Digital Health is Public Health:
Consumers' Privacy & Security in the Mobile Health App Ecosystem

By Holden Williams, Ginny Kozemczak, and Dan Kinney
December 15, 2021

Over the past two years, mobile digital health technologies have become vital worldwide public health tools that provide a critical lifeline to care. This transformation has laid bare the stark limitations of the analog-era consumer protections that govern the use of these technologies.

As the U.S. government pushes for greater data portability to give patients and their providers powerful new resources to manage their health and wellness, a new wave of health apps are exploding onto our screens. Patients who believe that decades-old laws like the Health Insurance Portability and Accountability Act (HIPAA) provide protections for the intimate details of their health and wellbeing that are collected by apps may be surprised to learn that this data collection and sharing falls into a nebulous gap in consumer protections that may leave them vulnerable. Most of the new apps that patients use to monitor their sexual and reproductive health, mental health, fitness, and weight loss are instead governed by a woefully inadequate patchwork of rules enforced by a range of federal and state agencies, from the Federal Trade Commission and state attorneys general to emerging rules in states like California, Virginia, and Colorado. Additionally, platforms like Google and Apple are thrust into dual roles as merchant and privacy beat cop, setting and enforcing many of the specific rules developers and publishers must follow to offer their apps on the Google Play Store and the iOS App store.

With support from the Rose Foundation, the International Digital Accountability Council (IDAC) launched an investigation of digital health apps to assess consumer protection risks in the digital health marketplace. Our technologists investigated health-related apps that utilize the most sensitive personal information. In partnership with Good Research and App Census, IDAC examined the privacy policies for 152 of these apps and then used sophisticated forensic techniques to examine the data flows from the apps to outside third parties.

Our investigation found that most of these apps are observing the letter of the laws and platform terms that they are required to follow. However, some widely-used apps fail to meet even basic platform requirements because they send unencrypted user data, have inadequate or missing privacy policies, or collect granular information about user location without adequate explanation. Additionally, several

apps appear to transmit user data to endpoints in countries such as Russia and China with weak data protection laws and poor human rights records.

The majority of apps investigated have questionable practices and disclosures around third-party data sharing, illustrating a clear mismatch between current legal protections and the widespread collection and sharing of sensitive health information.

Even when apps carefully follow existing rules, most users have little visibility into how their information is collected or shared. When it comes to sharing our most health sensitive data, our laws place a strong emphasis on the notion of notice and consent. But notice often means that apps carefully include a vague and legalistic statement about data collection and sharing; and consent often means that a user clicks through a jargon-filled document without reading or understanding the disclosures that are being made.

This report outlines our investigative findings and the broader ecosystem concerns that are emerging rapidly as our digital privacy health becomes more intrinsically tied to our public health. We also provide a set of best recommendations for handling sensitive health data and how to appropriately address these concerns in ongoing policy conversations at the federal and state levels.

Methodology

IDAC investigated 152 Android health apps that were available in the Google Play Store as of November 10, 2021. These apps were selected using keyword search results and classified into three categories: femtech, mental health, and fitness & weight loss.

We conducted a detailed analysis of the apps and all associated privacy policies. We then conducted both automated static and dynamic analysis of the data flows of each app. From this initial analysis, we identified 46 apps with problematic privacy or security practices and launched a deeper, second-level analysis. IDAC partnered with Good Research to conduct manual dynamic tests on each of these apps.

Our tests allowed us to observe a variety of behaviors associated with the collection and transmission of personal information, including the types of personal data these apps collect, to whom the data is being sent (looking with particular interest to transmission to third-parties), the types of permissions requested, the types of Software Development Kits (SDKs) present in the apps, and other data transmissions.

We then compared the findings of the observed behavior of these applications with what was stated in the respective apps' privacy policies and what is disclosed in the user interfaces of the applications.

A thorough explanation of our methodology and our full results are available in the Appendix.

Automated Testing

The automated testing consisted of static and automated dynamic tests. Static testing scans each application for code to identify the types of software development kits (SDKs) present and permissions used in the apps. The dynamic tests involved a process of running scripts to interact with an app by sending a series of stochastic actions (i.e., random taps and swipes) to simulate user interactions. We ran several automated tests on each app for approximately three minutes throughout the investigation.

Manual testing

In our deeper, second-level testing, our investigators conducted dynamic manual analysis tests on 46 Android apps to determine how they operate in real time. Using Android devices, we installed the apps and interacted with them as a typical user would, trying to use as much of the app as possible to test all potential subsections and screens within ten-minute tests. We ran our analysis on the network traffic and additional operating system information that was generated while we were interacting with the apps. From these results, we were able to observe a variety of behaviors associated with the collection and transmission of personal information, to whom the data is being sent, and other data transmissions.

Table of Contents

I. Key Findings

Our investigation revealed areas for improvement for app developers and companies. We have identified apparent violations of Google Play policies and some obvious bad practices.

A. Two apps appear to violate Google Play's secure transmissions policy, exposing personal information and identifiers

We observed multiple apps sending unencrypted transmissions. These apps did not use cryptographic protocols designed to provide communications security over computer networks such as transport layer security (TLS). Best developer practices, especially those that relate to sensitive health information, require encryption of all communications from the device to the destination.

One app, *I'm Pregnant*, sent unsecured transmissions that included personal information including users' emails and phone numbers.

App Name	Transmission Data	Endpoint
I'm Pregnant - Pregnancy Week By Week	User's email and phone number	First Party

Two apps, *Period Tracker Petal, Period & Ovulation Calendar* and *Daily Yoga*, sent unsecured transmissions of the Android Advertising ID. We did not observe personal data in these transmissions. In the case of *Period Tracker Petal, Period & Ovulation Calendar*, the unsecured transmissions were to a third-party endpoint, MoPub. The *Daily Yoga* transmissions were unsecured first party transmissions.

App Name	Transmission Data	Endpoint
Period Tracker Petal, Period & Ovulation Calendar	AAID	MoPub
Daily Yoga | Fitness Yoga Plan & Meditation App	AAID	First Party

Several apps sent unencrypted transmissions that did not appear to include any personal information or advertising identifiers: Femometer - Fertility Tracker, Lunar - Period Tracker & Ovulation Calendar, and Psytests.[1]

B. One app appears to have violated Google Play Ads policy by failing to state the purpose of location data collection.

[1] *Our investigation covers the observed behavior of these applications over 10 minute spans. It is possible that we did not capture all the possible information that is exposed by these apps sending unencrypted transmissions.*

In order for an app to use location data for advertising purposes, it must meet specific requirements, including providing users with the purpose for the collection of location data in its privacy policy or with in-app disclosures.

Our findings indicate that one app, PsyTests, potentially violates this Google Play Ads policy. During our manual testing of PsyTests, we captured multiple transmissions of location data to advertising and analytics services. These included: a.appbaqend.com, amazon-adsystem.com, api-us.bidmachine.io, and smaato.net. At the time this report was published, PsyTests did not provide a working URL link to its privacy policy on the Google Play Store.[2]

Additionally, the app appears to fail to meet Google's requirement that app developers "should never request location permissions from users for the sole purpose of advertising or analytics." The app does not provide an explanation of the purpose of the use of location data, and we could not identify any apparent features requiring the use of location data.

