Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Mobile Health and Fitness Apps: What Are the Privacy Risks? [1]

Posted Jul 01 2013
Revised Dec 16 2016

1. Wellness App Basics

Most Americans own at least one mobile device capable of running software applications (apps), and there are millions of apps available for almost every purpose imaginable. This includes health and fitness monitoring.

In 2013, Privacy Rights Clearinghouse (PRC) received a grant from the California Consumer Protection Foundation to study health and fitness app privacy. PRC analyzed 43 health and fitness apps (23 free and 20 paid) on the Apple iOS and Android platform. This guide includes a summary of our findings.

Wearables have continued to gain traction in the marketplace as a way to automate data entry into mobile apps.

The Apple App Store, Google Play [2], and Amazon [3] all make an effort to screen apps for security risks before the apps are available in stores, but the exponential growth of app use has made it impossible for companies to keep up.

a. Definitions

Mobile health and fitness apps comprise a significant segment of the app universe. This guide focuses on what we consider "wellness" apps intended for consumer use. It does not focus on applications that integrate with medical treatment or are intended for health professionals.

i. Wellness Apps

Wellness apps include those that support diet and exercise programs, pregnancy trackers, behavioral and mental health coaches, symptom checkers that can link users to local health services, sleep and relaxation aids, and personal disease or chronic condition managers.

Some apps are interactive, and others are informational. Consumers use some to participate in a program while others use them to look up information about diseases or medications, nutritional values of restaurant food, horoscopes or baby names, etc. A number of apps are simply mobile magazine subscriptions for health and lifestyle publications.

There are several options for downloading health and fitness applications. However, it's probably easiest, safest, and most common to use the App Store for iOS applications and Google Play for Android. You can search both by app name or type and can read about an app before you download it. You can find out what the app does (although not necessarily the exact information it collects), see sample screens—and sometimes videos of how an app operates--read user reviews, link to the developer's website and link to other comparable apps.

ii. Wearables

Wearables include any device or technology "worn" by the user. The vast majority of wearables aim to automate collection of

data that apps formerly required users to manually enter. Just like apps in the health and fitness space, there are many different types of wearables. They track many different types of data, but the aim of most is to track at least steps and sleep. More advanced wearables claim to be capable of tracking heart rate and even your brain signals. Our 2013 study did not explore wearables, but most of them do have a corresponding app. This means that many of the same concerns regarding researching the privacy policy for apps applies to wearables as well.

2. Risks Posed By Mobile Health and Fitness Applications/Devices

Any data that you share with an app or device could be shared with any number of third parties. A privacy statement may help you determine how risky an app or device is, and whether or not you are comfortable sharing your data with the app or device.

- **Mobile devices—phones, tablets, and wearables—are ideal tracking tools.** Despite their many benefits, mobile devices, apps, and wearables can all be highly privacy-invasive. Smartphones are internet- and geolocation-enabled, as are most tablets, and even some wearables. People who own these devices carry them almost everywhere they go and rarely turn them off.

Specific risks of using mobile health and fitness applications:

- **Many health and fitness applications collect a great deal of personal information.** Apps may prompt users to enter a name, email address, age, gender, height, weight, and photo. They may also ask for lifestyle information. For example, the app may ask questions about food consumption and exercise habits.
- **Mobile applications, especially apps that you download for free, depend on advertising to make money.** They may share personally identifiable information with advertisers, or allow ad networks to track you. Almost all applications send non-personal data about how you use an application to data analytics services. If an application collects your universal device ID (UDID) or embeds a unique ID in the application you download, analytics data can be tracked back to you personally.
- **Many mobile applications have poor security.** Although they may have a privacy policy that says they protect the privacy and confidentiality of your information, apps may transmit that data unencrypted and over unsecure network connections. They may also transmit information that includes your disease or pharmaceutical search terms—for sexually transmitted diseases or anti-psychotic drugs, for example— and allow it to be viewable by anyone watching on the network. The mere use of some apps discloses highly sensitive information. For instance, creating a profile in the “Hope” app would disclose that a user is Herpes-positive.

b. PRC’s analysis of mobile health and fitness app developers’ information practices

The PRC study of mobile health and fitness apps looked at developers’ information practices from two vantage points: the consumer-user experience and a computer scientist’s analysis of what was going on behind the user interface. The goals of the project were to discover as much as possible about:

- What information a range of health and fitness applications collect.
- Whether apps have privacy policies and how thorough and technically accurate they are.
- What privacy policies acknowledge doing with personal and non-personal information they collect.
- How developers’ actual information practices correlate with their privacy policies, through technical analysis of the apps.
- The extent to which users have access to and control over the information an app collects, both when installing the app and after using it.

i. The major consumer-level and technical-level findings of PRC’s study of mobile health and fitness applications

Our mobile medical apps project has resulted in several reports: consumer-level findings, a technologist’s report, tips for app developers, a webinar, and the evaluation criteria for our app analysis. The major findings are summarized below in this section. For more detailed information, you can link to the additional documents in Section 7 [4].

