‘Slide to Unlock?’ – Mobile convergence and collapsing contexts

Samir Passi
Royal Netherlands Academy of Arts and Science (KNAW)

Abstract:

This presentation will highlight privacy issues raised by increasing access to social networks made possible by various mobile applications. I will focus on the unintended consequences of the ability of third-party apps to interact not only with the online databases and services of social networks but also with a user’s personal data within the mobile device itself. The content of the presentation is based on the review work that I am currently doing for the EINS JRA 5.1.1 deliverable (Analysis of Privacy, Reputation, and Trust in Social Networks) and relates to the disciplines of Science and Technology Studies (STS) and Information and Communication Technology (ICT).

Online social networks – which primarily started out as web services – have now evolved into social platforms that not only serve individual users but also offer developers the means to interact with the platform. Social networks such as Facebook, Foursquare, and Google+ provide programming interfaces that developers can use to build applications that can interface and interact with the platform’s data and services. Depending upon the nature of the network, these third-party applications can then generate novel means to catalogue, classify, and correlate information pertaining to the entire user base of multiple social platforms. A famous example is the TweetDeck application that allows its users to simultaneously interact with Facebook and Twitter.

With the widespread diffusion of smartphones and tablets, such ability for novel and large-scale convergence of social information has implications for the sociology of user expectations concerning user information privacy. Through their mobile variants, these applications can scan a user’s contacts, messages, mobile photos, and location in addition to information from various social platforms. This sometimes leads to situations where the ability of these apps to ‘use’ the gathered data has unintended consequences. An oft-cited example of this was ‘Girls around me’. Through this app, a person could search around his/her location for nearby girls. The app took public data from Foursquare and coupled it with the public images of girls on Facebook to provide the user with an interactive map displaying a comprehensive visualization of information pertaining to girls around his/her location. Although the app was subsequently taken down, the example clearly depicts how third-party social applications can have consequences for societal notions of privacy and trust by facilitating novel means of large-scale tagging, identifying, and converging not only online information but also the exact locations of mobile users.

An in-depth understanding of public and private contexts in relation to characteristics particular to the mobile medium provides a relevant point of entry to examine such privacy and trust issues. Although Facebook photos and Foursquare check-ins might have separately been made public by certain users, the combination of the two coupled with an exact location on the map is certainly not what these girls explicitly consented to. By identifying and merging particular bits of scattered information, apps such as ‘Girls around me’ facilitate the collapsing of public and private contexts and pose a substantial threat not only to an individual’s privacy and personal security but also to socially acceptable forms of data mining.

Moreover, although such apps can be regulated on standardized app-stores provided by Google or Apple, the ease of working with social and mobile platforms makes it increasingly difficult to manage and govern the intentionality of the large number of mobile apps that are developed each day. Social networks and mobile devices have now become ubiquitous tools that are used by individuals to manage their everyday lives and mobile app development has become a substantial market in itself. In such a scenario, it is imperative to examine the implications of the ability of third-party applications to facilitate the large scale convergence of user information in ways that are quite novel and non-traditional. In a time when ‘privacy as contextual integrity’ and ‘privacy by design’ are issues that are featured prominently on the societal agenda, this presentation will provide insights into questions such as what contextual integrity translates to for the increasingly ubiquitous mobile medium or what must we know before we start designing privacy into mobile apps and social platforms?

Author Biography:

I work as a research assistant at the eHumanities group in the Royal Netherlands Academy of Arts and Science (KNAW). Along with Sally Wyatt, I am currently working on the EU project titled Excellence in InterNet Science (EINS). As part of this project, my work involves researching the social shaping of the notions of privacy and trust in relation to social media technologies as well as analyzing how various online technologies manage user expectations regarding the privacy of their data.

My academic and research experiences stem from the disciplines of Science and Technology Studies and Information Technology. I completed my research masters in ´Cultures of Arts, Science and Technology´ (CAST) at Maastricht University, The Netherlands. At an undergraduate level, I have been trained as an Information and Communication Technology (ICT) engineer at Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT), India.