Mobile Health and Fitness Applications and Information Privacy

Report to California Consumer Protection Foundation

By Linda Ackerman

Attorney at Law

July 15, 2013

Linda Ackerman is an attorney who works on health information privacy issues. She served as a consultant and project manager for purposes of this research and report

This project is funded by the California Consumer Protection Foundation. The Privacy Rights Clearinghouse is grateful to CCPF for enabling the organization to conduct the research described in this report.

Table of Contents

1. Executive Summary 3
1.1 App selection process 3
1.2 Why we don't name the apps we tested 4
1.3 Devices used to test apps 4
1.4 Analysis 5
1.5 General conclusions 5
2. Project Description 6
2.1 Project limitations 6
3. Definitions 6
4. Bias and Disclaimers 7
4.1 Objective and subjective criteria 8
4.2 Biases of individual reviewers 9
4.3 Additional disclaimers 9
5. Legal Framework 11
6. Methodology 12
6.1 Application selection 12
6.2 Assessment of privacy policy 13
6.3 Installation 14
6.4 Using the applications 14
6.5 Analyzing the information 15
7. Results 17
7.1 Findings from consumer/user-level analysis, from the technical analysis, and from the risk analysis for free and paid applications 18
Table 1. Mobile Health and Fitness Applications Privacy Policy Data 18
Table 2. Mobile Health and Fitness Apps Data-Handling Practices 18
Table 3. Aggregate Analysis of Quality of Privacy Policy for Free and Paid Applications 19
7.2 Technical results for free and paid applications 20
7.2.1 Assignment of risk levels 20
7.2.2 Overall technology assessment of risk: high, medium and low 21
7.2.3 Primary technological causes of risk 21
8. Conclusions 22
8.1 Privacy policies vs. privacy practices 22
8.2 How can consumers decide whether or not to use certain mobile health and fitness applications? 23
9. Related Developments 24
9.1 FDA guidance on medical devices 24
9.2 The National Telecommunications and Information Administration (NTIA) multi-stakeholder process 25

Mobile Health and Fitness Applications and Information Privacy

1. Executive Summary

Privacy Rights Clearinghouse (PRC) began this project to analyze the privacy and information practices of developers of mobile medical applications for smartphones and tablets from two vantage points: the consumer/user's perspective and what testing by a technical analyst revealed. The project was funded by the California Consumer Protection Foundation (CCPF).

While our bias going into the project was in favor of privacy, the consumer analysis started from a point of zero knowledge about the apps themselves. Along the way our focus shifted from looking for "medical" apps to looking for health and fitness apps that collect what is or could be considered medical information; call them "medical-like" apps. Our goal was to discover as much as possible about:

- What kinds of information a range of health and fitness applications collect
- Whether or not they have a privacy policy and how thorough and technically accurate it is
- What their 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.

1.1 App selection process

We looked at a total of 43 free and paid applications, half on Apple's iOS, half on Google's Android, choosing some of each type by a different selection process. We picked free apps that appeared to be medical or health-related based on what we learned from media sources. We also searched the Apple App Store and Google Play by categories, such as behavioral health, health and fitness, diet, pregnancy, stop smoking, and so on, and checked through the search results for apps that seemed to have enough substance to warrant exploring.

Selection of paid apps was more systematic. These were chosen based on what Google Play and the Apple App Store listed as their top 200 paid apps in the health and fitness category.

In all, we analyzed 43 health and fitness apps: 23 free and 20 paid apps, almost evenly divided between the iOS and Android platforms, with some apps that had versions on

both platforms. We tested paid and free apps to see how their information practices compared, based on a hunch that paid applications would be less privacy invasive because they would be less likely to rely on advertising for revenue, an assumption we found to be true in our technical analysis.

1.2 Why we don't name the apps we tested

Privacy Rights Clearinghouse is a California nonprofit corporation with 501(c)(3) tax-exempt status. The organization has over 20 years of experience educating consumers regarding their privacy rights and the steps they can take to protect personal privacy. The PRC also represents consumers' interests in state and federal legislative and regulatory proceedings.

The high-level goals of this project and this document are (1) to raise consumers' and developers' awareness of how health and fitness mobile apps affect personal privacy, (2) to inform developers on how to best build apps with strong privacy protections for their users, and (3) to empower consumers to take action to control their own personal information by providing practical tips on privacy protection when choosing and using these kinds of apps.

We worked to achieve these goals through analysis of subjective and objective dimensions across a representative sampling of 43 apps to provide consumers and developers a high-level overview of what is going on in the mobile health and fitness app space regarding personal privacy and security. We do not wish to shame, brand or claim that any particular app was "good" or "bad". Rather, our aim is to provide a high-level overview of the common trends we found during our analysis so that consumers and developers alike can make better decisions about how they choose to use, or how they choose to develop, mobile health and fitness applications.

To meet these goals, the results of our analysis are generalized as to the applications we reviewed. We do not name specific applications or developers because Privacy Rights Clearinghouse is not a seal or certification authority and as a policy does not endorse or criticize specific products or companies.

