Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 37 (2014) 348 – 355

Procedia Computer Science

The 4th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2014)

A privacy policy comparison of health and fitness related mobile applications

Mark Rowan[1] and Josh Dehlinger

Department of Computer and Information Sciences, Towson University, Towson, MD, 21252 USA

Abstract

Many mobile device end users believe that privacy is important when dealing with personal health-related information, but the challenge is to develop privacy policies in a meaningful way so that mobile software application developers can adequately meet the requirements of their intended end users. Comprehensive privacy policies, which meet self-regulatory guidelines of increasing transparency on data collection, are often written in a way that average mobile users cannot understand or completely ignore. This paper provides the results of a privacy policy comparison including application permissions requested and several readability metrics used to assess the current state of privacy policies in the health and fitness mobile application market. Our analysis indicates that developers may not be considering their end-users' reading comprehension levels and specific application permissions are not adequately addressed when developers are creating their privacy policies.

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.

Keywords: Privacy Policy; Readability; Mobile Applications; Health and Fitness; Trust and Privacy

1. Introduction

Recent headlines like, "This Flashlight Android app has been secretly and illegally sharing your personal data with advertisers" [1], "Android's app permissions were just simplified-now they're much less secure" [2] and "Users beware: leaks from health websites, apps cause for concern" [3] may influence end users to mistrust mobile applications and discourage their use. Microelectromechanical sensors (i.e., accelerometer, pressure, light sensors, etc.) in mobile phones can inform applications about its environment and be used by mobile applications in a variety of ways. For example, end users can install health and fitness applications on their mobile phones or use companion

[1] Corresponding author. Tel.: 011-1-410-704-2633; fax: 011-1-410-704-3868.
E-mail address: mrowan2@students.towson.edu

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.
doi:10.1016/j.procs.2014.08.051

wearable computing devices to track their own well-being (e.g., diet, fitness goals, pregnancy trackers, etc.) and then intentionally share their results with friends, family, coaches, and physicians. Personal health and fitness has become social for many end users for motivational purposes, reporting progress and goal attainment.

It has been reported that health and fitness applications are playing a pivotal role in changing the utility of mobile devices (i.e., tablets, phones) into medical instruments that capture blood test results, glucose readings, medical images and other medical information to better enable physicians and patients to manage and monitor health information [4]. The recent trend in wearable medical devices with biosensors is causing concern in the healthcare community about misdiagnoses that could have serious concerns for consumers [5, 6]. This uneasiness is amplified by the fact that there is no requirement for application developers to have any healthcare experience or fitness certification when creating and publishing health and fitness mobile applications. Many mobile application developers do not have the resources for legal counsel and may be more likely to make false claims to patients without seeking Food and Drug Administration (FDA) clearance [6] or lack the knowledge about privacy when handling personal health information of end users in some situations [7].

A major challenge is to improve transparency for end users about commercial data practices of mobile applications that collect, store and transfer personal information by presenting information in effective privacy policies. Readability is concerned with the ease with which a person can read (i.e., to extract, evaluate, and use information from a text source [8]. The inability to read and understand health information, privacy policies or terms of service agreements can have serious consequences for people by sharing personal information with the software application developer, publisher and some third parties. Privacy concerns have been raised that third party use of personal health information could lead to possible employment discrimination, loss of insurance coverage, higher insurance premiums, or other privacy intrusions [9]. The U.S. Federal Trade Commission (FTC) recommends that all users read privacy policies to understand how an application or website maintains accuracy, access, security, and control of personal information it collects and whether it provides information to third parties [10]. The FTC recently announced that a simple investigation into 12 popular health and fitness applications found them sending users' personal information (i.e., precise health metrics about the end users) to 76 different third parties [11].

The U.S. Food and Drug Administration (FDA) has stated that they will regulate mobile applications that do the same thing as traditional medical devices, which is intended for use in the diagnosis, cure, mitigation, treatment or prevention of disease or intended to affect the structure or function of the body of man or other animals [12]. The Privacy Rule of Health Insurance Portability and Accountability Act (HIPAA) defines protected health information (PHI) as individually identifiable health information held or transmitted by a covered entity (e.g., health care providers, health plans, health care clearinghouse) or its business associate, in any form or media [13]. Generally, software applications specifically for the end user would not be subject to HIPAA. If an end user shares the information with a HIPAA covered entity (e.g., CVS Pharmacy), then the information would become subject to HIPAA compliance [7].

There have been previous studies exploring privacy issues with mobile technologies related to healthcare, including [14, 15] and work on assessing privacy risks with consumer mobile health and fitness applications, such as [16]. Privacy policies are not an effective tool for notifying end users about data collection, storage and transmission practices of mobile applications. There are challenges with the perceived cost in time and effort in reading privacy policies [17], problems with valuation of end-user personal data [18], as well end-user reading comprehension challenges with privacy policies and terms of service [19, 20]. Also of note, a 2007 study found 75% of consumers think that as long as a website has a privacy policy means that the website will not share data with third parties [21].

This paper provides the results of a privacy policy comparison including Android application permissions requested and several readability metrics used to assess the current state of privacy policies in the health and fitness mobile application market. The analysis indicates that developers may not be considering their end-users reading comprehension levels when creating their privacy policies. An inability to understand privacy policies could lead to negative consequences, including end-users inappropriately sharing personal health information or simply an inability by end-users to understand the privacy policy may lead to end-users not installing their applications due to privacy concerns. The contribution of this paper is an assessment of privacy policies for 20 popular Android mobile applications dealing with health and fitness, as well as a comparison of their requested permissions. It is relevant for businesses and software developers to improve transparency to end-users and possibly create more effective privacy policies that could alleviate end-users' concerns over the uses of their personal information.