C. Two apps appear to violate Google Play policies by failing to provide a privacy policy.

Two apps did not provide users with a privacy policy. In apparent violation of Google Play policies, the following apps did not have a privacy policy linked in the Google Play Store or in the app itself:

- Ladytimer
- PsyTests

Our investigators attempted to access the privacy policies for both of these apps in the Google Play Console and were met with a 404-error due to an invalid URL link. Through an online search, we were able to find Ladytimer's policy.

Additionally, the app Menopause: All Information, has a privacy policy from a sample policy document without specific information about the app. The first line of the app's privacy policy has placeholder language "YOURDEVELOPERNAMEHERE." We found other placeholder values throughout.

D. Some apps are sharing information with third parties located in countries with weak data protection laws and a history of human rights abuses.

Our research raised concerns about international data flows to China and Russia, countries with weak data protection laws and a history of human rights abuses.

In June 2021, President Joe Biden issued an Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, taking steps to address data collection through apps that may share sensitive information to endpoints in countries that have been designated as foreign adversaries by the Secretary of Commerce. As defined by the Executive Order, sensitive health information about U.S. citizens includes personal health information.

---

[2] *"Use or collection of permission based device location data for advertising purposes must be clear to the user and documented in the app's mandatory privacy policy, including linking to any relevant ad network privacy policies addressing location data use." https://support.google.com/googleplay/android-developer/answer/9857753. There is a 2019 archived version of the privacy policy that we found through a web search.*

The following four apps transmitted data to companies in Russia:

- amma Pregnancy & Baby Tracker
- Breastfeeding Newborn tracker, pump and baby diary
- I'm Pregnant - Pregnancy Week By Week
- Mood Tracker Journal. Mental Health, Depression

Three of these endpoints are owned and operated by Yandex, a Russian technology company. The fourth is operated by TimeWeb.com.

Three apps transmitted data to companies in China:

- Daily Yoga | Fitness Yoga Plan & Meditation App
- Femometer - Fertility Tracker
- Period Tracker Petal, Period & Ovulation Calendar[3]

These endpoints are operated by Qiniu, Tencent QQ, and 3g.cn (GOMO developer of Period Tracker Petal). The Femometer developer is based in China and received first-party data transmissions.

[3] As previously noted, Daily Yoga and Period Tracker Petal are sending unencrypted transmissions to companies based in China.

II. Health App Ecosystem Trends

According to our research, analytics and advertising monetization is pervasive in the health app ecosystem. There is a clear mismatch between the relevant legal protections and the very sensitive purposes for which people now use their mobile devices.

Many apps that collect sensitive data regarding sex, ovulation, pregnancy, mental health, weight loss and fitness appear to utilize business models centered on sharing user data with third parties that use that data for advertising and analytics. Current laws and platform terms that are based on a notice-and-consent model may not adequately inform users about the risks and tradeoffs involved in sharing highly sensitive health-related data with these apps.

Greater consumer education would help effectuate the purposes of new state-level laws such as CCPA. But, ultimately, stronger baseline protections are required.

A. Failure to address how health information is collected results in inadequate privacy policies.

In the United States, outside of HIPAA, there is no one law that defines what constitutes sensitive health information. But in HIPAA-free spaces, the lack of any definition for this category of data means that entities are not obligated to afford it any special protections.

Our investigation revealed that the disclosures provided by the privacy policies that were linked in the Google Play Store varied widely. In most cases, these policies failed to contain sufficiently detailed information about the specific information that is collected and used.

While a small number of apps contain privacy policies that explicitly detail how they define health data[4], the majority do not disclose that they collect personal information.

Of the 152 apps we analyzed, 125 (82%) of those apps disclose that they collect personal information. Of that group, only 66 (54%) of those disclosed and addressed the collection of health information directly:[5]

- Femtech: 26 out of 49 apps (55%)
- Mental Health: 12 out of 40 apps (30%)
- Fitness and Weight Loss: 29 out of 36 apps (81%)

B. Collection of location data can leave users vulnerable to inappropriate tracking

[4] Two positive examples may help explain what we mean by providing information about how a policy defines health data. The femtech app Flo defines "Health and Well-being [personal data]" to include the following: weight, body temperature, menstrual cycle dates, details of pregnancy, any symptoms, and "[o]ther information about your health (including sexual activities), physical and mental well-being, and related activities, including personal life." The mental health app Bearable defines health data around information about the user's moods and daily activities.

[5] We determined if an app defines health data by: a) analyzing disclosures for the inclusion of the word "health", b) if the policy reasonably described health data in the context of the category, or c) if the app stated the use of Google Fit.

Location data is particularly sensitive because of the amount of information it reveals about a user, including their hobbies, lifestyle choices, and habits. When paired with health data, location data becomes even more sensitive.

In general, health-related apps should only collect location information when the collection and use of this information relates directly to the functionality of the app, such as an app that records a user's jogging route or a specific workout.

There are multiple ways to infer a phone's location without using the location services. Location data can be inferred from various different data and identifiers collected without explicit disclosure. The collection of longitude and latitude from device sensors using the ACCESS_FINE_LOCATION permission is very detailed and granular, and provides enough precision for turn-by-turn navigation apps. This information can be accurate to within 10 feet.

We identified multiple apps requesting a user's precise location[6]:

- 21 fitness apps (see Appendix B – Apps Requesting Fine Location).
- 14 femtech apps
- Six mental health apps

While the collection of location data makes sense in many fitness and weight loss apps, it is questionable why an ovulation tracker or counseling app needs access to precise user location.

We analyzed both the user interface/ user experience (UI/UX) and privacy policies of these apps to better understand the purposes for requesting access to users' devices' precise location. Nine of the femtech apps revealed in the privacy policies that users' location data is shared with advertisers, a concerning practice due to the lack of obvious use cases for location data and the possible extent of location tracking.

C. Many apps share data with third-party advertising, analytics, and other monetization services

We observed many health apps sharing advertising identifiers with third parties, which we identified as any entity that is not the developer of the app. According to researchers, advertising identifiers can be used to create digital profiles that can track consumers across services and devices.

Our researchers compared claims made in privacy policies against actual data flows to third party endpoints. Of the 46 health apps IDAC chose for deeper analysis, 39 were not fully transparent about third party data sharing.

The table below demonstrates which endpoints receive information, and whether or not the app privacy policy includes a disclosure about which third parties receive information. In some cases, we were able to observe communication between the app and these third parties, but not the specific content of the transmission.

---

[6] In our investigation we used automated testing to identify apps that have code to request access to a user's precise location data. This information is also provided in the Google Play Console of the app under the section "Additional Information" subsection "Permissions."