1.3 Devices used to test apps

We tested applications on four different mobile devices, two tablets and two smartphones, which represent the majority of iOS and Android devices and operating systems in current use. More extensive testing was done on the tablets than the smartphones, partly out of preference for the larger screens, which made the apps easier to see and navigate. Both platforms' tablets, however, can run apps designed for the tablet and the phone. We did not notice any particular differences between the different types of devices or the operating system platforms in how the apps worked or what the privacy risks were.

1.4 Analysis

We recorded our analysis in a spreadsheet that measured the apps by more than 150 different criteria or data points, some subjective (e.g., quality of privacy policy, privacy risk of using the app), others objective (e.g., permissions required to install the app, user access to data, and user control options). This information is in the Evaluation Spreadsheet, an unpopulated spreadsheet that shows all of our evaluation criteria, but not the specific applications we reviewed or the results for each one.

We took a two-pronged approach to the project. One part consisted of a consumer-level analysis of privacy and data practices based on using the applications. The findings are described in this document. The other part was a technological look "under the hood" to see what the apps were actually doing with the personal and non-individually identifiable data they collect. We determined how well that correlates to what their privacy policies *say* they're doing with the data.

We discuss detailed results from our analysis in Section 7. "Results" later in this document.

Here are a few key findings we found particularly surprising:

- 74% of the free apps and 60% of the paid apps we reviewed had a privacy policy either in the app or on the developer's website. In other words, 26% of the free apps and a shocking 40% of the paid apps had no privacy policy at all.
- Only 43% of free apps and 25% of the paid apps provided any kind of link from within the app to a privacy policy on the developer's website – the rest required the users to search for any relevant privacy policies themselves.
- 39% of the free apps and 30% of the paid apps sent data to someone not disclosed by the developer either in the app or in any privacy policy we found.
- Only 13% of free apps and 10% of paid apps encrypted all data connections and transmission between the app and the developer's website(s).

1.5 General conclusions

Our research brought us to the conclusion that, from a privacy perspective, mobile health and fitness applications are not particularly safe when it comes to protecting users' privacy. Consumers who have no hesitation about sharing personal information will probably find value in sharing the details of their pregnancies by linking their app with Facebook, participating in app-based chat groups and posting photographs of themselves as their pregnancies progress. Others will find that socializing their diet or exercise regimes provides support or competition that helps motivate them.

We do not intend to persuade consumers not to use mobile health and fitness applications, but rather to give them more information about what data apps collect and what they do with it. And, based on the project's technical analysis of the risks that developers' security practices raise, enable users, in a generalized way, to assess for themselves the overall privacy risks that mobile health and fitness apps pose.

2. Project Description

This project is an effort to analyze the segment of the mobile applications market concerned with health and fitness. Our focus is on developers' privacy and information practices, and on discrepancies between what they say they are doing with information and what they actually do, along with highlighting some rather casual security practices that are surprisingly common. The goal is to provide consumers with a basis for understanding the privacy risks that mobile health and fitness applications present in order to help them make better-informed decisions about using them.

2.1 Project limitations

The scope of what was possible to do in this project was somewhat constrained by its modest budget and short timeline (just over nine months). This limited the number of applications we were able to examine and the time we were able to spend analyzing them. For example, for cost reasons, we limited the paid apps tested to a price range of $1.50 to $20, and did not include apps that required additional measuring devices—at additional cost—like pedometers, weight scales or glucose meters.

We were also unable to use certain apps for an extended period, and thus accumulate more personal data by interacting with them regularly. And we lacked certain specific qualifications that would have made our conclusions about some apps, like blood glucose levels and pregnancy trackers, more meaningful.

We believe that we have nevertheless covered a representative sample and that it is possible to generalize certain industry standards and practices about the collection and uses of data and the approach to data security from the results we obtained.

3. Definitions

We shall attempt to avoid jargon in this report, but some terms need to be defined.

- **Personally identifiable information (PII):** Information that identifies an individual, and which can be traced back to that individual is PII. It may include name, address, email address, phone number, birth date, or Social Security number (SSN). Sometimes only one data point is sufficient to identify a specific individual (e.g., SSN), but generally any other two data points are enough to make a specific identification with a high degree of certainty. Widespread collection and dissemination of personal information are a concern because they can lead to

identity theft, to embarrassment or reputational harm, and to potentially detrimental exposure of information you would prefer to keep private from, for example, employers or insurers. Also, if you believe that privacy and anonymity are important social values, the Himalaya of data that's accumulated about all of us by now is simply very troubling

- **Non-personally identifiable information ("anonymized" information):** This is information that may correspond to a particular person but is insufficient by itself to identify, contact or locate the person to whom it pertains. In the context of mobile applications and online activities in general, it is the information that cookies, web beacons and other bits of tracking code collect about users' online actions or behavior. It is generally used for data analytics (see below) and serving ads. Mobile app developers that have privacy policies usually say that they collect and analyze this data in order to improve their products and the user's experience.

