**IoT privacy:**

Brush et al [11] identified the barriers that stop the IoT devices at home from being widespread. These barriers include shoddy management systems and security concerns. Other researchers, such as Randall [12] found that control systems can be so complicated that the end-user sensed that they have less control over their devices. Page et al [13] found that IoT devices that are designed for the consumers tend to follow an agentic technology viewpoint, where the user-centric viewpoint takes a backseat.  
  
He et al. discussed how sharing of IoT devices inside a home occurs among relationships and how they differ based on time of the day, scenarios, location of the device, etc. They also discussed ways to authenticate users so that the IoT devices stay secure while upholding the usability of the device[1]. This work, however, does not discuss sharing IoT devices with people living outside of their homes. Researchers find that giving guests access to your IoT device in a smart home [21] and being specific with policies regarding the shared devices [22] is important but can be a complex task.

**Smart home access control:**Researchers [27] have shown that the cost of hardware is not an issue when implementing security and privacy for IoT devices. Denning et al. [9] discussed how rushing to release IoT devices to market is causing those devices to have security and privacy issues for the end-users. These issues include being eavesdropped, losing control of the devices in question, loss of private data, etc. Fernandes et al. show in their paper [2] that apps (SmartThings by Samsung) controlling the IoT devices can have more access than necessary, making the devices insecure. It can be exploited to steal key security information (i.e Door lock codes), disable some security features and even make false fire alarm. Another research [25] shows that apps can accumulate additional and unnecessary access just by asking users for more permissions. Felt et al.[26] shows that users tend not to pay much heed to these requests. Fernandes et al. along with others [3][4] have proposed limiting and reconsidering permission granted to those apps to solve this problem.

Kim et al. interviewed 20 people who do not yet use smart home devices to understand the user’s need for proper access control policies [18] [19]. According to these interviewees, the capability of requesting permissions to be approved or denied, proper logging of devices and physical presence are useful criteria for a well designed access-control policy. In a separate research paper [20], researchers found that access-control policies based on time ( blocking children from watching TV at night), special preventive measures for highly sensitive devices like cameras and locks, limiting of application’s access to devices is also highly desirable among users. An empirical study on 15 families done by Brush et al.[24] reveals that family members trust each other while keeping separate profiles on IoT devices. They do this to impede the teenagers of the house from using the PC or to block strangers with malicious intent.  
  
Ur et al. [14] found that the access control system of popular IoT devices like the Kwikset door lock and Philips Hue lighting system is so isolated that it is useless in simple use cases where the user wants to share the devices with other users like temporary works and children. If the user is away from home the access control of the home IoT devices can be challenging as it has to be trustworthy enough to operate on their own [15].

**Community-based privacy(privacy beyond the individual):**

Mazurek et al. [16] discussed that even if the IoT system is designed to share in between users, the kind of access control it has is very much different from the kind of access control the user has in his/her mind. They also show that most of the time the user needs a complex access control policy and they try to achieve that by using makeshift methods. For domestic IoT devices, the access control decisions are especially complex because of the varied amount of data and the kind of trust users have between themselves[8]. Brush et al. [17] found that even when sharing IoT devices and sensors among neighbors can help increase the security of the neighborhood, the level of trust they have between themselves can interfere with this sharing.

Few research studies [5][6] show that the multi-user scenario can be perceived as a privacy and security concern to users. This concern exists because of the social relationships between the users and they can vary depending on the relationships such as guests [7], roommates [8], and children [9][10]. Moncrieff et al. [23] find that providing users the information about the data being monitored by the sensors in a smart-home setting can help pacify the privacy concern they have but at the same time it is perceived as being burdensome. Kostianinen et al. [22], tried to introduce an access control policy for smart home networks limited to family members which would pose a nominal amount of burden on the end-user by testing a few access control policies.

