In recent years, a massive number of devices have emerged with the capability to connect to the Internet, thereby providing users with unprecedented benefits. These Internet of Things (IoT) devices are increasingly used to improve energy efficiency, home security, and convenience, and by 2025, it is estimated to have an installed base of 75 billion IoT devices throughout the world. The cybersecurity threats of these devices, however, are not as appealing as their benefits. Baby monitors get hacked, Amazon Echo devices send private conversations to others, and Samsung Smart TVs start recording without users’ knowledge. One explanation for these overwhelmingly challenging risks of IoT devices could be overlooking privacy and security early on in the product life cycle due to lack of resources (e.g., expertise, money). Integrating privacy and security safeguards into IoT devices could reduce their risks or mitigate their potential harms. At the same time, IoT manufacturers are not transparent about their privacy and security practices, leaving consumers with little information when purchasing IoT devices. This lack of information at the time of purchase could result in people bringing home a vulnerable device and easily scaling up the threat by connecting the device to their home network.

Thanks to privacy and security experts and media reports, people are becoming aware of the threats of smart devices. However, despite growing concerns about the privacy and security of IoT devices, people have difficulty specifying their privacy and security preferences and considering them when making IoT-related purchase decisions. To enable informed decision making during the purchase process of IoT devices, we need to understand how people feel about the privacy and security implications of these devices. Moreover, effective ways of communicating important privacy and security factors to consumers of IoT devices need to be carefully studied.

In this thesis, we first explore the factors influencing users’ privacy concerns and preferences toward data collection of smart devices. To this end, we quantify users’ privacy preferences and expectations with the aim of statistically modeling privacy-related attitudes and reported behaviors by factors such as the collected data, the purpose of data collection, and the retention time. In a 1,007-participant online study, we found that participants are significantly more comfortable when seemingly innocuous information such as the room’s temperature or their presence is being collected, as compared to when more sensitive information like their biometrics (e.g., fingerprints) are being collected. In addition, participants are significantly more willing to allow data collection in a public space (e.g., library) than a private location (e.g., at home).

Next, we explore how users’ IoT-related privacy decision making would be influenced when receiving social cues from privacy experts and friends. We found that both friends and privacy experts significantly impact participants’ privacy-related decision making. Following our overarching goal to inform privacy-related decision making, we delve into designing a label to effectively inform consumers about the privacy and security practices of smart devices at the time of purchase. To achieve this, we first interviewed 24 IoT consumers on the factors they consider when purchasing smart devices and found that currently, seeking understandable privacy and security information for smart devices is difficult or impossible. This finding motivated us to seek an effective mechanism to inform consumers by better communicating this information at the point of sale. We proposed creating a usable privacy and security nutrition label for IoT practices, building on prior projects that have used nutrition labels in other privacy contexts. To explore the actual content of such a label, we conducted a study with experts from diverse domains and identified 47 privacy and security attributes to include on a two-layer label. Finally, we evaluated the efficacy of attribute-value pairs presented on the label in conveying risk to consumers as well as its effect on their willingness to purchase the smart device. Our results show that data privacy and security information is more powerful in swaying consumers’ risk perception than changing their willingness to purchase.

Committee: Dr. Yuvaraj Agarwal (Co-Chair), Dr. Lorrie Faith Cranor (Co-Chair), Dr. Lujo Bauer, Dr. Mohammad Reza Haghhighat (Intel Corporation)