App Name	Third Party Data Sharing (analytics, advertising, and other monetization endpoints)	Disclosed in Privacy Policy?
280days: Pregnancy Diary	amazon-adsystem.com, doubleclick.net, facebook.com, googleadservices.com, and mopub.com	No
amma Pregnancy & Baby Tracker	2mdn.net (doubleclick), adapty.io, adjust.com, adsmoloco.com, amplitude.com, applovin.com, appsflyer.com, doubleclick.net, facebook.com, flurry.com, googleadservices.com, liftoff.io, mixpanel.com. Mopub.com, and report.appmetrica.yandex.net	No
Balance: Meditation & Sleep	amplitude.com, braze.com, facebook.com, revenuecat.com, segment.io, and singular.net	No
Bearable	facebook.com, mixpanel.com, revenuecat.com, and segment.io	No
BetterMe	appsflyer.com and facebook.com	Yes
Breastfeeding Newborn tracker, pump and baby diary	doubleclick.net, googleadservices.com, and report.appmetrica.yandex.net	Yes
	adcolony.com and applovin.com	No
Calm	amplitude.com, appsflyer.com, branch.io, facebook.com, and iterable.com	No
Daily Yoga	doubleclick.net and facebook.com	No
Depression Therapy	analyticscounsel.com, appsflyer.com, and ayetstudios.com	No
Fabulous	facebook.com	Yes
	adjust.com and amplitude.com	No
Femometer	appsflyer.com, qq.com and weibo.com	No
Flo Period Tracker	appsflyer.com	Yes
Eve Period Tracker - Love, Sex & Relationships App	adsmoloco.com, amazon-adsystem.com, appsflyer.com, branch.io, doubleclick.net, facebook.com, googlesyndication.com, postrelease.com, and yahoo.com	No
GLOW. Ovulation & Period Tracker	adsmoloco.com, amazon-adsystem.com, appsflyer.com, doubleclick.net, facebook.com, googlesyndication.com, kochava.com, liftoff.io, and postrelease.com	
GLOW. Pregnancy & Baby Tracker + Baby Registry App	amazon-adsystem.com, appsflyer.com, doubleclick.net, doubleverify.com, facebook.com, googlesyndication.com, and postrelease.com	
GLOW. Baby Tracker & Feeding, Diaper, Sleep Log	adsmoloco.com, amazon-adsystem.com, appsflyer.com, doubleclick.net, doubleverify.com, facebook.com, googlesyndication.com, kochava.com, liftoff.io, and postrelease.com	

Headspace	branch.io, braze.com, mparticle.com, and optimizely.com	No
I'm Pregnant	none	Yes
Intellect	mixpanel.com and revenuecat.com	No
Ladytimer	doubleclick.net and branch.io	No
Lose Belly Fat at Home - Lose Weight Flat Stomach	doubleclick.net and facebook.com	Yes
	adsmoloco.com	No
Lunar	applovin.com, appsflyer.com, facebook.com, kayzen.io, liftoff.io, and unity3d.com	No
Menopause	facebook.com and flurry.com	No
Mind Journal	doubleclick.net	Yes
Mindvalley	facebook.com	Yes
	appsflyer.com, apptimize.com, braze.com, elula.com, revenuecat.com, and segment.io	No
Mood Tracker Journal	report.appmetrica.yandex.net	Yes
My Days X - Ovulation Calendar & Period Tracking	cuebiq.com, doubleclick.net, facebook.com, google-analytics.com, and googleadservices.com	Yes
	amplitude.com, supersonicads.com, and unity3d.com	No
Noom	branch.io, facebook.com, and mixpanel.com	No
ParentLove	branch.io, doubleclick.net, facebook.com, and googleadservices.com	No
Peanut	branch.io and facebook.com	No
Period Tracker Petal	appsflyer.com, facebook.com, and mopub.com	No
Pregnancy Tracker + Countdown to Baby Due Date	adjust.com, adsmoloco.com, amazon-adsystem.com, appsflyer.com, doubleclick.net, facebook.com, scorecardresearch.com, and localytics.com	No
Pregnancy Tracker	doubleclick.net and googleadservices.com	Yes
Premom Ovulation App	appboy.com (braze), appsflyer.com, and facebook.com	Yes
PsyTests	adjust.com, amazon-adsystem.com, appbaqend.com, applovin.com, bidmachine.io, criteo.com, doubleclick.net, googleadservices.com, dspunion.com, and smaato.net	No (no privacy policy)
Replika: My AI Friend	adjust.com	No

	amplitude.com and facebook.com	Yes
Sanvello	branch.io, braze.com, and facebook.com	No
Simple Habit	branch.io and braze.com	No
	facebook.com and segment.io	Yes
Sweat	appsflyer.com, braze.com, emarsys.net, and facebook.com	No
Ten Percent Happier - Meditation & Sleep	amazon-adsystem.com, amplitude.com, appsflyer.com, apptimize.com, branch.io, braze.com, and localytics.com	No
The Tapping Solution	amplitude.com, appsflyer.com, apptimize.com, branch.io, braze.com, facebook.com, and google-analytics.com	No
theAsianparent: Track Pregnancy & Count Baby Kicks	doubleclick.net,, googleadservices.com, and googlesyndication.com,	Yes
	facebook.com, kochava.com, moengage.com and webengage.com	No
UP!	none	Yes
Muscle Booster Workout Planner	amplitude.com, appsflyer.com, branch.io, and facebook.com	Yes
Wysa	branch.io	Yes
Youper - Mental Health	adjust.com, mixpanel.com, and revenuecat.com	No

"Disclosed?" signifies if the privacy policy names the third-party service. Analytics, advertising, and other monetization endpoints were determined to be so on a case-by-case basis. Most of these endpoints are the result of an SDK or tracking cookie. Most of these transmissions included the user's AAID. App names are abbreviated where needed.

The disclosures and sharing we observed varied significantly.

- In two of the 46 apps, we did not observe any third-party data sharing.
- Five of the 46 apps listed all of the third-party endpoints we observed.

In the remaining 39 apps, we observed transmission of users' advertising identifiers to at least one third party endpoint that was not disclosed in the app's privacy policy.

In some cases, the apps named some analytics and advertising services, but failed to state all the third-party services observed in our investigation.

- In the Headspace privacy policy, for example, there is a disclosure about the use of third-party services. Google Analytics is directly mentioned. In addition to Google Analytics, our investigation revealed that Headspace also transmitted the user's AAID to branch.io, braze.com, and mparticle.com. We also observed communication with optimizely.com. All of these third

parties are advertising and analytics services. None of these endpoints are disclosed in Headspace's privacy policy.

Even when these apps explain their practices in the fine print of privacy policies and comply with the letter of the law and applicable platform terms, aggressive data collection and sharing practices raise public policy concerns that deserve greater attention — especially with respect to categories of health data that are particularly sensitive such as sexual wellness, reproductive health, mental health, weight loss, and fitness.

D. Simultaneous transmissions of persistent and resettable identifiers can lead to a practice we call "shadow profiling."

Throughout our investigations, IDAC has observed a disturbing trend of apps organizing and linking information gathered through unique identifiers, a practice that we refer to as "shadow profiling."

In order to monetize users' personal information through third party profiling and advertising, many mobile apps collect multiple identifiers without informing users or offering them a choice. Even when users take advantage of privacy-enhancing features that allow them to reset the identifiers that uniquely identify them, shadow profiling can allow third parties to re-identify the user and opens the door to tracking users over time and across devices without user consent.

