Privacy Notice in IoT Homes

Christine Geeng
Cornell University
Ithaca, Ithaca 14850, USA
cg447@cornell.edu

Abstract

An artifact building on existing home conventions can provide notice and consent for guests who otherwise may remain unaware of surveillance practices when entering an Internet-of-Things connected house.

Author Keywords

Agency; privacy; domestic; home; Internet of Things.

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Background

The technology for Internet-connected tools has become remarkably more reliable and cheap, leading to a proliferation of ubiquitous computing spaces. There are now many Internet-of-Things (IoT) tools and sensors available for home use, from toasters to HVAC controls (heating, ventilation, and air conditioning) [4]. However, privacy controls for information flow have not adapted quite as fast. The dominant method currently used to address information flow is notice and consent, where services will have the user read and then decide whether to agree to their privacy terms, allowing them to use the product [7]. Notice and consent has its limitations, such as a dependency on a visual interface for the user to see the terms and conditions, and also a tendency for users to skip reading the text entirely.

On top of these weaknesses, the notice and consent system has other issues in context of IoT tools in the home. Many home IoT products, such as security cameras, toys, and humidity sensors, have little screen real estate for long privacy agreements. While this issue can be addressed by displaying the notice on a phone connected to the product, this only solves the issue for the primary user who first uses it, ignoring other household members and guests. Given the newness of wifi-connected sensors in the house, cultural norms do not address notice and consent for guests at all. Stepping into someone's house is tantamount to relinquishing control over one's information recorded inside.

While the knowledge of surveillance can put strain on social interaction and communication in ubiquitous computing environments [6], it is necessary to ensure that people within these environments have a good understanding of what happens to data collected from them. This is important for two reasons. First, most IoT manufacturers do not have as much cybersecurity experience as traditional software companies, making IoT hardware extremely vulnerable to hackers, which can pose physical dangers [4]. Second, data collection can be harmful even if the surveilled "have nothing to hide" [10]. For example, home security footage could be exploited for use outside of checking for wrongdoing. Two guests were shocked to find a home security camera in an Airbnb home they rented, where they had discussed personal matters, among them finances [2]. Surveillance in a home produces power imbalances between the homeowner and the people who visit.

Point of Debate

How can IoT homes accommodate data control for guests while balancing functional goals and social ties?

Notice and Consent for House Guests

There is typical protocol in western society for guests when they enter the host's home: wipe your shoes on the mat, put your coat in the closet, and more recently ask for the wifi password (if you know the host well enough). However, there is no strict social protocols for how hosts and guests deal with home security, making the negotiation of surveillance awareness and data control a precarious situation. While webcams typically have notice and consent for primary users, people who purchase the product, there isn't a system in place that provides notice to "incidental users, such as bystanders, who may not even be aware that information about them is collected by a system" [9], e.g. house guests. Their awareness requires either spotting the camera themselves or someone telling them of it.

The aim of this artifact is to build on existing norms for house guests to make incidental users aware of home data collection practices. Awareness of these home security systems is necessary for guests to have more control over how, where, and when data about them is being collected, as they can directly intervene with the host.

This artifact mimics a welcome mat, a traditional item placed at the threshold of a house. This can be placed by the homeowner at the front door. When the guest steps on it, it triggers a pressure sensor that pulls up information on data collection occurring in the home on a screen near the entrance.

