Chapter 75

Ambiguities in the Privacy Policies of Common Health and Fitness Apps

Devjani Sen
Algonquin College, Canada

Rukhsana Ahmed
https://orcid.org/0000-0003-0381-4491
University at Albany, SUNY, USA

ABSTRACT

With a growing number of health and wellness applications (apps), there is a need to explore exactly what third parties can legally do with personal data. Following a review of the online privacy policies of a select set of mobile health and fitness apps, this chapter assessed the privacy policies of four popular health and fitness apps, using a checklist that comprised five privacy risk categories. Privacy risks, were based on two questions: a) is important information missing to make informed decisions about the use of personal data? and b) is information being shared that might compromise the end-user's right to privacy of that information? The online privacy policies of each selected app was further examined to identify important privacy risks. From this, a separate checklist was completed and compared to reach an agreement of the presence or absence of each privacy risk category. This chapter concludes with a set of recommendations when designing privacy policies for the sharing of personal information collected from health and fitness apps.

INTRODUCTION

Mobile leisure, health, and wellness applications (apps) are ubiquitous. Research suggests that there are approximately 97,000 varieties of inexpensive and easy to use mobile health apps available in the market; at such a pace numbers are becoming outdated almost as soon as they are published (Privacy Clearinghouse, 2013). With approximately 320,000 of health and fitness apps in major app stores (Young, 2018),

DOI: 10.4018/978-1-7998-8954-0.ch075

the question arises as to what happens to the sensitive data consumers enter into these apps, and what happens when these apps share data with advertisers and other third parties without the user's knowledge.

A growing topic of interest in both Canada and the U.S. concerns exactly what third parties can legally do with personal data. American law dictates that health insurance companies cannot discriminate based on a history of illness, specifically, severely restricting the dissemination and distribution of private health information without documented consent. However, while data held by a health plan, health care provider, or lab may be protected by the federal Health Insurance Portability and Accountability Act (HIPAA), legal scholars warn that if a patient is going to upload health or wellness data to a mobile application (app), it may not be covered by those laws (Rogers, 2014). Such legal ambiguities have implications for Canadian users of health and wellness apps, because many of these devices are based in the U.S., with the data being stored on U.S. servers and thus they may not conform to privacy requirements (Akkad, 2013). Clearly, such privacy concerns apply globally in any cases where personal data may be shared to third parties across two or more countries anywhere in the world.

There are some other important concerns with privacy and security issues related to mobile health and fitness applications (Huckvale et al. 2015; Rajindra et al. 2014). For example, personal apps collect all sorts of personal information like name, email address, age, height, weight, and in some cases detailed health information. When using such apps, many users may share a host of personal information and consequently make themselves targets to misuse of this information by unknown third parties. Moreover, according to Gralla et al. (2011), apps can gather the phone number and the unique ID number of each type of phone. In this way, personal information that apps gather about an end-user can be matched to these IDs, which means that ad networks can easily combine various pieces of information collected by multiple apps to build a sophisticated profile about a given end-user and thereby posing a major privacy risk to personal data. Therefore, un-informed decision by end-users raises important concerns regarding the ethics around sharing personal data gathered from health and fitness apps to third parties. To summarize, the issues raised above may be broken down to the following concerns:

(1) ownership and veracity of sensitive data shared on personal apps
(2) what end users really understand about the use of their data (what data are being collected and the specifics of how it may be used)
(3) the ethics of sharing end-users' personal information and sharing it with third-parties

Despite the important role of informed consent in the creation of health and fitness mobile applications, the intersection of ethics and sharing of personal information is understudied and is an often-ignored topic during the creation of mobile apps. After reviewing the online privacy policies of a select set of mobile health and fitness apps, this chapter will conclude with a set of recommendations when designing privacy policies for the sharing of personal information collected from health and fitness apps.

BACKGROUND

Online privacy policies, which regulate the relationship between the user and the website with the purpose of limiting companies' legal liability during site use, are also employed by users to inform their understanding of the manners in which personal data are treated by companies. Despite their importance to users, however, studies suggest that these policies are often ignored (Angulo, Fischer-Hübner, Wea-