In the past two decades, technology advancements have pushed social platforms from their online versions to mobile counterparts. This migration allowed platforms to provide users with many attractive ‘on-the-go’ services like posting current location, searching for deals and events nearby and completing tasks and surveys for incentives. Most users do not realize the personal information they are giving away while using these platforms. Notably, a user’s location is necessary for most of these services and a privacy breach would lead to the disclosure of sensitive location information. This may lead to attacks like tracking and profiling. In most social platforms, user privacy is given less priority as applying any privacy would drastically reduce the quality of services provided.

My research focuses on developing user-centric privacy mechanisms to provide enough privacy as per user needs but still retain enough information to provide quality service. To accomplish this, we identify user interaction patterns and group them. In each group, we identify features that require more privacy and conceal them by using techniques like generalization and obfuscation. Our results show that these techniques can be successfully implemented on different social platforms, with just the right amount of information loss that a service can tolerate. Focusing on user privacy is critical and will benefit both parties, with users being able to take advantage of services and the social platforms obtaining more revenue with users not exiting the platform fearing information disclosure.