Our investigation found several apps transmitting users' identifiers to third party analytics and advertising companies. While our research shows the simultaneous transmission of permanent and advertising identifiers, we cannot definitively confirm that these identifiers are connected, or bridged, by the developer or a third party.[7]

Of the 46 apps we analyzed, we observed 28 sending multiple identifiers to third parties. This includes many popular health-related apps.

- The weight-loss app Noom with over 10 million downloads, transmits users' Android ID and Advertising ID to Branch.io, an analytics company.
- Calm, a widely-used meditation app, sends identifiers to Amplitude and Iterable, another two companies providing advertising and analytics services.

Google Play recently took a positive step and updated its User Data policy to prohibit linking persistent device identifiers with other personal and sensitive data or resettable device identifiers. The new policy went into effect on October 28, 2021. As part of the investigation, we retested all 28 apps during the week of November 9, 2021, and observed all 28 apps still simultaneously transmitting persistent and resettable identifiers.

Endpoint	Apps	PI and Ids
branch.io	Ladytimer Ovulation & Period Calendar	SSAID, AAID
	ParentLove: Baby Tracker, Feeding, Breastfeeding	SSAID, AAID

[7] *The act of bridging identifiers occurs on the server-side of the transmissions. The tools IDAC used in this investigation cannot directly observe what happens to data once it reaches a third party endpoint.*

	Peanut - Meet other Women	SSAID, AAID
	Headspace: Meditation & Sleep	SSAID, AAID
	Noom: Health & Weight	SSAID, AAID
	Sanvello: Anxiety & Depression	SSAID, AAID
	Simple Habit: Meditation, Sleep	SSAID, AAID
	Ten Percent Happier - Meditation & Sleep	SSAID, AAID
	The Tapping Solution	SSAID, AAID
	Workout Planner by Muscle Booster	SSAID, AAID
appsflyer.com	BetterMe: Health Coaching	SSAID, AAID
	Period Tracker Petal, Period & Ovulation Calendar	SSAID, AAID
	Workout Planner by Muscle Booster	SSAID, AAID
revenuecat.com	Bearable - Symptoms & Mood tracker	SSAID, AAID
	Mindvalley: Learn and Transform Your Life	SSAID, AAID
	Youper - Mental Health	SSAID, AAID
segment.io (Twilio)	Balance: Meditation & Sleep	AAID, First name, Email, SSAID
	Bearable - Symptoms & Mood tracker	SSAID, AAID, Email
	Simple Habit: Meditation, Sleep	SSAID, AAID, Name
Metrica (Yandex.net)	AMMA Pregnancy Tracker & Baby Due Date Calculator	SSAID, AAID
	Breastfeeding Newborn tracker, pump and baby diary	SSAID, AAID
	Mood Tracker Journal. Mental Health, Depression	SSAID, AAID

Shadow profiling in health apps is particularly concerning because it is possible that health information can be re-identified by third parties, even if the app only shares “de-identified” or “anonymized” data in the first instance.

Apps that use third party SDKs are not entirely in control of what the third parties do with user data once it is transmitted. These companies may have their own terms of service and privacy policies.

III. Recommendations for App Developers

Safeguarding users' health information requires multi-actor, ecosystem-wide change. Here are some practical steps developers can take to mitigate risks, follow best practices, and promote user trust.

Platforms, too, could enforce these rules on their app stores.

The following recommendations are based on current Google Play Store policies:

1. **Encrypt all transmissions.**
   Developers should use modern encryption methods such as TLS for all transmissions regardless of the content of the transmission.

2. **Enhance privacy policies to include collection and management practices.**
   Privacy policies within health apps should explain in detail how a user's health information is collected and managed.

   At a minimum, apps should be required to disclose third party data-sharing to better protect users from having their data shared and possibly sold without their knowledge. This practice is necessary in order for users to exercise their rights to opt-out of health data collection and sharing.

3. **Regardless of whether there is affirmative proof of back-end bridging, apps should not share persistent and resettable identifiers simultaneously. Apps should also take care in the integration of SDKs.**
   Although users may believe that they can reset their identifiers to protect their privacy — as the privacy protection tools intend — shadow profiling allows companies to potentially circumvent those privacy protections to track users over time.

   When apps transmit multiple identifiers at once to third parties, there is the potential for third parties to recognize and associate a series of numbers with an individual user in order to monitor their online activity over time.

   Developers should scrutinize the SDKs and other third-party services used in an app to avoid engaging in shadow profiling.

   As part of its recent policy changes prohibiting apps from linking persistent device identifiers to other personal and sensitive user data or resettable device identifiers, Google Play now has the ability to enforce the existing Android best practices.

4. **Apps should only collect location data if there is a prominent disclosure and a tight fit between the service offered and the need for user location.**
   If it is necessary for an app to collect location data, such as a fitness app, it must make clear to users why and how this information will be used. For health apps that have no clear need for location tracking, such as an ovulation app or a mental health app, developers should refrain from collecting location data. Additionally, apps should not provide location data to data brokers who then sell users' location information.

5. **Health app developers should utilize Google Fit.**

   Google Fit provides a centralized secure storage for sensitive data that is backed by a reputable party. This means that users do not necessarily have to trust the developer to handle their data, only the platform. Google Fit collects user health data and allows apps to access that data through controlled, secure Application Programming Interfaces (APIs). Google Fit collects and stores users' health data on its own servers so that applications, with the consent of the user, can access this data without needing to collect the data from the user directly. In other words, a health app could utilize personal health data without collecting that data from the user. Perhaps most importantly, Google Fit prohibits the sharing of Google Fit health data with third parties.

Additionally, these recommendations are based on the current and developing public policy and legal landscape:

6. **Apps collecting sensitive data from U.S. citizens should be particularly careful about sharing sensitive user data, such as health data, with companies based in countries identified as "adversaries" by the U.S. Secretary of Commerce.**

   Developers should take steps to prevent the transmission of sensitive data relating to US citizens to third parties that are associated with governments such as China and Russia that have been designated as foreign adversaries pursuant to executive orders issued under the International Emergency Economic Powers Act (IEEPA).

7. **Developers should be required to provide users with opt-*ins* to the collection and sharing of consumer health information.**

   Consumers should have to opt-in to sharing health information. The California Consumer Privacy Act (CCPA) requires that types of personal information are listed in privacy policies, including health data. This requirement effectively makes the collection and sharing of health information an opt-*in*, but it could be made more effective with in-app disclosures.

8. **Developers should consider alternative business models to avoid third party data sharing.**

   We recommend that developers that are not subject to the requirements of HIPAA should avoid monetizing personal data through advertising and analytics. The data that is shared and exposed to third parties is sensitive information users should not have to provide in order to reap the benefits of these applications. Developers might consider subscriptions or first-party, contextual advertising to finance the app.

IV. Comments to Lawmakers and Regulators

In addition to developers and platforms, lawmakers and regulators are key actors in helping to create a more trustworthy health app ecosystem. There are important changes that can be made at the U.S. federal and state levels, as well as how government agencies can work together with civil society groups.