- **Data analytics:** Data analytics involve organizing raw data in ways that permit the extraction of usable information. Virtually all of the mobile applications we researched collect non-PII. If they connect to a web browser, they collect usage data by means of embedded bits of tracking code, like cookies and web beacons. If the app operates independently of a browser, they do it by assigning a unique number to the app you install on your mobile device. The main analytical uses developers acknowledge for this data are "improving the user experience" and marketing. Many applications also collect and store considerable personal information, either on devices themselves or remotely. Privacy policies generally say the developer will use this information only to service your account and beyond that, only with your permission.

- **Risk:** There are many ways to define risk, but what we mean in the context of mobile applications is the likelihood of secondary uses or public exposure (even if self-inflicted) of personal information.

4. Bias and Disclaimers

We tried to conduct this study as objectively as possible, but as consumer privacy advocates, we are not an entirely neutral reviewer. Our understanding of the base-level considerations for protecting the privacy of personal information is founded on principles that have come to be known as Fair Information Practices.

- **Fair Information Practices:** Privacy Rights Clearinghouse has a strong bias in favor of personal privacy. We strongly support the application of Fair Information Practices (FIPs) to the treatment of personal information in any context. That is,

    - **Notice/awareness.** Consumers should be notified of an entity's information practices before any personal information is collected from them. Notice

should include:

- Who is collecting the data
- How the data will be used and by whom
- What data is being collected and by what means
- Whether providing data is voluntary or required, and the consequences of not providing it
- What the data collector is doing to ensure the confidentiality, integrity and quality of the data.

- **Choice/consent.** Consumers should have choices about how their PII is used, particularly about secondary uses beyond the purpose for which it's collected. They should be able to consent or not, either by opting in to permit the stated uses of their information, or by opting out.

- **Access/participation.** Consumers should have access to personal information collected about them and also be able to correct it in order to ensure accuracy. With mobile applications, they should also be able to delete personal information—their user profiles and additional data they enter while using the app—that they have not made public themselves.

- **Integrity (accuracy)/security:** Ensuring the accuracy of data requires consumer access and the ability to correct and delete personal information. Security includes proper data management and technical measures, like encryption and secure data transmission, to protect against unauthorized access.

- **Enforcement/redress:** Privacy protections have meaning only if they can be enforced. Enforcement may be through self-regulation or government regulation. For the moment, mobile apps seem to dwell in a somewhat gray area, although to the extent that mobile applications operate within web browsers or link to them, if they collect PII from California residents, they must have a privacy policy, and the Attorney General will enforce its terms. (California Online Privacy Protection Act, Business and Professions Code §§ 22575–22579; see the Attorney General's COPPA website: http://oag.ca.gov/privacy/COPPA)

4.1 Objective and subjective criteria

We have analyzed and measured mobile health and fitness applications by objective and subjective criteria. Some examples of objective criteria are the permissions an app requires in order to install it, whether it has a privacy policy, and if the app uses third parties for analytics, advertising, or to provide core functionality. The subjective criteria and measurements, particularly, are based on our support for Fair Information Practices as the standard for handling personal information. Examples include the quality of an app's privacy policy, how much the app promotes social

sharing of personal information and how legitimate a company developing an app appears to be.

4.2 Biases of individual reviewers

The applications reviewed in this study were analyzed by two different individuals, each of whom brought different knowledge and experience to the process.

- The free applications were reviewed by a non-technologist with high privacy standards and a tendency to equate more data collection and more required permissions with higher risk of using an app—even if the data and permissions were related to (or appeared to be related to) the application's functionality. This bias comes from an assumption that data is a commodity and an opportunity, and that once a developer has it, there's a good chance it will eventually if not immediately be put to uses beyond those required for the app's functionality.

- Both free and paid applications were reviewed by a technologist who also has a strong privacy bias, but in addition brings a technical (as opposed to only consumer-user) understanding of how the apps work and what the permissions mean in terms of functionality and how they can be abused for surreptitious data gathering. Along with road-testing free and paid apps at a consumer level, the technologist's other roles in the project were: 1) analyzing what data apps were collecting (what they acknowledged and did not acknowledge); 2) determining to the extent possible where the data was going and what developers were doing with it; and 3) assessing the security of data transmission and storage.

4.3 Additional disclaimers

- The results of our analysis are generalized as to the applications we reviewed. We do not name specific applications or developers, because Privacy Rights Clearinghouse is not a seal or certification authority and as a policy does not endorse or criticize specific products or companies.

- The goal of the project has not been to label individual applications as good or bad, but rather to conduct a broad survey of a segment of the mobile app marketplace. The result is a high-level sample that identifies application behaviors in the aggregate and, primarily in the technology report identifies common technical causes of privacy risks and offers suggestions for building the apps to improve privacy protections.

