Chapter 93
Eliciting Design Guidelines for Privacy Notifications in mHealth Environments

Patrick Murmann
Karlstad University, Karlstad, Sweden

ABSTRACT

The possibilities of employing mobile health (mhealth) devices for the purpose of self-quantification and fitness tracking are increasing; yet few users of online mhealth services possess proven knowledge of how their personal data are processed once the data have been disclosed. Ex post transparency-enhancing tools (TETs) can provide such insight and guide users in making informed decisions with respect to intervening with the processing of their personal data. At present, however, there are no suitable guidelines that aid designers of TETs in implementing privacy notifications that reflect their recipients' needs in terms of what they want to be notified about and the level of guidance required to audit their data effectively. Based on an analysis of gaps related to TETs, the findings of a study on privacy notification preferences, and the findings on notifications and privacy notices discussed in the literature, this paper proposes a set of guidelines for the human-centred design of privacy notifications that facilitate ex post transparency.

1. INTRODUCTION

The number of users of mobile health (mhealth) devices is increasing (Statista, 2018), as is the spectrum of applications related to personal informatics (Knowles et al., 2018). However, few users of online services know how their personal data are processed by the data services they are relying on (Lau et al., 2018). This imbalance of knowledge, and hence power, between service providers and users is in stark contrast to the statutes of the EU General Data Protection Regulation (GDPR) (European Parliament and the Council of the European Union, 2016), which mandate transparency with respect to how personal data are processed. The Regulation considers data transparency a prerequisite for enabling data subjects to make informed decisions about intervening with the processing of their personal data, i. e. the right

DOI: 10.4018/978-1-7998-8954-0.ch093

to access, rectification, to object to processing and profiling, and to have their data erased (GDPR Art. 12 et seq.). The deviation from the legal statutes is particularly remarkable because 'data concerning health' are considered special categories of data (GDPR Art. 9) whose processing warrants special care and responsibilities on the part of data controllers (Art. 29 Working Party, 2011).

One way of providing users of online data services with insight about the processing of their personal data is by means of *ex post transparency-enhancing tools* (TETs). Ex post TETs provide intelligible information about how their personal data *have been processed*. In this respect, ex post TETs differ from *ex ante* TETs, the latter of which communicate risk and potential outcome *before* users perform an action, such as before signing up for a data service or before installing an app. For the sake of readability and unless the context in question requires clarification as to whether it refers to an ex ante or ex post scenario, the term 'TET' will be used in lieu of 'ex post TET' throughout this article to refer explicitly to *ex post* transparency-enhancing tools.

TETs retrospectively provide users of online data services with transparency about the processing of their personal data and guide them in making informed decisions with respect to managing the data they have disclosed previously. Hence, TETs can serve as indicators of facts that help users to hold data controllers accountable for how their personal data have been processed. The medium that facilitates ex post transparency discussed in this paper is privacy notifications, which notify users about events related to personal data processing deemed relevant for them. However, many TETs discussed in the literature are limited in terms of their usability in that their design does not systematically reflect the needs of their final users (Murmann and Fischer-Hübner, 2017a). This suggests research that addresses usable TETs specifically through the lens of human-centred design (International Organization for Standardization, 2010), and motivates the following research questions:

1. What kind of model is required to adequately describe the conceptual and functional nature of TETs that employ privacy notifications to enable intervenability?
2. What findings exist in the body of literature that lend themselves to conceptualising design guidelines for privacy notifications received on mobile devices?
3. What guidelines can be inferred from the model and the findings in the literature for the design of TETs that best reflect the individual needs of their users?

The context of use considered throughout this article is ex post transparency of personal data processed in mhealth environments. Data subjects disclose their health data to online services who process the data, and potentially share them with third parties. As users of the online mhealth services, data subjects take the role of both originators and auditors of their personal data, and achieve data transparency by obtaining retrospective information about how their data have been processed by means of a TET. In this regard, mhealth specifically pertains to scenarios of fitness tracking and self-quantification. Conceptually, this domain differs from clinical mhealth environments in that personal data generated therein are managed and audited by the data subjects themselves rather than by a professional caretaker or administrator. Hence, the final user of a TET is typically a lay person with respect to information privacy. The TET itself is considered to be a technological artefact in the form of an application running on a mobile device that is controlled by the user.

The main contribution of this paper is to analyse the findings established in the literature, to apply them to a model that reflects the asynchronous nature of privacy notifications, and to derive from them