Personal data is considered an important commodity in the market for online services (e.g., mobile apps, Amazon, Facebook). These services typically collect massive amounts of user data. On one hand, this data can be used as an advantage for better personalization of users, better understanding of trends from aggregated data, etc. On the other hand, the data provides an essential monetization opportunity to online services, i.e., by selling data to ad-networks and third party data brokers, the services can make revenues and generate profits. However, the research community has raised various privacy concerns in the current market for online services. As a result, considerable research efforts are currently centered on developing tools and techniques to detect and resolve privacy threats in order to protect users of online services. These solutions are collectively called privacy enhancing technologies (PETs), e.g., Differential Privacy, and are based on the principle of data disclosure minimization.

Although the technical concept of data disclosure minimization is an important one with respect to resolving privacy threats, the problem of privacy improvement in online service markets is a multi-dimensional one, i.e., apart from providing solutions on the technical plane alone, efforts should be targeted at resolving privacy related issues on the social, behavioral, economic, and policy planes. Therefore, in spite of technical improvements via PETs, it is unlikely that we will be able to achieve a robust privacy guarantee for end-users in the online services market. In such a scenario, the need of the hour is to design alternative methods of privacy preservation. In this context, various recent research efforts have proposed the idea of incentives: charging or benefiting various entities in data markets to promote environments for robust privacy guarantees. Solution concepts using incentives have the potential to align with economic requirements of the primary entities affecting privacy, viz. online service providers, policy makers, application users, and third parties (ad networks and data brokers). However, despite initial hopes, incentive mechanisms are not widely adopted by the industry to protect user privacy. On the contrary there are incentives for users to leak private information - mainly to generate more revenue for the non-end users in the services market. We are driven by the following important question: can incentives induce privacy preserving online services markets (OSMs)? Proper implementation of incentive mechanisms can help provide mobile application ecosystems more privacy guarantees, with profound benefits to all entities – individuals, applications’ owners, ad-networks etc. In addition, by providing an accountable incentive model that is tightly coupled with privacy concerns and guarantees, and nudging users to make privacy friendly choices with the help of proper incentives, our efforts can provide a two fold solution to the industry, (1) on one hand they can help users to make informed decisions about data exchange, and (2) they can provide economic stability to applications and services.