- We did not integrate social media into our research by taking up the option within many mobile applications to connect with Facebook, Twitter or Google+. We acknowledge that this may not represent normal use of applications that are designed to be social and that promote the benefits of socializing your information, for example, by making an exercise program competitive or creating a support network for a pregnancy or diet. It illustrates our bias for limiting the torrent of personal information that is constantly pumped out to the web to be monetized in any way possible. The effect of this is that we did not use some apps as the developers intended and, in the process, also limited the amount of third-party data collection and use that might have been discovered. However, we do not believe that this limitation makes our findings any less accurate or valuable, since the privacy practices of various social media are well publicized, especially when seemingly abusive behaviors are discovered.

- We did not select applications that were only informational resources about a given subject (symptoms, diseases or prescription drugs, for example) but did not collect any personal information. With hindsight, it would have been interesting to know if these applications were keeping a non-personally identifiable record of the information users looked up, or if, for example, user searches and clicks were linked to a unique device ID (UDID) or application ID that could make them personally identifiable, but we did not consider that possibility at the time.

- We did not choose applications that appeared to be for use by professionals, because we wanted to learn about developers' information practices with regard to consumers and the personal and non-personal data their use of a consumer-focused application generates. Mobile health applications for professional use would be a subject for another project.

- We did not use actual medical devices for a number of reasons, not the least of which was their cost. Also, we would have had to simulate the typical use of these devices in order to study the kinds of data they collect and how it is used. This would not have been possible with, for example, devices that monitor chronic medical conditions, because it would have been necessary actually to have the condition to learn how the app treated the data and how it interacted with a user based on what it was measuring—like glucose levels. For somewhat similar reasons, we did not consider devices that remotely monitor and control implanted devices, like pacemakers.

  Mobile applications that act as medical devices—including apps offering diagnostic features like pregnancy testing, urinalysis and glucose monitoring—are the subject of a recent Guidance from the Food and Drug Administration (FDA), titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for

Industry and Food and Drug Administration Staff."

- As noted, time and budget constraints limited the number of applications we were able to analyze and test. We believe, however, that we obtained a representative sample of applications and their information practices, while acknowledging that our data represents a snapshot in time in a product area that continues to grow exponentially, with existing products being updated, new products appearing and old products disappearing.

- Time and budget constraints also played a role in deciding not to evaluate applications that required subscriptions or additional memberships, such as one diet app and a health app that seemed to be a portable health coach that linked to providers and had a number of add-on monitoring devices. The same was true for apps that promoted paid upgrades to access any but the most basic features.

- Time and budget were a factor in not selecting apps that required or promoted add-on devices, like heart-rate and glucose monitors, pedometers and weight scales. We also consider this universe of health and fitness applications to be a subject for a separate project.

- Some results may be incomplete where we did not use all the features of an app, for example, keeping an app-based photo record of the stages of a pregnancy. We do not believe that omissions like this hindered our overall evaluations of the apps or affected the accuracy of our findings or our recommendations, because we used most of the apps' features.

- We did not include applications specifically marketed to or for use by children. This, too, could be the subject of a separate project. We did note where developers included references to COPPA (the federal Children's Online Privacy Protection Act) in their privacy policy and stated that the application was not for use by children under 13.

5. Legal Framework

Health and fitness apps may collect personal health information (such as weight and smoking status), which in this context, is not (yet) covered by the federal HIPAA privacy and security regulations. HIPAA applies only to what the regulations themselves define as "covered entities," which are health care providers, health plans and health care clearinghouses (businesses that standardize health information; e.g., a billing service that processes or facilitates the processing of data from one format into a standardized billing format). One app focused on health had an embedded questionnaire that asked what kind of health insurance you have and your household income. This linked to more surveys and the

chance to win prizes by completing them. Because the survey was performed by a third-party site, none of this survey information was covered by the privacy policy of the app itself, which we think many users will find surprising and disturbing.

California's Confidentiality of Medical Information Act (CMIA) may cover mobile applications that collect what HIPAA would define as "protected health information" (PHI)*, but its applicability seems unclear. Under Calif. Civ. Code § 56.06(a), "Any business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual. . . ."

The question is whether mobile health and fitness applications are being developed by businesses that are "organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care." Actual medical devices that send individuals' data—like heartbeat monitor data or lab results—to health care providers or into systems of electronic medical records may very well fall under the CMIA, but we are less than certain that the kinds of health and fitness apps we looked at, even if they collect personal health information, meet the statute's purpose qualifications.

* PHI under HIPAA generally includes demographic information, medical history, diagnostic test and imaging results, insurance information and other data a health care professional would collect that identifies an individual and is for the purpose of medical treatment.

6. Methodology

6.1 Application selection

The process of selecting applications varied somewhat between those that were free and those that were paid. Selection of free apps began with extensive reading in online media ranging from newspapers to trade publications to blogs. A Google Alert for mobile medical applications provided many links to articles and blogs, but these were not always useful because they were very repetitive.

Paid applications were selected more systematically, or to put it another way, a little less randomly. We looked at what the top-trending paid apps of the moment were at the primary sources for buying them: the Google Play Marketplace for Android apps and the Apple App Store for iOS. Then we considered the different types of apps in the health and fitness category with the largest number of ratings. We then selected representative apps from each usage type (e.g. pregnancy, fitness, and so on) and from different pricing tiers.