Consumer-level findings:
The main things we looked for at the consumer level were:

- How much notice did developers give users about their information practices? Was there a privacy policy? How complete is it in terms of including recognized Fair Information Practices? How accessible is the policy? How readable is it to someone with a high school education?
- How much access and control over personal information did an application give users? Are they able to update and correct their personal profiles? Can they delete any personal information entirely? What choices do users have about sharing both personal and de-identified information?

The table summarizes the highlights of our consumer-level findings about the quality of notice in the privacy policies of free and paid health and fitness applications, along with the availability of some user controls of information.

The acronym PII stands for “personally identifiable information.”

	Free apps	**Paid apps**
App has link to website privacy policy	43%	25%
Notifies user that privacy policy does not apply to 3rd party links	48%	25%
Notifies user that personal information made public is not protected	57%	15%
Shares user-generated PII data with advertisers	43%	5%
Shares aggregate (non-PII) data with marketers	52%	55%
Uses anonymized (non-PII) data for analytics	70%	70%
Contact info: developer’s email address listed in policy	57%	100%
Can opt out of developer/vendor sharing data with 3rd parties	57%	30%

Can opt in to data sharing with 3rd parties	35%	30%

Most recent date of analysis: May 7, 2013

Technical findings:
The technical analysis assigned risk levels to the applications tested based on the amount of personal information they collected, along with our judgment as to the sensitivity of that information. We assigned risk based on the criteria below, on a scale of 0-9. For the sake of convenience, this numerical rating scale was converted to "high," "medium," "low," "none":

- High risk (7-9)—includes address, financial info, full name, health information, geo-location, date of birth (DOB), ZIP code
- Medium risk (4-6)—enhanced privacy risk to PII; email, first name, friends, interests, weight, potentially embarrassing/sensitive info
- Low risk (1-3) —moderately low risk; anonymous tracking, device information, a third party knows the individual is using a mobile medical app
- No risk (0) — no PII or health-related information

Based on these criteria, we determined the following:

- 40% of the apps were high risk (17 of the 43 apps)
- 32% of the apps (14 of 43) were medium to high risk
- 28% of the apps (12 of 43) were low to medium risk
- none of the apps were evaluated to be no risk

The technical analysis identified the three main technical causes of informational privacy risks in mobile health and fitness apps to be the following:

- **Unencrypted network connections:** Insecure network communications posed the greatest risk to privacy. Only a single paid application used HTTPS (SSL) exclusively for all of its network connections. None of the apps used additional encryption (such as PGP), for secure transmission of personal information.

- **Advertising:** The next greatest risk to the privacy of users' personal information was apps that sent personal information to advertisers to use for serving personally targeted ads. This occurred far more often with free applications (43% of 23 apps analyzed) than with paid apps (only one of 20 analyzed). This should be expected, because free apps often rely on advertising as their only source of revenue, while paid apps depend on app sales to generate most of their revenue and rarely include advertising.

- **Analytics:** Data that apps transmit to third-party analytics services also present a serious privacy risk. Almost all applications collect and send non-personally identifiable usage data to third parties for analysis, in order to "improve the user experience" and for developers' own marketing purposes. We observed that data with privacy-invasive details of usage behavior is generally sent over HTTP, not HTTPS (for example, What information did you access to deal with PTSD symptoms? What store products' bar codes did you scan with your phone for enhanced nutrition and calorie information? Which STDs did you research in an app's symptom checker?). This data can potentially be collected in a central database that links an individual's usage of other apps that employ the same analytics services. We found that 55% of paid and 60% of free apps which we investigated use third-party analytics services.

3. Laws

The mobile applications ecosystem is largely unregulated. This is a particular concern with health and fitness apps, which often collect both demographic and health (or medical-like) information that does not fall under the protections of any health privacy laws. When you use the apps, you often create a record of data such as your diet, daily exercise, glucose readings, pregnancy, and/or menstrual cycle.