1. F W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). 255–272.
2. FERNANDES, E., JUNG, J., AND PRAKASH, A. Security Analysis of Emerging Smart Home Applications. In Proc. IEEE SP (2016).
3. JIA, Y. J., CHEN, Q. A., WANG, S., RAHMATI, A., FERNANDES, E., MAO, Z. M., AND PRAKASH, A. ContexloT: Towards Providing Contextual Integrity to Appified IoT Platforms. In Proc. NDSS (2017).
4. TIAN, Y., ZHANG, N., LIN, Y.-H., WANG, X., UR, B., GUO, X., AND TAGUE, P. SmartAuth: User-Centered Authorization for the Internet of Things. In Proc. USENIX Security Symposium (2017).
5. NAEINI, P. E., BHAGAVATULA, S., HABIB, H., DEGELING, M., BAUER, L., CRANOR, L. F., AND SADEH, N. Privacy Expectations and Preferences in an IoT World. In Proc. SOUPS (2017).
6. ZENG, E., MARE, S., AND ROESNER, F. End User Security and Privacy Concerns with Smart Homes. In Proc. SOUPS (2017)
7. JOHNSON, M., AND STAJANO, F. Usability of Security Management: Defining the Permissions of Guests. In Proc. SPW (2006).
8. LEKAKIS, V., BASAGALAR, Y., AND KELEHER, P. Don’t Trust Your Roommate or Access Control and Replication Protocols in “Home” Environments. In Proc. HotStorage (2012).
9. T. Denning, T. Kohno, and H. M. Levy, “Computer security and the modern home,”Commun. ACM, vol. 56, no. 1, pp. 94–103, Jan. 2013.[Online]. Available: http://doi.acm.org/10.1145/2398356.2398377
10. SCHECHTER, S. The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button! In Proc. HUPS (2013).
11. A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home Automation in the Wild: Challenges and Opportunities. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’11), 2115–2124. https://doi.org/10.1145/1978942.1979249
12. Randall, D. Living Inside a Smart Home: A Case Study. In: Harper, R. (ed.) Inside the Smart Home, 227-246. Springer, Heidelberg (2003)
13. Page. X., Bahirat, P., Safi, M.I., Knijnenburg, B.P., Wisniewski, P. (2018) “’The Internet of What?’ Understanding Differences in Perceptions and Adoption for the Internet of Things,” Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), Issue 4.
14. B. Ur, J. Jung, and S. Schechter, “The current state of access control for smart devices in homes,” inWorkshop on Home Usable Privacy and Security (HUPS). HUPS 2014, July 2013. [Online]. Available:<http://research.microsoft.com/apps/pubs/default.aspx?id=204947>
15. W. K. Edwards and R. E. Grinter. At home with ubiquitous computing: seven challenges. In Proc. UbiComp, pages 256–272, 2001.
16. M. L. Mazurek, J. P. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. F. Cranor, G. R. Ganger, and M. K. Reiter. Access control for home data sharing: Attitudes, needs and practices. In Proc. CHI, pages 645–654, 2010.
17. A. B. Brush, J. Jung, R. Mahajan, and F. Martinez. Digital neighborhood watch: investigating the sharing of camera data amongst neighbors. In Proc. CSCW, pages 693–700, 2013.
18. T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Challenges in access right assignment for secure home networks. In Proc. HotSec, 2010.
19. T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Access right assignment mechanisms for secure home networks. Journal of Communications and Networks, 13(2):175–186, April 2011.
20. C. Dixon, R. Mahajan, S. Agarwal, A. J. Brush, B. Lee, S. Saroiu, and P. Bahl. An operating system for the home. In Proc. NSDI, 2012.
21. M. Johnson and F. Stajano. Usability of security management: Defining the permissions of guests. In Proc. Security Protocols Workshop, 2006.
22. K. Kostiainen, O. Rantapuska, S. Moloney, V. Roto, U. Holmström, and K. Karvonen. Usable access control inside home networks. Technical Report NRC-TR-2007-009, Nokia Research Center, April 2007.
23. S. Moncrieff, S. Venkatesh, and G. West. Privacy and the access of information in a smart house environment. In Proc. MM, pages 671–680, 2007.
24. BRUSH, A. J. B., AND INKPEN, K. M. Yours, Mine and Ours? Sharing and Use of Technology in Domestic Environments. In Proceedings of Ubicomp (2007)
25. ENCK, W., ONGTANG, M., AND McDANIEL, P. Understanding Android Security.IEEE Security & Privacy 7, 1 (2009), 50–57.
26. FELT, A. P., HA, E., EGELMAN, S., HANEY, A., CHIN, E., AND WAGNER, D. Android Permissions: User Attention, Com-prehension, and Behavior. InProc. SOUPS(2012).
27. B. Pearson, L. Luo, Y. Zhang, R. Dey, Z. Ling, M. Bassiouni, and X. Fu, ‘‘On misconception of hardware and cost in IoT security and privacy,’’ in Proc. IEEE Int. Conf. Commun. (ICC), May 2019, pp. 1–7.