Chapter 57
Trapped in My Mobility:
How a Principle of "Control over Communicative Interaction" Can Guide Privacy by Design in Mobile Ecosystems

Lemi Baruh
Koç University, Turkey

Mihaela Popescu
California State University, USA

ABSTRACT

In the wake of the quick penetration of mobile devices into the everyday lives of individuals, protection of privacy in mobile ecosystems has become a hot button issue. Existing regulatory efforts on mobile privacy primarily focus on protection of the informational privacy of individuals. While necessary, focusing solely on informational privacy may not be sufficient in terms of protecting users' privacy in mobile environments. The chapter discusses the privacy implications of design architectures and economic arrangements in the mobile ecosystems and argues that mobile environments create privacy-threatening "sticky" relationships that make it increasingly difficult for individuals not only to control flow of information about themselves, but also flow of communication that targets them. This chapter argues that an important supplement to protecting users' privacy is to restore users' control over the communicative interaction with the companies seeking to target them. To that purpose, the chapter offers a set of principles, called "home mode" for mobile privacy, in implementing remedies for threats to privacy in mobile environments.

INTRODUCTION

As consumers increasingly gravitate toward mobile technologies to fulfill many of their primary computing needs, marketers tout mobile ecologies for their ability to increase consumer convenience and market efficiency by delivering the most relevant messages at the right time and place to the right people. However, the rhetoric of convenience and efficiency that now legitimates the seamless integration of advertising delivery into users' mobile experience often clouds the

DOI: 10.4018/978-1-4666-8111-8.ch057

underlying system of ubiquitous data collection made all the more pernicious by the fact that a majority of users are unaware of its extent (Turow et al., 2007).

In 2012, both the Federal Trade Commission (FTC) in the United States and the European Parliament introduced new privacy frameworks meant to address the privacy challenges posed by social media and other large data-collection platforms delivered through online and mobile technologies. In the U.S., the FTC issued a long-awaited list of recommendations for better online and mobile privacy practices in the marketplace (FTC, 2012). Similarly, the European Parliament formulated a proposed amendment to its General Data Protection Regulation meant to inform the privacy legislation of the individual Member States by outlining principles for better control over commercial data sharing and collection (European Commission, 2012). Despite their differences of scope (the FTC privacy framework is a template for privacy self-regulation, while the amendments to the EU Data Protection Directive outlines a legislative framework to be implemented by individual states), both privacy frameworks drew inspiration from the privacy by design approach, initially developed in 1990s by Ann Cavoukian (Information & Privacy Commissioner of Ontario), and emphasized the need to increase the transparency and accountability of data practices of companies and the need to enhance individuals' control over the collection and use of information about themselves.

Using the privacy by design framework and the FTC 2012 privacy guidelines as a starting point, this chapter will 1) discuss whether privacy protection schemes focused on informational privacy adequately protect individual privacy in the context of the emerging mobile marketing practices; and 2) outline the principles of a "home mode" for mobile privacy as a privacy approach informed by the need for control over communicative interactions rather than control over personal information. Thus, the aim of this chapter is to offer a supplement to interpreting the "privacy by design" framework, understanding that can be used to evaluate the privacy implications of mobile communications and devise privacy protection schemes for the mobile environment.

The chapter will start with a background section that summarizes the original "privacy by design" principles and their implementation in American context. The next section will discuss the limitations of this privacy framework as implemented in the U.S. In particular, the section will explain how economic arrangements in the current mobile environment, as well as the design imperatives of content-delivery platforms, create lock-in situations and situations of compelled persuasion (Popescu & Baruh, 2012) that threaten the privacy of the mobile users and cast doubt on the ability of current privacy policies to account for users' need for meaningful choices among privacy regimes. The larger implication of this argument is that privacy policies should not focus exclusively on data collection, appropriation, and sharing, but also enable user autonomy and choice of solitude over communication. The next section will discuss why, within the context of interactive media in general and mobile communications in particular, the fuzzy boundaries between public and private make it increasingly difficult for individuals to signal their preferences regarding communicational privacy. As a remedy, the section will propose several principles for a "home mode" for mobile users meant to restore the mobile users' ability to have control over communicative interactions.

BACKGROUND: PRIVACY BY DESIGN

The objective of the privacy by design approach is to ensure that individuals have control over their information. To that purpose, the essence of the approach is to consider privacy protections at the outset, at the level of design and implementation