In most cases, your health and fitness data is only protected to the extent it is stated in a privacy policy—if there is a privacy policy at all. Also, many health and fitness apps allow and encourage users to share what you might consider sensitive information via social media. Once information is public you have little to no control over it.

Section 5 of the Federal Trade Commission Act protects consumers from "unfair and deceptive acts". Under this provision, when companies tell consumers they will safeguard their personal information, the FTC can enforce to make sure that companies live up these promises. See the FTC's guide *Enforcing Privacy Promises* [5] for more information.

Note: The FTC does *not* resolve individual complaints, but such complaints may contribute to an investigation or enforcement action.

State Attorneys General have jurisdiction to enforce each states' own laws similar to section 5 of the FTC Act.

4. Protecting Your Privacy

Mobile health and fitness apps offer many benefits and are very convenient to use. Since they collect a great deal of personal information in ways that are not currently regulated and may have poor information security practices, balancing the risks versus benefits before using is a reasonable thing to do. These tips all apply to the use of wearables and their corresponding apps as well.

a. Settings/Permissions

Perhaps most important is ensuring that every app you have or download is set to share only what you expect it to share, and only with whom or what you expect to share it with. Permissions commonly refer to which of your device's features the phone can access. For example, you may grant an app permission to allow your device to access location services when you use the app.

i. Permissions to access device features

Figure out which permissions an app asks for, and turn off those that appear to be unnecessary for the app to function. Fortunately, public pressure has led to operating systems offering users more control over app permissions.

ii. Permission to share information

Many apps offer the option to share information through social networking sites. Make sure that you know whether these options are turned on or off, and make an informed choice.

b. Tips

Here are some general points to be aware of when using wellness apps:

- **Assess the "Creepy" Factor.** Make your own assessment of an app's creepiness or intrusiveness based on the personal information it asks for in order to use the app. For example, what information are you putting into a personal profile that you might not want advertisers to have or to become public? Are you giving away information about a disease or mental condition or a pregnancy problem that could have negative repercussions for you if it ends up with data brokers? Consider, too, the possibility of negative emotional repercussions of discussing private matters—such as your weight or a miscarriage—in an application-based chat group.

- **Assume your app is selling you out.** Assume that any information you provide to an app may be distributed to the developer, to third-party sites the developer may use for functionality, and to unidentified third-party marketers and advertisers. Only provide information you are comfortable with the app sharing with those third parties.

- **Think twice about telling your app your personal information.** Try to limit your input of personal information and exercise caution when you share it. Widespread sharing may have as much impact on personal safety as it does on privacy. This is particularly true of location sharing, for example, of your running or bicycling route in a time-and-distance competition with other app users.

- **Research the app developer before you download the app.** Although it's difficult to evaluate the validity of a great deal of information on the Internet, try to assess how credible the app developer is. Assess the quality and content of information on the app developer's website. Look for user reviews either through the app store or online. Finally, you can often learn about the app or the developer in the media.
- **Read the app's privacy policy.** If the app has a privacy policy—and many do not—it is increasingly common to find it (or a link to it) prior to download. If you are unable to find a privacy policy through the app store, you may be able to find one on the developer's website. Note that, if there is no website, there may not be a privacy policy either. Find any relevant contact

information and contact the developer with questions.

- **Consider paying for privacy.** For maximum privacy, consider only using paid health and fitness apps and avoid applications that embed advertising or that seem to be primarily about selling products related in some way to the purpose of the app. However, you should still read the privacy policy to determine whether you are comfortable with it.
- **If an app allows you, try the features first without entering personal information.** Some apps give you the option of trying out the features without entering personal information. Take advantage of this opportunity when it's offered to decide whether you want to proceed with using the app at all.
- **If you stop using an app, delete it.** You will free up some memory to download other apps, and it won't continue to do things like broadcast your location or interact with other apps on your device—or remain in "always on" mode, draining your battery.
- **If you have the option, also delete your personal profile and the data archive you've created by using the app**—of your food intake, exercise routines, pregnancy stages, etc. You can't recall what's already been shared or that you've made public, but you may be able to prevent continuing use of stored data after you're no longer using the app. If you want to retain any data you've already entered, many apps offer the option to download your data as a .csv (a file which can be opened by Microsoft Excel). However, take into consideration that if the app sends you your data over e-mail which is not encrypted, that data could be intercepted and read by others without your knowledge.
- **Check the app's notification settings**. Do the app's notifications show up on your lock screen? If so, someone could pick up your phone and potentially be alerted to an event such as a high blood pressure warning.

