: How do consumers transfer their knowledge about security/privacy of traditional information technology devices to IoT devices, if at all?

- Many consumers are less concerned about security/privacy with IoT devices - perhaps because they are less aware of how the devices work
- Security awareness training in organizations should include IoT, too.
- Consent is meaningless if people don't understand to what they are consenting
- With IoT smart home devices, consent may apply to the consumer that buys them but not those who may also be impacted by the devices
  - Example - a consumer may have a voice-controlled assistant in their home. However, when visitors enter the home, they may not be aware of the existence of the device. This situation may cause issues if the visitor has privacy concerns about these kinds of devices.
  - One attendee witnessed negotiations about turning these devices off when someone visited a home and became aware of a voice assistant.

Question: What do you think are the potential advantages and disadvantages of having consumer rating systems/symbols/labels for smart home privacy and security?

- Ratings system would be difficult without standard evaluation criteria in place
- Consumers need an accurate threat model for the label to be meaningful
- Consumers need to understand the consequences of security or privacy functionality not being implemented, but they usually don't – example - people are familiar with what can happen if there is a small child in the backseat of a car during an accident, but they may not know the consequences of IoT devices being hacked

Question: A speaker expressed the opinion that consumers will just have to accept the fact that IoT devices are becoming ubiquitous. It appears that users are resigned to accepting privacy and security risk if they purchase IoT. Is there a way to change this?

- A speaker said that power is shifting more to the consumer, but it seems like consumers do not seem empowered when it comes to privacy and security.
- Short lifespan of IoT devices hints at planned obsolescence
- It might come to a point where consumers may not be able to buy a device (like an appliance) without a "smart" capability. However, the consumer may not be equipped to safely take advantage of it.
- Many smart home consumers think their devices have AI. But do they really understand what it means to be "smart" and how not all smart home use AI?
- An issue with systems that use AI is that people have unrealistic expectations of what the systems can do. If their expectations are not met, they may go in the completely opposite direction (distrust of manufacturer, lack of adoption).
- Users need to be ready and able to jump in if the smart technology or AI fails or is hacked – analogy of the potential need for user intervention in a self-driving car.
- Wildly diverging industries can maybe now call themselves tech companies if they enable some kind of "smart" feature on their products
  - Protecting the security and privacy of these "things" may be challenging for those just entering into this space.
  - There is a need for standards and clear definitions to help these industries.

Question: From a research perspective, where do you think we should go from here? What areas need immediate investigation?

The following are potential research questions derived from the discussion of the framing questions.

- What is the best balance between privacy/security transparency and consumer trust? Is transparency beneficial or detrimental to consumer trust in this product space?
- How do manufacturers decide what privacy/security information to provide to consumers? What kind of information would be most beneficial to consumers?
- How would consumer ratings for smart home privacy/security affect purchase decisions, if at all? What information should the ratings convey?
- How do device manufacturers view responsibility for security/privacy? How much responsibility do they think belongs to them? How much do they think is that of the consumers?
- How can consumers be more empowered with respect to their smart home privacy and security?

Feedback and Additional Information

NIST is committed to maintaining an open dialogue. The community is encouraged to participate in this topic area by providing feedback, sharing insights, and emailing questions to susanne.furman@nist.gov or julie.haney@nist.gov. Presentation slides and the workshop agenda are available on the NIST Usable Cybersecurity Workshops web page.

References

[1] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", 2019, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] M. Fagan, K. Megas, K. Scarfone, and M. Smith, NIST IR 8259, "Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers," July 2019, https://csrc.nist.gov/publications/detail/nistir/8259/draft

[3] D. Dodson, W. Polk, M. Souppaya, et al., NIST Special Publication 1800-15, "Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)," April 2019, https://csrc.nist.gov/publications/detail/sp/1800-15/draft

[4] IFTTT, 2019, https://ifttt.com/