Then, looking at our stock of potential applications, we organized a preliminary sample of apps into the following categories:

- Mental or behavioral health
- General health
- Disease management
- Health and fitness
- Diet
- Pregnancy

We eliminated some applications we were initially interested in for reasons noted above: budget constraints, use of add-on devices, or memberships required for meaningful use of the app. We eliminated applications that, upon searching for them, turned out to be more aspirational than real.

Eventually, we settled on a list of 43 total applications, evenly divided between iOS and Android, with some testing of applications that had versions available on both platforms.

We checked the developers' websites, if they had a website, read privacy policies and terms of service, and made notes about developers' stated information practices.

6.2 Assessment of privacy policy

The first question was whether an application had a privacy policy. If so, was it available only on the developer's website; was it linked from the app to the website; or was it available within the app itself? Then we considered the contents of the policy. A complete privacy policy should contain all of the following:

- Information the app collects about individuals, both personally identifiable and non-personally identifiable.
- The means by which both kinds of information are collected—that is, by user entry or tracking device.
- How the developer uses both types of information—obviously to service users' accounts and deliver on the app's functionality, but also in regard to data analytics and third-party relationships with marketers, advertisers, data brokers and whatever other entities they share data with.
- What choices and controls users have over their information, including consent, access and ability to correct and delete user-entered data.
- A warning that information individuals make public by using the app (for example, by linking to the public areas of social media applications, or participating in public user groups within a mobile application) is not protected.
- A similar warning that linking to third parties—like advertisers—from within the app takes users outside the boundaries of the app's privacy policy.
- Some notification about age restrictions on using the app, generally with a reference to COPPA (the Children's Online Privacy Protection Act).

- How the developer protects the privacy and security of the information an application collects, both personally identifiable and non-personally identifiable.
- Contact information for questions and complaints, preferably with a live email link.

Mobile app users who read privacy policies should be aware that they are generally written by lawyers, and that their primary purpose is to protect developers from litigation, rather than protect users' interest in their personal privacy.

6.3 Installation

We used the standard installation procedure for apps by downloading them from either the Google Play Marketplace or Apple's App Store.

We read everything in the app's description and then installed it. One app crashed three times on installation and was abandoned. It is possible it was just a buggy version of the app that was available when we downloaded it.

With Android devices, app users see a list of permissions they must agree to before installing an app. The only choice you have if you want to install the app is to agree to all the permissions. With iOS devices you can see the permissions each app uses in your device's Settings options, but only after installation. You may be able to turn off some of the permissions (such as location services, or that the app boots when you start your device or is always running) and the app will still work, but developers usually warn that you'll lose functionality or won't be able to use the app at all if you turn off permissions. Even when you know what permissions you're granting, without a technological background, it's impossible to understand everything they might actually do in terms of capturing information or interacting with your device and the data and other applications that are already on it.

One application that we think should be a model for other developers had an FAQ on its website that actually explained what you were agreeing to by accepting the app's permissions.

After an app was installed, we looked for privacy policies, links to website privacy policies, terms of service or license agreement—anything that informed users about an app's information practices.

6.4 Using the applications

At this point we were ready to use and evaluate the apps. We toured the app first without entering any information, if that was possible, especially looking for privacy or user control settings. We noted what PII an app collected at the outset in order to

set up an account—though not all of them do this. Some apps start by having you create a user profile, which might include any of the following personal data: name, email address, phone number, credit card information, photo, date of birth, height, weight and gender. Diet apps usually ask you to set weight goals and request an email address in order to send you regular reminders about meeting your diet goals, along with other communications, such as recipes and helpful hints; exercise apps want your exercise profile or daily activity level (i.e., "lifestyle" information).

A number of applications that promoted motivation and competition—a common feature of diet and exercise apps—offered opportunities to sign up for "challenges" (and supply more information about yourself) in order to win points or badges. The more interactive apps request an email address as part of your profile and regularly send email reminders—about meeting diet and exercise goals or achieving a better balance in your food intake or exercise regime, for example, or about upgrades or products. Some send motivational messages via the app; some have newsletters, which you can generally decline to receive. The applications that seem most complete, or multi-faceted, try to make you feel as if you're joining an organization or a community that you can identify with personally, not just using a program on a device, all by yourself.

As part of setting up your account, an application may ask you to create a list of "friends" you want to share information with, either from the contacts list or address book on your device or via your Facebook account. Another alternative is to create a contacts list of names and email addresses within the app.

Some applications have a feature that lets you keep—and share—a diary, for example, of your diet, exercise or pregnancy, which may include the ability to add photos.

As you use an application that collects personal information, you build a cumulative body of data in a variety of ways. You may just keep up with the program by adding new data about food/calorie consumption and weight loss, for example. You could regularly investigate medical diagnoses by clicking through symptoms, conditions and treatments. You could respond to messages an application emails or communicates on-screen, taking actions the app promotes or clicking on ads. With each application, we looked at users' ability to access, modify and delete at least the record of personal, self-entered information they create while engaging with the app.