At the national level, the Federal Trade Commission (FTC) stated earlier this year that investigating health apps would be a priority for the agency, citing equity concerns, particularly how issues of privacy and health may disproportionately affect marginalized communities. More recently, the U.S. Senate Commerce Committee held a series of hearings looking at the future of the FTC and how the agency could be more effective in its oversight of health apps. Panelist Ashkan Soltani, now the Executive Director of California's Privacy Protection Agency (CPPA), stated that the definition of health data needs to be broadened to include all data that is "health related." This is especially important when it comes to machine learning and data-driven inferences about users' health. To that end, Soltani suggested that the FTC needs to identify these problems and create rules and standards for safeguarding that information.

The FTC can be more proactive in identifying such problems by working with civil society actors like IDAC, who can identify harms before they manifest and violate users' privacy. For example, in 2020, IDAC conducted an investigation into the popular fertility app Premom, which we believed was violating federal and state laws and the Google Play terms of service, and referred the case to the FTC and the Illinois Attorney General.

Furthermore, organizations such as the Center for Democracy and Technology (CDT) and the E-Health Initiative (EHI) have created the Proposed Consumer Privacy Framework for Health Data, which can raise the bar and ensure best practices for participating entities without the involvement of law enforcement.

Most importantly, however, a federal privacy law is a crucial step to protecting consumers online. There must be privacy rules established at the federal level to include enforceable codes of conduct and robust accountability mechanisms. A federal privacy law should include fundamental principles, such as companies' affirmative duties to engage in ethical practices, companies' obligations to refrain from harmful practices, and consumers' digital rights. Specific rules, including those applying to the handling of sensitive health data, should be fleshed out through multi-stakeholder processes that lead to enforceable codes of conduct.

In the meantime, state privacy laws are a significant player in this space. In the absence of a federal privacy law, the privacy laws in California (CPRA), Virginia (VCDPA), and Colorado (CPA) are some of the strongest in the United States. Both the VCDPA and CPA have opt-in requirements for the use of sensitive data, going beyond the requirements of the CPRA and setting a precedent that is causing companies to re-evaluate their practices to come into compliance when the laws become enforceable in 2023.

In this report, however, we direct our policy comments to the CPRA's new enforcement agency, the CPPA, due to its recent invitation for public comment. The CPRA is positioned to significantly influence companies' privacy practices in the coming years. Most if not all of the developers of the apps we investigated may fall under the CPRA's jurisdiction.[8]

[8] *Cal. Civ. Code § 1798.140.*

Recently, the CPPA invited comments from the public for its rulemaking. In IDAC's public comment to the CPPA, we address several provisions of the CPRA that affect the privacy and security of users' health information. Our comment primarily focuses on the CPRA's new category of personal data, "sensitive personal information"[9] (SPI). SPI includes, among other items, "personal information collected and analyzed concerning a consumer's health," or "personal information collected and analyzed concerning a consumer's sex life or sexual orientation." In line with CDT and EHI's framework, we encourage the CPPA to adopt rules that understand SPI broadly as information that relates to an individual's physical or mental health. We echo Mr. Soltani's concerns that, in the age of machine learning, any rigid definition may be over- or under-inclusive in addressing data-driven inferences.

We also encourage the CPPA to build on its encouraging move away from traditional notice-and-consent models, and instead focus its rulemaking on creating clearer guidelines for minimizing data collection as well as what companies can and cannot do with the data they do collect. These rules would place the burden on app developers, rather than on users, to adopt better privacy-enhancing practices.

Acknowledgements

We would like to express our sincerest gratitude to IDAC's President, Quentin Palfrey, and former Acting President, Leslie Harris, for their leadership of this project. We also would like to thank our partners at Good Research and AppCensus, including Nathan Good, Will Monge, Bobby Richter, Jennifer Chen and Eric Khumalo for their technical research and review. Thank you, as well, to John Verdi, Christy Harris, and Andrew Crawford for their feedback. Lastly, we thank the Rose Foundation for their indispensable support of this project.

[9] *Cal. Civ. Code, § 1798.140.*

Appendices

Appendix A: Detailed Methodology
Appendix B: Apps requesting access to Fine Location
Appendix C: Shadow Profiling
Appendix D: List of femtech apps IDAC investigated
Appendix E: List of mental health apps IDAC investigated
Appendix F: List of fitness & weight loss apps IDAC investigated

Appendix A: Detailed Methodology

App Identification and Selection

The objective of this research was to better understand the mobile app ecosystem, specifically with health data. In the two main mobile app digital marketplaces, the iOS App Store and Google Play, there are two relevant categories for this research: Medical and Health & Fitness.[10] By looking at the apps ranking the highest in these categories in both downloads and grossing, we identified three general subcategories of interest of apps: femtech, mental health, and weight loss/fitness apps.

> **Femtech** apps are specifically for women's health, like period tracking, pregnancy tracking, menopause, and breastfeeding.
>
> **Mental Health** apps are a much broader category. These can range from sleep trackers to meditation guides to video counseling. We did not select apps like Talkspace if the app was stated to be a covered entity under HIPAA.[11]
>
> **Weight Loss** apps are also a broad category and make up a majority of the Health & Fitness category. Weight loss apps can focus on calorie consumption, work out plans, and wearable fitness trackers.[12] These apps typically do not fall under HIPAA protections.

Each category of these apps typically collects health information, particularly the kind that many users would expect to remain private. Femtech health data is more focused on menstrual cycles and pregnancy health. Mental health apps are collecting more information about users' states of mind, daily routines, and moods, which is data that can also be inferred from other sources of information. Weight Loss is more focused around activity and calorie consumption.

We selected 50 apps from each category because we wanted to analyze 100 to 150 apps to understand the life cycle of health data in the Google Play ecosystem. The objective of the selection process was to reflect the process of identification a consumer would go through when they identify apps to download for themselves. The process of identification was slightly different for each of these categories of health apps because of the nature of the Google Play store.

The selection of weight loss apps was fairly straightforward because these apps tended to dominate the Health & Fitness category. We selected 25 apps from the top Free category and 25 apps from the top Grossing categories. Our decision to include apps was in part based on our technical limitations of analysis and what the app description advertised as the purpose of the app.[13] For example, we did not include all yoga apps because they all did not advertise themselves to be beneficial for weight loss. We also excluded apps that require a subscription to an external entity or device, like apps for gym

---

[10] Our research focused on the Google Play store because of the compatibility with our tools.
[11] "This includes medical history, diagnoses, treatments, current medical condition, and use of prescription medications. If you are a US subscriber to Talkspace services, your personal information in our possession is protected health information ("PHI") protected by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), and the applicable provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act. In addition to this Privacy Policy, the HIPAA Notices of Privacy Practices of Talkspace or your Talkspace Provider apply to your PHI." https://www.talkspace.com/public/privacy-policy
[12] We avoided selecting apps that rely on the use of an external device.
[13] In addition to wearable devices apps, we excluded paid apps. The most popular and downloaded apps in the Google Play store tend to be free to download so we do not believe this affected our results for reflecting the apps most used by the average consumer.

membership or workout equipment, like Peloton, because we are unable to test these apps for their intended purposes.[14] Most of the apps in this category were calorie counters and activity trackers. The list of apps we selected can be found in Appendix D.

