A Framework for Protecting Worker Location Privacy in Spatial Crowdsourcing

*Spatial Crowdsourcing (SC)* is a novel and transformative platform that engages individuals, groups and communities in the act of collecting, analyzing, and disseminating environmental, social and other spatio-temporal information. This new paradigm for data collection can reduce costs significantly, and is particularly useful in the case of disaster response or censorship, when traditional means fail. The objective of SC is to outsource a set of spatio-temporal tasks to a set of *workers*, i.e., individuals with mobile devices that perform the tasks by physically traveling to specified locations of interest. SC is gaining a lot of traction in scenarios such as participatory sensing (e.g., environmental monitoring) and news media. However, current solutions require the workers, who in many cases are simply volunteering for a cause, to disclose their locations to untrustworthy entities. An adversary with access to individual whereabouts can infer sensitive information about a person, such as political and religious views, alternative lifestyles, etc. In this study, we introduce a framework and develop a prototype system, namely PriGeoCrowd, for protecting location privacy of workers participating in SC tasks. PriGeoCrowd allows the cell service providers to release their customers' location data with a specified privacy level, mutually agreed upon with their customers. Thereafter, multiple SC companies can use the sanitized data to provide spatial crowdsourcing services. We argue that existing location privacy techniques are not sufficient for SC, and we propose a mechanism based on differential privacy and geocasting that achieves effective SC services while offering privacy guarantees to workers. We investigate analytical models and task assignment strategies that balance multiple crucial aspects of SC functionality, such as task completion rate, worker travel distance and system overhead. Extensive experimental results on real-world datasets show that the proposed technique protects workers' location privacy without incurring significant performance metrics penalties.