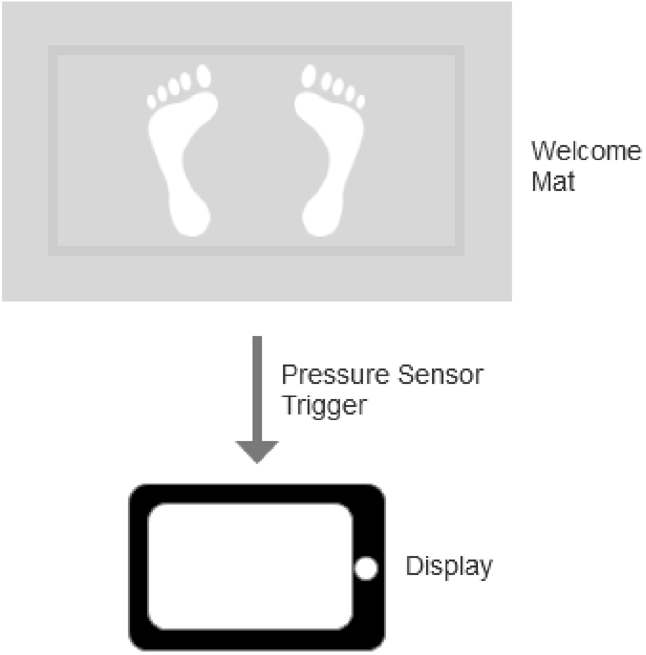

Figure 1: Pressure sensors activated in the welcome mat will trigger the screen display to pull up data collection information in the home.

It displays the IoT products in the house that the owner selects to appear, and also displays details about what kind of data is being collected and how it is being stored. With this awareness, guests have the opportunity to ask the host to change data collection settings, despite not being the primary user.

However, the design of this artifact ultimately leaves the control of whether or not the guest becomes aware of the security camera, and therefore control over data collection, firmly with the homeowner. Making people aware of the security camera's existence can be counterproductive to the main product goal of keeping the room safe, as knowledge of the camera can lead to circumvention. The host who puts out the welcome mat will have to weigh these values of their guests' privacy versus potential security.

Also, having an explicit form of consent raises the issue of not having plausible deniability. Under federal law in the United States, 18 U.S.C. § 2511(2)(d), it is legal for conversations to be recorded as long as one party in the conversation has consented. In some states, such as California, the state law requires two-party consent for a conversation to be legally recorded. Showing explicit consent even though the secondary party may not fully understand the implications may remove future possibility of legal recourse.

Conclusion

This artifact generates notice for house guests about security cameras and other devices in the home. While the notice and consent framework has many issues with appropriately informing users of privacy policies and data collection, it does provide a basis for giving data control to incidental users. Making guests aware that data is being collected from them is a small step towards balancing the power dynamics between the host and other users in a domestic space that surveils audio and visual data.

Author

Christine Geeng is a tinkerer and researcher interested in exploring alternative modes of privacy feedback in the age of ubiquitous computing. She is currently a graduate student in Information Science at Cornell University.

References

1. Bellotti, V., & Sellen, A. 1993. Design for Privacy in Ubiquitous Computing Environments*. Proceedings of the Third European Conference on Computer-Supported Cooperative Work* 13–17 September 1993, Milan, Italy ECSCW '93, 77-92. doi:10.1007/978-94-011-2094-4_6
2. Brandom, R. "A woman is suing Airbnb over an alleged hidden camera." 2015. Retrieved February 1, 2017 from http://www.theverge.com/2015/12/16/10318300/airbnb-hidden-camera-lawsuit-california.
3. Calo, Ryan. Against Notice Skepticism in Privacy. 2011.
4. Hong, Jason. "Toward a Safe and Secure Internet of Things." 2016. Retrieved January 2, 2017 from http://www.cmuchimps.org/uploads/publication/paper/177/toward_a_safe_and_secure_internet_of_things.pdf
5. Hsieh, G., Tang, K. P., Low, W. Y., & Hong, J. I. (n.d.). 2007. Field Deployment of IMBuddy: A Study of Privacy Control and Feedback Mechanisms for Contextual IM. *UbiComp 2007: Ubiquitous Computing Lecture Notes in Computer Science*, 91-108. doi:10.1007/978-3-540-74853-3_6
6. Mancini, Clara, et al. 2011. "In the Best Families: Tracking and Relationships." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2419-2428. ACM, 2011.
7. Nissenbaum, Helen. 2011. "A Contextual Approach to Privacy Online." *Daedalus* 140, no. 4 (2011): 32-48.
8. Palen, L., & Dourish, P. 2003. Unpacking "privacy" for a networked world. *Proceedings of the conference on Human factors in computing systems - CHI '03*. doi:10.1145/642633.642635
9. Schaub, F., Balebak, R., Durity A. L., & Cranor, L.F. 2015. *Symposium on Usable Privacy and Security (July 2015).*
10. Solove, Daniel J. 2011. "Why Privacy Matters Even if You Have 'Nothing to Hide.'" *The Chronicle* (May 15, 2011).