For the femtech and mental health apps we utilized keyword searches to identify and select 50 apps. Keyword searches are a common tool consumers use to discover new apps. Apps that fall under the term *femtech* and *mental health* are not limited to the Health & Fitness category. In addition to falling into the Medical category, these apps can be found in categories like parenting, lifestyle, and education. There are no dedicated categories for these two types of applications. It is reasonable to assume that if a user is looking for an app to help treat something like depression, they will not want to search through dozens of apps that are unrelated to their problems in these categories.

However, there are also limitations to using keyword searches in Google Play because it is not clear to the user what leads to certain apps being ranked higher than others and what combinations of keywords to use to find the right app. To facilitate our keyword search, we used the App Annie service to mimic searches in Google Play but with more information about what factors Google Play might be considering to generate the results. These factors include: keyword rank, cumulative ratings, and downloads in the past 30 days.[15] The keyword search helped to provide a diversity of apps for each category, but we also made sure to avoid selecting apps with relatively low user bases or bad ratings.[16] The keywords we used for femtech were: "period tracker," "pregnancy," "breastfeeding," "fertility [tracker]," and "menopause." For mental health the keywords were: "mental health," "depression," "anxiety," and "meditation."

We excluded some apps from mental health due to the content of the application such as sleep trackers, noise makers, daily quote generators, vibration apps, and some apps like Talkspace that are considered covered entities under HIPAA. Our objective was to look at health apps in the HIPAA grey-zone, but the borders of this grey-zone were not always clear. Some of the apps we excluded could probably fit in our definition of the HIPAA grey-zone, but were nonetheless excluded for purely research capacity purposes. Another subjective measure we used to exclude some apps were the Google Play metrics for downloads and ratings. Unless the app was in the first five results, we generally excluded apps with low ratings, relatively low downloads (this depended on the subcategory), or if the app was not working.[17]

The app ecosystem is vulnerable to dynamic changes in available applications, thus we decided to oversample applications in these categories. Throughout our research, some apps were removed from the app store, but for the most part the search results and app store ranking remained the same.[18]

Privacy Policy Checklist Questions

Below are the questions that our team used to analyze the privacy policies for each app during the investigation.

---

[14] There was also a trend of apps being miscategorized, such as image editors and games that did not actually have to do with physical health and fitness.

[15] These are imperfect measures, but helpful nonetheless in our research. Searches conducted on August 12 for femtech and August 23 for mental health.

[16] Like any automated process, there are going to be gaps or inconsistencies in the results. The top 10 apps in a given keyword search does not necessarily mean the top femtech apps in that category, and some apps that serve the same functions might not use the same keywords.

[17] The most clear example of this is with the Medela Family: Baby & Pregnancy Tracker | Pum Log app which users reported to have issues installing on their Android devices.

[18] At the time of writing this report some apps have surfaced higher in ranking and some have dropped lower.

- Is there a privacy policy? Does it address the specific app?
- When was the privacy policy last updated?
- Does the app policy disclose that the app collects personal information? Does the privacy policy define the categories of data it collects?
- Does the privacy policy define health data?
- Does the app share data with third parties?
    - Does the privacy policy identify who those third parties are?
    - Does the privacy policy state the purpose for sharing?
- Does the policy disclose where data is stored?
    - If stored remotely, does it disclose where is it stored?
    - Does it disclose how long the data is retained?
- Does the policy disclose its security practices?
- Does the policy disclose that it complies with the CCPA?
    - Does the user have rights of access, deletion, and correction?
    - Can the user opt out of the sale of their information?

AppBot Static and Dynamic Analysis

To identify apps that are engaging in questionable behavior with user data, we used AppBot, a tool developed by AppCensus, to do a first level scan of all the selected apps. AppBot automates static and dynamic testing.

- Static: scanning the app for permissions, SDKs, and other code/program-based information; these does not involved interacting with the application
- Dynamic: interacting with the application to generate normal user behavior

For each app we ran automated tests with three minute long durations on a modified Android device with an Android 9 Operating System. The automated tests simulate a user interacting with an app to trigger different in-app events. These interactions are random, but are sufficiently reliable to generate some basic behaviors of the apps. We ran these tests frequently throughout the investigation to make sure we were working with information from the most recent versions of the apps.

The factors that we used to determine if an app is potentially problematic are as follows:

- Is the app sending unencrypted transmissions?
- Where is the app sending data?
- Is the app transmitting non-resettable identifiers from the device?
- Is the app potentially linking non-resettable identifiers with resettable identifiers?

In addition to using AppBot, we identified a handful of apps for a deeper dive of analysis if the app had a history of legal and regulatory scrutiny. For example, Premom is an app that IDAC previously investigated and discovered bad practices.

Deeper Dive

The second-level of analysis was done in two parts. First, we did a deeper examination of the apps selected with the help of the Good Research team. Then, once we received the results from Good Research, we compared these results with what was found in the first level analysis with AppBot and we took another, more intensive, look at the privacy policies of these apps. In addition, we examined each app's business model to better understand the observed app behavior.

Good Research added to the first level analysis by conducting manual app tests for each of the 46 apps IDAC found to be engaging in potentially problematic behaviors observed by AppBot or from other app analysis. The breakdown of the apps by subcategories:

- Femtech: 21
- Mental: 19
- Fitness: 6[19]

These tests were conducted on the same modified Android devices (Android 9 OS) in the state of California, but instead of random interactions simulated on the device for three minutes, the user explored all the app's features from start up for 10 minutes. When prompted, the user would input fabricated personal information so when we analyzed the transmissions we could identify when and where apps were sending personal information.

Limitations

The goal of this second-level analysis was to confirm the findings from AppBot with greater detail and find any behaviors that might have been missed from the automated tests. One of the largest limitations to the automated tests was the potential for the test to become stuck at user interface interactions similar to CAPTCHAS; for example, if an app requires verification of an identity to progress through the app. In the second-level analysis we were able to avoid most of these blocks, but there were still a few limitations to the extent of testing we could do on some apps. Some of the apps were also limited to a short free trial that requires users to commit to a subscription before spending more time on the app. We choose to include these apps because even if the user chooses not to pay for a subscription the app can still collect and share their personal information.

[19] Due to resource constraints, we had to limit the amount of fitness apps

Appendix B: Apps requesting access to Fine Location

Apps requesting access to Fine Location		
Femtech	Mental Health	Fitness and Weight Loss
amma Pregnancy & Baby Tracker Femometer - Fertility Tracker GLOW. Baby Tracker & Feeding, Diaper, Sleep Log Kindara Fertility & Ovulation Tracker Lunar - Period Tracker & Ovulation Calendar[i] Maya - Period, Fertility, Ovulation & Pregnancy MenoLife: Free Menopause Health Tracker My Days X - Ovulation Calendar & Period Tracking Ovia Fertility: Ovulation, Period & Cycle Tracker Ovia Pregnancy Tracker: Baby Due Date Countdown Pregnancy Tracker & Baby App Premom Ovulation Tracker. My Cycle & Fertility app The Bump - Pregnancy & Baby Tracker theAsianparent: Track Pregnancy & Count Baby Kicks	iFriend AI Companion Lojong: Meditation and Mindfulness +Calm -Anxiety PsyTests TalkLife for Anxiety, Depression & Stress UP! - Depression, Bipolar & Borderline Management Youper - Mental Health	AllTrails: Hiking, Running & Mountain Bike Trails BetterMe: Health Coaching Calorie Counter - MyFitnessPal CashWalk - Pays You To Get Fit DDP YOGA NOW - Workouts, Motivation & Tracking Heroband ||| iFIT - At Home Fitness Coach JEFIT Workout Tracker, Weight Lifting, Gym Log App Map My Run by Under Armour Mindbody: Home Workout & Fitness App Nike Run Club - Running Coach Noom: Health & Weight Relive: Run, Ride, Hike & more Samsung Health Simple: Intermittent Fasting and Water Tracker Step Counter - Pedometer Free & Calorie Counter Strava: Track Running, Cycling & Swimming Sweat: Fitness App For Women VeryFitPro WalkFit: Walking Tracker App

