Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives

Kentrell Owens
University of Washington

Anita Alem
Harvard Law School

Franziska Roesner
University of Washington

Tadayoshi Kohno
University of Washington

Abstract

Electronic monitoring is the use of technology to track individuals accused or convicted of a crime (or civil violation) as an "alternative to incarceration." Traditionally, this technology has been in the form of ankle monitors, but recently federal, state, and local entities around the U.S. are shifting to using smartphone applications for electronic monitoring. These applications (apps) purport to make the monitoring simpler and more convenient for both the community supervisor and the person being monitored. However, due to the multipurpose nature of smartphones in people's lives and the amount of sensitive information (e.g., sensor data) smartphones make available, this introduces new risks to people coerced to use these apps.

To understand what type of privacy-related and other risks might be introduced to people who use these applications, we conducted a privacy-oriented analysis of 16 Android apps used for electronic monitoring. We analyzed the apps first technically, with static and (limited) dynamic analysis techniques. We also analyzed user reviews in the Google Play Store to understand the experiences of the people using these apps, and also the privacy policies. We found that apps contain numerous trackers, the permissions requested by them vary widely (with the most common one being location), and the reviews indicate that people find the apps invasive and frequently dysfunctional. We end the paper by encouraging mobile app marketplaces to reconsider their role in the future of electronic monitoring apps, and computer security and privacy researchers to consider their potential role in auditing carceral technologies. We hope that this work will lead to more transparency in this obfuscated ecosystem.

1 Introduction

Smartphone apps are increasingly being used in the U.S. for electronic monitoring (EM) of people on probation, parole, pretrial release, or people in the juvenile or immigrant detention systems [14, 35, 37, 62, 65]. EM has typically been administered to people deemed "high risk," but prison industry companies are marketing their apps as a low-cost and efficient way to expand the scope of surveillance to include "low risk" people as well [80]. People made to use EM apps often must pay regular fees to the app companies, do frequent biometric verifications, and ensure their devices do not run out of battery [65]. Failure to meet the conditions of one's release (as determined at least in part by the app) could lead to re-incarceration [35]. Yet, despite the high-stakes nature of these apps, we know of no external audit evaluating their monitoring mechanisms, accuracy, or user impact. These apps have gained visibility due to prior reporting [35, 37, 65] but have received no noticeable attention from the computer science research community.

We conducted a privacy-focused analysis of a subset of smartphone EM Android apps from a technical, human, and legal point of view. We identified 16 apps that are used by tens of thousands of people in the U.S.

We seek to answer the following research questions through our exploratory analysis of these apps:

- **What are the privacy-related technical properties of the apps, including what permissions they request and what network endpoints they contact?**

We analyze this question through static and (limited) dynamic analysis. We found that all apps but one requested fine-grained location access, and that the difference in the number of permissions requested by the most privileged app (14) and the least privileged app (0) was significant. Regarding network traffic, passive observers (e.g., ISPs) may be able to identify that someone is using an EM app based on the domains contacted.

- **What are the experiences and concerns of people using these apps?**

We investigate this question through a qualitative analysis of user reviews in the Google Play Store. We found that app reviews surface concerns about malfunctions, these apps' disruptiveness, and dissatisfaction with the *proper function* of these apps. Malfunctions discussed were mainly related to an inability to use the app to successfully perform a check-in—an

important requirement of community supervision. Disruptions caused by the apps included 1) loud alerts in inappropriate settings (e.g., work or church) or at inappropriate times (e.g., they were asleep), 2) taking up significant resources on their smartphones, such as space and battery, and 3) causing the entire smartphone to crash or freeze, potentially jeopardizing an EM condition that their phone is always running and available.

- **What is the relationship between what is stated in the apps' privacy policies and the potential risks and harms surfaced by our first two research questions?**

We investigate this question through an analysis of the privacy policies. Three apps do not have a privacy policy available in the Google Play Store, indicating that they may be in violation of its user data policies [43]. Only 9 of 16 apps had a privacy policy that explicitly addresses the apps' usage, and we discovered that one app company may have taken down its privacy policy in response to public scrutiny. While the level of details regarding data collection vary, almost all the apps said that they share data with third-parties, sometimes for marketing or advertising purposes.

