Ethical Ambiguities in the Privacy Policies of Mobile Health and Fitness Applications

M

Devjani Sen
University of Ottawa, Canada

Rukhsana Ahmed
University of Ottawa, Canada

INTRODUCTION

Mobile leisure, health, and wellness applications (apps) are ubiquitous. A recent study reveals 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of inexpensive and easy to use mobile health apps available in the market; at such a pace numbers are becoming outdated almost as soon as they are published (Privacy Clearinghouse, 2013). It is predicted that by 2017 half of the world's more than 3.4 billion smart phone users will have downloaded health and fitness apps (Comstock, 2013), which raises the question: what happens to the sensitive data consumers enter into these apps?

Indeed, a hot topic in both Canada and the U.S., concerns exactly what third parties, such as insurance companies, can legally do with personal data. American law dictates that health insurance companies cannot discriminate based on a history of illness. 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; Whitman & Mattord, 2012). 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).

There are some other important concerns with privacy and security issues related to mobile health and fitness applications. 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 trustfully log everything from diet to sleep patterns in the apps. By sharing such personal information end- users may 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: the Unique Device Identifier (UDID) on an iPhone, the International Mobile Equipment Identity (IMEI) number on a BlackBerry, and (depending on the make) the IMEI or the Mobile Equipment Identifier (MEID) on an Android 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, uninformed decision making by end-users raises important concerns regarding the ethics around sharing personal data gathered from health and fitness apps to third parties. These concerns can be much graver when Martínez-Pérez and colleagues (2014), in a review of privacy and security in mobile health apps, found evidence of insecure handling of clinical and medical data.

DOI: 10.4018/978-1-5225-2255-3.ch528

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 is 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 used by users to inform their understanding of the ways personal data are treated by companies. Despite their importance to users, however, studies suggest that these policies are often ignored (Angulo, Fischer-Hübner, Weastlund, & Pulls, 2012; Jensen & Potts, 2004; Kesan, Hayes, & Bashir, 2012; Tsai, Egelman, Cranor, & Acquisti, 2011). As pointed out by Steinfeld (2016), since agreeing to the terms of the policy is usually a prerequisite for subscribing to a website or a web service, users typically sign their consent almost automatically, so that these terms are rarely considered as reasons for joining or avoiding a given website.

Studies suggest that many apps do not have a privacy policy, or that apps do not grant users access to and control over personal information before users downloads and/or after use apps (Privacy Rights Clearinghouse, 2013). Nevertheless, having a privacy policy or providing a link to it is not enough to safeguard end-users' right to data privacy. Studies have also identified a number of cognitive factors which limit the comprehension of existing privacy policies, including complexity, legal language, and length (Angulo et al., 2012; Milne & Culnan, 2004; Nissenbaum, 2011; Tsai et al., 2011), use of vague terms and concepts (Anton et al., 2003), as well as design issues such as format and font size (Milne & Culnan, 2004).

IDENTIFYING PRIVACY RISKS IN HEALTH AND FITNESS APPLICATION PRIVACY POLICIES

Clearly, if privacy policies are not being read, there is a need for more readable policies that will be better understood and will more effectively inform users decisions on whether it is prudent for them to join a given website service agreement. Indeed, given the varied educational levels and socio-economic backgrounds of online consumers that encompasses a wide range of the global population, it is critical that companies communicate effectively with customers through their online privacy policies (Wheatman & Ghiselli, 2014). With these considerations in mind, the purpose of the present chapter was to investigate the presence of important information and its presentation in plain language format in privacy policies of health and fitness applications. To this end, a close examination of the privacy policies of selected commonly used health and fitness applications was performed. Considering the limited scope of this chapter, the number of apps to examine was limited to four in order to properly execute a combined approach of using a checklist and discussing relevant excerpts from the selected privacy policies.

Health and fitness applications are application programs that offer health-related services on