Appendix C: Shadow Profiling

There are two main types of identifiers "persistent device identifiers" and "user-resettable."[20] Persistent device identifiers are often unchangeable numbers corresponding with the device hardware. The most common persistent identifier relevant to our investigation is the Secure Settings Android ID (SSAID) or otherwise called the Android ID. A resettable identifier can be reset by the user, thus this identifier is similar to a pseudonym because it can be changed at any point.[21] The most common resettable identifier observed in this investigation was the Android Advertising ID (AAID).

One of the primary benefits of the AAID is that users have the control to reset it when they choose and want to prevent the tracking of their online activities and behavior for advertising purposes. However, when apps engage in shadow profiling, it opens the door to these identifiers being linked — also referred to as "bridging" — so that if the AAID is reset or change to a string of zeros, an app or third party can easily relink the new AAID to the permanent persistent identifier, as well as any server-side history or profile, which may include other personally identifiable information, and resume tracking.

[20] *https://developer.android.com/training/articles/user-data-ids#advertising-ids*
[21] *https://digitalwatchdog.org/wp-content/uploads/2021/05/IDAC-Shadow-Profiling-Report-FINAL.pdf*

Appendix D: List of femtech apps IDAC investigated

Apps	Play Store Category	Play Store Installs
280days: Pregnancy Diary	Parenting	1,000 K
amma Pregnancy & Baby Tracker	Medical	1,000 K
Baby Daybook - Breastfeeding & Sleeping Tracker	Parenting	100 K
Baby tracker - feeding, sleep and diaper	Parenting	1,000 K
Baby Tracker. Breastfeeding Tracker. Newborn	Parenting	1,000 K
balance - Menopause Support	Lifestyle	100 K
Breastfeeding - Baby Tracker	Parenting	100 K
Breastfeeding Newborn tracker, pump and baby diary	Parenting	1,000 K
Clue Period Tracker, Cycle & Ovulation Calendar	Health & Fitness	10,000 K
Eve Period Tracker - Love, Sex & Relationships App	Health & Fitness	1,000 K
Femometer - Fertility Tracker	Health & Fitness	1,000 K
Fertility Diet Guide - Getting Pregnant Faster	Health & Fitness	10 K
Fertility Friend Ovulation App	Health & Fitness	1,000 K
Flo Period Tracker & Ovulation. My PMS Calendar	Health & Fitness	50,000 K
GLOW. Baby Tracker & Feeding, Diaper, Sleep Log	Parenting	500 K
GLOW. Ovulation & Period Tracker	Health & Fitness	1,000 K
GLOW. Pregnancy & Baby Tracker + Baby Registry App	Parenting	1,000 K
Health & Her Menopause App	Health & Fitness	50 K
I'm Pregnant - Pregnancy Week By Week	Parenting	1,000 K
Kindara Fertility & Ovulation Tracker	Medical	100 K
Ladytimer Ovulation & Period Calendar	Medical	5,000 K
Lunar - Period Tracker & Ovulation Calendar	Health & Fitness	500 K
Maya - Period, Fertility, Ovulation & Pregnancy	Health & Fitness	5,000 K
MenoLife: Free Menopause Health Tracker	Health & Fitness	10 K

Menopause: All Information	Health & Fitness	10 K
My Calendar - Period Tracker	Medical	10,000 K
My Days X - Ovulation Calendar & Period Tracking	Lifestyle	1,000 K
Ovia Fertility: Ovulation, Period & Cycle Tracker	Medical	1,000 K
Ovia Pregnancy Tracker: Baby Due Date Countdown	Medical	1,000 K
Ovulation Calendar & Fertility	Parenting	1,000 K
ParentLove: Baby Feeding Tracker, Breastfeeding	Parenting	100 K
Peanut - Meet other Women	Social	500 K
Period and Ovulation Tracker	Medical	5,000 K
Period Tracker	Health & Fitness	10,000 K
Period Tracker	Health & Fitness	1,000 K
Period Tracker - My Calendar	Beauty	1,000 K
Period Tracker - Period Calendar Ovulation Tracker	Health & Fitness	100 M
Period tracker & Ovulation calendar by PinkBird	Health & Fitness	1,000 K
Period tracker for women. Ovulation calculator	Health & Fitness	1,000 K
Period Tracker Petal, Period & Ovulation Calendar	Health & Fitness	1,000 K
Period Tracker, Ovulation Calendar & Fertility app	Health & Fitness	10,000 K
Pregnancy + | tracker app, week by week in 3D	Parenting	10,000 K
Pregnancy Tracker & Baby App	Parenting	5,000 K
Pregnancy Tracker + Countdown to Baby Due Date	Parenting	10,000 K
Pregnancy Tracker Week by Week	Parenting	1,000 K
Pregnancy Tracker, Week by Week, Day by Day	Parenting	500 K
Pregnancy Week By Week	Medical	5,000 K
Premom Ovulation Tracker. My Cycle & Fertility app	Health & Fitness	1,000 K
The Bump - Pregnancy & Baby Tracker	Health & Fitness	1,000 K
theAsianparent: Track Pregnancy & Count Baby Kicks	Parenting	5,000 K
WomanLog Period Tracker & Calendar	Health & Fitness	10,000 K