6.5 Analyzing the information

In order to organize the subjective and objective information we collected by reading websites and privacy policies, then downloading, installing and using the apps, we created a spreadsheet to organize the data.

First we identified the elements we considered necessary for a complete privacy

policy:

- What data is collected.
- The means of collection, either by user entry or tracking devices.
- How the data is used and with whom is it shared.
- What information choices and controls users have, including consent, access and ability to correct and delete user-entered information.
- Caution that information users make public is not protected.
- Caution that links to third-party information are not protected by the developer's privacy policy.
- Notification about age restrictions on using the app; that is, not for use by children under 13.
- How the developer protects the privacy and security of information that it collects, stores and transmits.
- Contact information for questions and complaints.

We then broke these down into subcategories concerning notice, collection and treatment of personal and non-personal information, types of third-party uses, and various user options for controlling their data. We broke out different data security practices, such as data encryption and use of secure socket layer (SSL) for encrypted network connections. And we included a checklist of all the permissions that go with iOS and Android applications. Not all apps require all permissions, although many appear to require permissions in excess of what seems necessary just to use the app, for example, making an app part of a device's start-up process or setting the app to be always on (which drains a device's battery).

We eventually built a spreadsheet that measured the apps by more than 150 data points, some as subjective measurements and others as objective. Sometimes the answer to a question was a simple yes or no. The rating in categories related to the risk to the privacy of personal information in using an app was done on a 0-9 basis, which allows for too many gradations of interpretation and in hindsight was probably a mistake. We found that it was easier to report our analysis based on low/medium/high segmentations, so this is how we translated the 0-9 rankings:

- 0 = no risk
- 1-3 = relatively low privacy risk in using an application
- 4-6 = medium risk
- 7-9 = high risk

The full list of spreadsheet criteria, without the ratings and names of the applications, is available in the Evaluation Spreadsheet that accompanies this project.

7. Results

An important goal of this project was to give consumers a basis for assessing the privacy risks inherent in using mobile health and fitness applications, by posing some questions they might want to consider before installing and using the apps on smartphones and tablets. The consumer education goals are met in several project deliverables listed below:

- This consumer-oriented report
- A Fact Sheet for the Privacy Rights Clearinghouse website aimed at consumers
- An e-mail alert to the Privacy Rights Clearinghouse mailing list that briefly summarizes the Fact Sheet information
- A webinar presentation on the project findings.

Another goal of the project was to assess app developers' information practices based on their privacy policies. This is discussed in detail in the technical report, which looks at what developers tell consumers about their use and collection of information compared to what developers are not telling consumers (or not telling them in a meaningful, understandable way) and what they are actually doing.

The most valuable outcome of the project's technical assessment of mobile health and fitness apps, however, is the technical report—a "Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications." The report identifies the riskiest information practices that developers commonly use, along with the HOW TO that advises developers on methods for building privacy protections into their applications.

The Evaluation Spreadsheet lists the 150 criteria used by the project technologist and project manager to evaluate the apps.

7.1 Findings from consumer/user-level analysis, from the technical analysis, and from the risk analysis for free and paid applications

Table 1. Mobile Health and Fitness Applications Privacy Policy Data

Table 1 lists some of our non-technical, consumer-level analysis about the existence of, and contents of, the privacy policies of the 43 free and paid applications we analyzed:

	Free apps	Paid apps
Privacy policy found in app or on developer's website	74%	60%
Uses non-personally identifiable information for analytics	70%	70%
Notifies users that information they make public (e.g., in chat groups, by sharing with friends or linking to social media) is not protected	57%	15%
Notifies users that their privacy policy does not apply to third-party links	48%	25%
Notifies users that they might share data with advertisers	52%	30%

Table 2. Mobile Health and Fitness Apps Data-Handling Practices The technical analysis to determine what actually happened with data the apps collected is revealed, in part, in Table 2. For more such analysis, read the complete technical report.

	Free apps	Paid apps
Sends data to someone not covered in privacy policy	39%	30%
Connects to third-party sites as part of basic functionality	48%	40%
Encrypts all connections to the developer	13%	10%

Table 3. Aggregate Analysis of Quality of Privacy Policy for Free and Paid Applications

Table 3 represents highlights of the aggregate results of our analysis of free and paid applications' privacy policies.

	Free apps	Paid apps
Provides links to website privacy policy from within app	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 found on store, on developer's website, in app, or in privacy policy	57%	100%
Contact info: in-app option for contacting developer	48%	50%
Contact info: web-based form outside of app	43%	20%
Can opt out of developer/vendor sharing data with 3rd parties	57%	30%
Can opt in to data sharing with 3rd parties	35%	30%
Specifically addresses children's privacy	61%	20%

Based on those and other data points, we found that of the apps tested, for which we were able to enter answers in the spreadsheet, the subjective risk average for 23 free applications was medium high (7.4 score out of a maximum of 9 of all the apps' risk factors combined). We found the 20 paid applications that were subjectively assessed to pose a medium risk to users (6.05 score out of a maximum of 9).

