Although technologies such as mobile apps, web browsers, social networking sites, and IoT devices provide sophisticated services to users, they are also increasingly collecting privacy-sensitive data about them. In some domains, such as mobile apps, this trend has resulted in an increase in the breadth of privacy settings made available to users. These settings are necessary because not all users feel comfortable having their data collected by some of these technologies. On mobile phones alone, the sheer number of apps users download is staggering. The same is true in other domains as well, such as social networks, browsers, and various IoT technologies. The result of this situation is that users feel overwhelmed by all of the settings available to them, and are thus unable to effectively take advantage of them.

This dissertation examines whether machine learning techniques can be utilized to help users manage an increasingly large number of privacy settings. It specifically focuses on mobile app permissions. The research presented herein aims to simplify people’s tasks in regard to managing their massive amount of app privacy settings. We presented our methods of learning models of users’ privacy preferences and designed an interactive assistant for users to configure their settings with the help of personalized recommendations. The objective of this work is to alleviate the burden placed on users while increasing alignment between a user’s preferences and his or her settings.

This thesis details three different studies. Specifically, in the first study, we used a dataset of mobile app permission settings obtained from over 200K Android users, explored different machine learning models, and analyzed different combinations of features to predict users’ mobile app permission settings. The results suggest that a relatively small number of privacy profiles derived from clusters of like-minded users can help predict many of the permission settings that users in a given cluster prefer. The second study was designed to validate these findings in a field study with actual users. We designed an enhanced version of Android permission manager and collect rich information of users’ actual app permission settings. Results of this study confirm that a relatively small number of profiles (or clusters of users) can capture users’ diverse privacy preferences and predict their privacy settings. They also indicate that privacy nudges can be very effective at motivating users to engage with their permission settings and deriving privacy profiles with strong predictive power. In the third study, we evaluated our profile-based preference models by developing a privacy assistant that helps users configure their app permission settings based on the developed profiles from our second study. We report on the results of a pilot study (N=72) conducted with actual Android users using our privacy assistant on their smartphones while performing their regular daily activities. The results indicate that participants accepted 78.7% of the recommendations made by the privacy assistant and kept 94.9% of these settings on their phones over the following six days, all while receiving daily nudges designed to motivate them to further review their settings. The dissertation also discusses the privacy profiles designed for this research and identifies essential attributes that separate people associated with different profiles (or clusters). The app has been refined and was released to the Google Play store for future explorations and research.