c. Filing a Complaint

If the company does not comply with its privacy policy, you can file a complaint with the FTC or the state attorney's office. To do this, visit these websites:

- Federal Trade Commission (FTC)
  Online: The FTC has a secure complaint form [6].
  Phone: (877) 382-4357
  TTY: (866) 653-4261
  Mail: 600 Pennsylvania Avenue, NW
  Washington, DC 20580

Your State Attorney General

For California:
Online: Use the Consumer Complaint Against A Business/Company [7] form.
Phone: (916) 322-3360/ (800) 952-5225 Toll Free - CA only
TTY/TDD; (800) 735-2929 (California Relay Service)

To mail the form, download the Consumer Complaint Against A Business/Corporation [8], available in .pdf, and send it to:

> Public Inquiry Unit
> Office of the Attorney General
> P.O. Box 94425
> Sacramento, CA 94244-2550

For information on the State Attorney General of California's collection and use of personal information, please see Information Collection, Use and Access [9].

4. Additional reports from PRC's study

Mobile Health and Fitness Applications and Information Privacy: Report to California Consumer Protection Foundation [10] (the consumer-level report)
Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications
Privacy-Aware Checklist for Mobile Application Developers [11]Webinar summarizing the project methodology, findings, and tips [12] (a how-to)

Evaluation of the mobile apps: data elements examined and questions asked of each app [13]

5. Resources

California Attorney General:
Privacy on the Go: Recommendations for the Mobile Ecosystem [14] (January 2013)

Federal Trade Commission:
Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report [15] (February 2013)
Understanding Mobile Apps [16] (September 2011)

The Pew Internet & American Life Project:
Privacy and Data Management on Mobile Devices [17] (September 2012)

NTIA (National Telecommunications and Information Administration):
Privacy Multistakeholder Process: Mobile Application Transparency [18] (November 12, 2013)

Privacy Rights Clearinghouse:
Slides: Mobile Health & Fitness Apps: What Are The Privacy Risks? [19] (October 29, 2013)
Webinar: Mobile Health & Fitness Apps: What Are the Privacy Risks? [20] (October 29, 2013)

International Association of Privacy Professionals:
Privacy Tech: A Deep Dive Into the Privacy and Security Risks for Health, Wellness and Medical Apps [21] (April 6, 2015)

Center for Digital Democracy:
Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection [22] (December 15, 2016)

Source URL (modified on December 16, 2016): https://www.privacyrights.org/consumer-guides/mobile-health-and-fitness-apps-what-are-privacy-risks

Links
[1] https://www.privacyrights.org/consumer-guides/mobile-health-and-fitness-apps-what-are-privacy-risks
[2] http://www.theverge.com/2015/3/17/8231125/android-apps-now-reviewed-by-google
[3] http://www.computerweekly.com/news/2240162449/Amazon-Appstore-opens-up-Android-to-attack
[4] https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks#section%207
[5] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises
[6] https://www.ftccomplaintassistant.gov/
[7] https://oag.ca.gov/contact/consumer-complaint-against-business-or-company
[8] https://oag.ca.gov/sites/all/files/agweb/pdfs/contact/business_corpform.pdf?
[9] https://oag.ca.gov/sites/all/files/agweb/pdfs/contact/business_info_cua.pdf?
[10] https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf
[11] https://www.privacyrights.org/mobile-medical-apps-privacy-developers-howto-report.pdf
[12] https://www.privacyrights.org/node/57081
[13] https://www.privacyrights.org/mobile-medical-apps-privacy-evaluation-spreadsheet-report.pdf
[14] http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf
[15] http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf
[16] http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps
[17] http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx?utm_source=Mailing+List&utm_campaign=2251646e41-Mobile_privacy_09_05_2012&utm_medium=emailhttp://pewinternet.org/Reports/2012/Mobile-Privacy.aspx?utm_source=Mailing+List&utm_campaign=2251646e41-Mobile_privacy_09_05_2012&utm_medium=email
[18] http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency
[19] https://www.privacyrights.org/smartphone-health-apps-slides-Oct29-2013.pdf
[20] http://www.kismetworldwide.com/clients/prc/PRC-Mobile-Privacy-Webinar-20131029.mp4
[21] https://iapp.org/news/a/a-deep-dive-into-the-privacy-and-security-risks-for-health-wellness-and-medical-apps/
[22] https://www.democraticmedia.org/CDD-Wearable-Devices-Big-Data-Report