YesMom - Fertility, Ovulation & Period Tracker	Health & Fitness	100 K

Appendix E: List of mental health apps IDAC investigated

Apps	Play Store Category	Play Store Installs
7 Cups: Online Therapy for Mental Health & Anxiety	Health & Fitness	1,000 K
Abide: Christian Meditation, Mindfulness & Prayers	Health & Fitness	1,000 K
Anxiety Relief Hypnosis - Stress, Panic Attacks	Lifestyle	100 K
Anxiety Tracker - Stress and Anxiety Log	Health & Fitness	50 K
Balance: Meditation & Sleep	Health & Fitness	100 K
Bearable - Symptoms & Mood tracker	Health & Fitness	100 K
Breethe - Meditation & Sleep App	Health & Fitness	500 K
Calm - Meditate, Sleep, Relax	Health & Fitness	10,000 K
Calm Harm - manages self harm	Health & Fitness	500 K
CBT Guide to Depression Self-help: Mood Log, Diary	Health & Fitness	100 K
Control and Monitor: Anxiety, Mood and Self-Esteem	Lifestyle	1,000 K
Dare: Anxiety & Panic Attack Relief	Health & Fitness	100 K
Daylio - Diary, Journal, Mood Tracker	Lifestyle	10,000 K
Depression Test	Medical	100 K
Depression Therapy - how to deal with depression	Lifestyle	1 K
Fabulous: Daily Motivation & Habit Tracker	Health & Fitness	10,000 K
Hallow: Catholic Meditation & Prayer App	Books & Reference	500 K
Headspace: Meditation & Sleep	Health & Fitness	10,000 K
iFriend AI Companion	Health & Fitness	50 K
InnerHour Self-Care Therapy: Anxiety & Depression	Health & Fitness	1,000 K
Insight Timer - Meditation, Sleep, Music	Health & Fitness	5,000 K
Intellect: Create a Better You	Health & Fitness	1,000 K
Let's Meditate: Meditate, Relax & Sleep	Health & Fitness	1,000 K
Lojong: Meditation and Mindfulness +Calm -Anxiety	Health & Fitness	1,000 K
Medito: Free Meditation, Sleep & Mindfulness	Health & Fitness	500 K
Mind journal: Diary, Mood tracker & Gratitude	Lifestyle	500 K
MindDoc: Your Mental Health Companion	Medical	1,000 K
MindShift CBT - Anxiety and Panic Relief	Health & Fitness	100 K
Mindvalley: Learn, Evolve and Transform Your Life	Education	1,000 K
Mood Tracker Journal. Mental Health, Depression	Lifestyle	1,000 K
MoodSpace - Stress, anxiety, & low mood self-help	Medical	100 K
MyLife Meditation: Meditate, Relax & Sleep Better	Health & Fitness	1,000 K
PsyTests	Medical	1,000 K

Reflectly: Diary, Gratitude Journal & Mood Tracker	Health & Fitness	1,000 K
Remente: Self Care, Mental Health, Personal Growth	Health & Fitness	1,000 K
Replika: My AI Friend	Health & Fitness	5,000 K
Rootd - Panic Attack & Anxiety Relief	Health & Fitness	500 K
Sanvello: Anxiety & Depression	Medical	1,000 K
Serenity: Guided Meditation & Mindfulness	Health & Fitness	1,000 K
Shine: Calm Anxiety & Stress	Health & Fitness	100 K
Simple Habit: Meditation, Sleep	Health & Fitness	1,000 K
Stop Panic & Anxiety Self-Help	Health & Fitness	500 K
TalkLife for Anxiety, Depression & Stress	Health & Fitness	1,000 K
Ten Percent Happier - Meditation & Sleep	Health & Fitness	500 K
The Tapping Solution	Health & Fitness	500 K
UP! - Depression, Bipolar & Borderline Management	Health & Fitness	100 K
Wim Hof Method -Making you strong, healthy & happy	Health & Fitness	1,000 K
Woebot: Your Self-Care Expert	Medical	100 K
Wysa: anxiety, depression & sleep therapy chatbot	Health & Fitness	1,000 K
Youper - Mental Health	Medical	1,000 K

Appendix F: List of fitness & weight loss apps IDAC investigated

Apps	Play Store Category	Play Store Installs
168 Fasting App: Fasting Tracker Intermittent Fast	Health & Fitness	10,000 K
Achievement - Rewards for Health	Health & Fitness	1,000 K
AllTrails: Hiking, Running & Mountain Bike Trails	Health & Fitness	10,000 K
Beachbody On Demand - The Best Fitness Workouts	Health & Fitness	1,000 K
BetterMe: Health Coaching	Health & Fitness	10,000 K
BetterMe: Home Workouts & Diet	Health & Fitness	5,000 K
BODY by Blogilates: Best Body Toning Workouts	Health & Fitness	100 K
BodyFast Intermittent Fasting Tracker - Diet Coach	Health & Fitness	10,000 K
Buttocks Workout - Hips, Legs & Butt Workout	Health & Fitness	10,000 K
Calorie Counter - MyFitnessPal	Health & Fitness	50,000 K
Calorie Counter - MyNetDiary, Food Diary Tracker	Health & Fitness	1,000 K
Calorie Counter by Lose It! for Diet & Weight Loss	Health & Fitness	10,000 K
Carb Manager: Keto Diet Tracker & Fasting App	Health & Fitness	5,000 K
CashWalk - Pays You To Get Fit	Health & Fitness	100 K
Centr, by Chris Hemsworth	Health & Fitness	1,000 K
Daily Yoga | Fitness Yoga Plan&Meditation App	Health & Fitness	10,000 K
DDP YOGA NOW - Workouts, Motivation & Tracking	Health & Fitness	500 K
Fastic: Fasting App & Intermittent Fasting Tracker	Health & Fitness	5,000 K
Fitbod Workout & Fitness Plans	Health & Fitness	500 K
FitOn - Free Fitness Workouts & Personalized Plans	Health & Fitness	5,000 K
Heroband|||	Health & Fitness	1,000 K
Home Workout - No Equipment	Health & Fitness	100 M
iFIT - At Home Fitness Coach	Health & Fitness	1,000 K
iTrackBites - Easy Weight Loss Diet and Tracker	Health & Fitness	500 K
JEFIT Workout Tracker, Weight Lifting, Gym Log App	Health & Fitness	5,000 K
Lifesum - Diet Plan, Macro Calculator & Food Diary	Health & Fitness	10,000 K
Lose Belly Fat at Home - Lose Weight Flat Stomach	Health & Fitness	50,000 K
Lose Weight App for Men - Weight Loss in 30 Days	Health & Fitness	50,000 K
Lose Weight App for Women - Workout at Home	Health & Fitness	50,000 K
Map My Run by Under Armour	Health & Fitness	10,000 K
Mindbody: Home Workout & Fitness App	Health & Fitness	1,000 K
Muscle Booster Workout Planner	Health & Fitness	10,000 K
Nike Run Club - Running Coach	Health & Fitness	10,000 K

Noom: Health & Weight	Health & Fitness	10,000 K
Pedometer - Free Step Counter App & Step Tracker	Health & Fitness	10,000 K
Relive: Run, Ride, Hike & more	Health & Fitness	5,000 K
Samsung Health	Health & Fitness	1,000,000 K
Simple: Intermittent Fasting and Water Tracker	Health & Fitness	1,000 K
Six Pack in 30 Days - Abs Workout	Health & Fitness	100,000 M
Step Counter - Pedometer Free & Calorie Counter	Health & Fitness	50,000 K
Step Tracker - Pedometer Free & Calorie Tracker	Health & Fitness	10,000 K
Strava: Track Running, Cycling & Swimming	Health & Fitness	10,000 K
Sweat: Fitness App For Women	Health & Fitness	5,000 K
Sweatcoin — Walking step counter & tracker	Health & Fitness	10,000 K
VeryFitPro	Health & Fitness	10,000 K
WalkFit: Walking Tracker App	Health & Fitness	10,000 K
Women Workout at Home - Female Fitness	Health & Fitness	50,000 K
WW Weight Watchers Reimagined	Health & Fitness	10,000 K
Yoga for Beginners | Nandy	Health & Fitness	100 K
Yoga-Go: Yoga For Weight Loss	Health & Fitness	10,000 K

[i] *Lunar was removed from the Google Play Store on December 13, 2021*