Some findings of note, in addition to those included in the previous tables:

- Of the mobile health and fitness apps we analyzed, we found that 83% of the free apps and 60% of the paid apps send data to the developer. However, only 13% of the free apps and 10% of the paid apps encrypt all of their communications with SSL. The rest send some or all of the data in the clear over HTTP.

- Of the apps we analyzed that send personally identifiable information over the Internet (PII, such as name, email address, address, geo-location, etc.), only 53% of the free apps and 44% of the paid apps transmit that PII encrypted.

- Of the apps we analyzed, 48% of the free apps and 40% of the paid apps send data to third-party sites as part of their core functionality. Of these, no free apps and only a single paid app encrypted all of the communications with SSL. The rest send some or all of the data in the clear over HTTP**.**

- None of the apps we analyzed that use third-party advertising services send usage data over an HTTPS connection (encrypted SSL). Each app we analyzed sends the data to advertisers in the clear over HTTP.

- Insecure data storage is also a serious problem. 83% of the free mobile health and fitness apps we analyzed store data locally on the device and none encrypts the stored data.

7.2 Technical results for free and paid applications

Technological risk assessment of mobile health and fitness applications was particularly valuable, because it was able to show what developers' actual information practices are, as opposed to what their privacy policies say they do.

7.2.1 Assignment of risk levels

Technology risk levels were assigned based on the privacy risk of using the app, including what data it collected, stored and/or transmitted. 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, DOB, ZIP code

Medium risk (4-6)—enhanced privacy risk to PII; email, first name, friends, interests, weight, potentially embarrassing/sensitive information

Low risk (1-3) —moderately low risk; anonymous tracking, device info, a third party knows the user is using a mobile medical app

No risk (0) — no PII or health-related information

7.2.2 Overall technology assessment of risk: high, medium and low

The cumulative risk assessment results of the technology analysis of all 43 apps tested showed the following:

- 40% of the apps (17 of 43) were high risk (risk levels 7-9)
- 32% of the apps (14 of 43) were medium to high risk (risk levels 4-6)
- 28% of the apps (12 of 43) were low to medium risk (risk levels 1-3)
- none of the apps were evaluated to be no risk (risk level 0)

7.2.3 Primary technological causes of risk

The technical analysis looked at three primary causes of privacy risks in application development that, if addressed in building the apps, would make them more private and secure for users. These are included in both the technical report for this project, titled "Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications," and in a "Privacy HOW TO for Mobile App Developers," which is intended as a guide for developers to help build privacy into their applications.

We identified the three main technical causes of informational privacy risks in mobile health and fitness 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, free or paid, 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), as would be expected. The reason for the discrepancy is that 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. Data with privacy-invasive details of usage behavior (e.g., 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?) is generally sent over HTTP, not HTTPS. This data can potentially be collected into 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 use third-party analytics services.

8. Conclusions

We must conclude from our study that information privacy is not currently a priority for developers of mobile health and fitness applications, even though building technical protections into apps is not difficult. Users' interest in the benefits of some applications, particularly those that help motivate them to diet and exercise, may trump their concerns about what happens to personal information apps collect from them. Nonetheless, users of mobile health and fitness apps should understand that mobile app usage is another conduit for collection and distribution of personal information, some of it quite sensitive, into the unregulated domain of public information.

8.1 Privacy policies vs. privacy practices

To revisit one our major findings, 74% of the free apps and 60% of the paid apps we reviewed had a privacy policy either in the app or on the developer's website. This means that 26% of the free apps and 40% of the paid apps had no privacy policy at all.

During our technical analysis we found that among the apps with a privacy policy, the majority of technical practices that we considered a risk to users' privacy were not accurately disclosed or described in a way that would enable non-technical users to understand what is actually going on. Even users who read most of the privacy policies we found would be surprised to learn what data is actually collected, transmitted, and shared with unidentified third parties.

For example, while almost all privacy policies say they protect the privacy and security or integrity of your data, we found that many did not use the most basic security for data transmission: HTTPS, rather than HTTP.

The project's technologist, who read privacy policies along with testing applications' data collection and security practices, observed that there was generally an inverse correlation between how detailed a privacy policy was and the privacy risk of using the app. Put another way: the more detailed an app's privacy policy was, the more privacy invasive its actual information practices tended to be. Over our sample of 43 apps, this was observed to be the rule, rather than the exception. We acknowledge that although this observation may be subjective, it nevertheless derives from an intensive technical analysis of how the applications we analyzed actually operate.

8.2 How can consumers decide whether or not to use certain mobile health and fitness applications?

As the rapidly expanding market for mobile applications shows, users have already decided to use the apps *en masse*. Based on our analysis and findings, we must caution users about the risks of putting personal information that directly reveals their health status into the unregulated stream of data that mobile apps collect and disseminate in a variety of ways. Accordingly, we offer the following advice:

- 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—in an application-based chat group.

