Privacy and security concerns are growing rapidly as a result of ubiquitous data collections by IoT devices. One way to alleviate such concerns is to design privacy assistants that can provide users with transparency around these pervasive data collections so that they can gain some level of control over their data. Building such privacy assistants requires a thorough understanding of people’s privacy-related preferences and concerns toward IoT data collection.

In this thesis, I will first focus on exploring how users’ comfort with data collection and their desire to allow or deny data collection can be explained by privacy factors such as data type or the purpose of data collection. I will then discuss how social influence from privacy experts and friends can influence people’s privacy-related decisions toward allowing or denying IoT data collection. Next, I will study the impact of privacy and security on consumers’ IoT-related purchase behaviors. More specifically, I will explore how consumers would want to be presented with information related to privacy and security for IoT devices while making their purchase decisions.

Currently, finding privacy and security information for IoT devices at the time of purchase is very difficult for consumers, if not impossible. Due to the unavailability of such information at purchase time, consumers may overlook the importance of privacy and security information, hence exposing themselves to a great number of risks and vulnerabilities. Drawing on prior work and results from my previous studies, I propose to develop prototype privacy and security labels for IoT devices and evaluate their usability as well as their effectiveness by conducting user and expert studies. Finally, I plan to explore how much information related to privacy and security as well as user behavior can be extracted from the IoT network data.