- 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 to those third parties.

- Try to limit your input of personal information and exercise caution with whom 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.

- If you can figure out the permissions, possibly with the help of someone more technologically savvy, turn off the ones that appear to be unnecessary to the functioning of the app. For example, you may want to disable location services, or the always-on setting, which eats up battery charge.

- Although it's difficult to evaluate the validity of a great deal of information on the Internet, try to assess how genuine and credible the developer of an app is by 1) whether the app has an associated website; 2) the quality and content of information on the website, including the privacy policy; 3) whether there is contact information and it actually gets a response from the developer; and 4) what you can learn about the app or the developer in the media.

- If you're sensitive about your information privacy, avoid applications that embed advertising or that seem to be primarily about selling products related in some way to the purpose of the app.

- For relatively less exposure of personal information, we recommend only using paid health and fitness apps.

- Some apps give you the option of exploring the features without entering personal information. Take advantage of this opportunity when it's offered to decide whether you want to proceed with the using the app at all.

9. Related Developments

There are currently two ongoing processes that affect mobile devices and mobile applications. One is a U.S. Food and Drug Administration guidance, which, while not the same as a regulation, may have an impact on future development of health and fitness applications. The other, the National Telecommunications and Information Administration's (NTIA) multi-stakeholder process, is an effort to get device and application developers to agree to greater transparency and more consumer control of data collection practices.

9.1 FDA guidance on medical devices

The Food and Drug Administration recently published the "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff." The final guidance, after comments on the draft have been taken into account, should be out before the end of 2013.

The FDA's guidance for mobile health application developers is an effort to achieve the goal of regulating a rapidly growing industry while not stifling development. Some developers want the Department of Health and Human Services (HHS) to stop the FDA from releasing a final guidance until an ONC (Office of the National Coordinator of Health Information Technology, part of HHS) workgroup that is developing a risk-based framework for health IT regulations finishes its work. Others want the guidance now so investors in medical devices and mobile health applications will have the clarity they need to put money into development.

What the FDA's guidance does not do is resolve a major question concerning mobile applications; that is, what the difference is between a disease-related app and a wellness-related app. It seems clear enough that a diet app with a calorie tracker, food diary, barcode checker and recipes is a wellness app. But if the same app is marketed to people with diabetes as a way to manage their condition, does that make it a medical device, and therefore subject to FDA regulation?

Another question the current guidance won't deal with is whether an application that connects a medical device—like a glucose meter—to a smartphone or tablet is an accessory to a medical device and subject to regulation.

9.2 The National Telecommunications and Information Administration (NTIA) multi-stakeholder process

The NTIA multi-stakeholder process is an ongoing effort "to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data." (http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency) In other words, it intends to give developers that collect personal information from mobile applications some non-binding guidance about what they should tell users about their data collection and sharing practices.

Companies that comprise the mobile industry have a strong interest in being able to collect as much personal data as possible. Privacy advocates are also participating in the process, and their interest is in having more user controls on the collection and use of personal data and greater transparency about both. An agreement on short-form privacy notices is expected to be the major result of the NTIA's multi-stakeholder process.

Regarding health and fitness apps of the kind reviewed in this project, the current draft of voluntary guidelines would ask developers to notify users if an app collects identifiable "Health, medical or therapy information." The definition includes "health claims and Information used to measure health or wellness," and would certainly apply to most of the apps reviewed in this study.

Both quotes, above, are from the NTIA's June 13, 2013, draft "Code of Conduct to Promote Transparency in Mobile App Privacy Practices Through Short Form Notices."

Developers who adhere to the code would also tell users if they share user-specific data with:

- Ad networks; that is companies that display ads through apps.
- Mobile service carriers.
- Consumer data resellers, also known as data brokers, which are in the business of selling consumer information in order to target individuals with ads for products and services, among other things.
- Data analytics services, or companies that analyze how people use apps, what they link to from them and generally, what their behavior is with regard to an application. Developers use this information to

improve their apps and the marketing of their apps, among other things.

- Government: includes any sharing of data with the government except where required or expressly permitted by law.

- Operating systems, which can include the companies that power a mobile device (iOS and Android, in this study), their app stores, and companies that provide common tools and information for developers about app consumers.

- Other apps of companies that the consumer may not have a relationship with.

- Social networks, to which users may connect from an app and which facilitate information sharing.

For up-to-date information on the multi-stakeholder process, see the NTIA's website: http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

The draft referred to in this study, is titled "Code of Conduct to Promote Transparency in Mobile App Privacy Practices Through Short Form Notices" (June 13, 2013). It can be found on the NTIA website, along with more information about the multi-stakeholder process.

For more information about this project and its findings, please contact:

Beth Givens, Director, Privacy Rights Clearinghouse, bethg@privacyrights.org

This project was funded by the California Consumer Protection Foundation. We are grateful for its support.