Given the answers to our research questions, we present a case study of the least and most privileged apps and discuss the legal landscape related to these applications, in partnership with a legal collaborator. Collectively, our work contributes the *first systematic analysis of the electronic monitoring apps ecosystem*, and we conduct this analysis from a technical, human and legal perspective. We provide recommendations for mobile app marketplaces to increase transparency, and to the computer security & privacy community to reduce the potential harms of carceral technologies.

2 Background and Motivation

2.1 Community Supervision in the U.S.

The U.S. is the most incarcerated country in the world by both incarceration rate and total number of people incarcerated [75]. In 2020 there were 2.3 million people incarcerated. Recent polls indicate most adults in the U.S. believe that the prison and jail population should be reduced [10, 12]. However, they may be unaware of the related problem of community supervision. In the words of one district attorney, "mass supervision is the evil twin of mass incarceration" [16].

In 2020, approximately 4.5 million people in the U.S. were under "community supervision," which can include people on probation, parole, pretrial release, or people in the juvenile or immigrant detention systems [14, 50, 61]. People in these programs must comply with conditions (typically 18–29 rules [19]) that could result in incarceration if violated. These conditions include things like passing regular drug tests (even if someone's conviction was not drug-related), curfews, paying a supervision fee, and complying with geofencing [50]. Because these rules are extensive, and difficult to follow, people often fail to meet them and return to prison or jail due to "technical violations"—things would not be considered a crime if the person were not under community supervision (e.g., failing to pay a fine, missing an appointment) [15]. Around one-fourth of admissions to state prisons in the U.S. are due to technical violations [76], and over half of the people incarcerated in the U.S. are in state prisons [75].

2.2 Electronic Monitoring

Many people under community supervision are also under "electronic monitoring" or EM, also known as "e-carceration" [53]. While there is no national count of the number of people on EM, a Pew report [44] stated there were 131,000 people on EM in 2015, up 140% from 2005; that number is an under-count, as it only includes GPS and radio-frequency (RF) units. EM agreements may involve twice as many conditions compared to ones that do not involve an electronic monitor [30, 86].

Historically, EM has taken the form of an ankle monitor (GPS or RF-enabled), but smartphone apps are increasingly being used for EM. People made to use these apps have reported problems such as poor connectivity, general malfunctions, and false positive alerts sent to their EM supervisor (e.g., a probation officer) [35, 37, 65]. EM apps typically track location and are used to perform check-ins with EM supervisors, in addition to or in lieu of in-person meetings [35, 37, 62]. Check-ins might require people to face their phone's camera (for live facial recognition) or capture a photo or video of themselves. Check-ins might also use voice recognition and require people to read off a random string of numbers while facing their phones [65]. People using these apps may receive loud notifications, sometimes at random times, alerting them to complete a check-in. Similarly, apps may send loud, warning notifications caused by incorrect sensor data (e.g., location); one report indicated that these have occurred while people are sleeping [65].

Smartphone apps can be used to impose stricter conditions of supervision than would be possible under physical surveillance. For example, in a civil parental rights case, a father was ordered by a juvenile court to submit to random smartphone breathalyzer tests five times per day using `Outreach Smartphone Monitoring`, one of the apps we analyzed; any non-compliance or failure to submit within 30 minutes of an alert was assumed to constitute a positive alcohol screen [9]. The appeals court found the father's failure to complete 993 tests, out of a total of 2,317 check-ins in the span of about one year, to support terminating his parental rights. Mandating a check-in *five times* a day is only possible because of the smartphone app (and its companion Bluetooth breathalyzer); such a condition would be virtually impossible if it required travel to a physical location.

Unlike most apps, which are subject to an open market,

these apps involve people being more or less forced to use them. That is, the apps are not being built for the people using them, but for the carceral system. As these apps continue to grow in usage and cause problems for the people coerced to use them [35, 37, 65], there is a pressing need for external auditing and accountability. Although there has been some reporting on this ecosystem, there has been no systematic analysis — we aim to close that gap here.

3 Methods

We conducted static and limited dynamic analysis of 16 EM apps. Static analysis reveals what an app could *potentially* do by examining the app's code, and dynamic analysis reveals what an app *does* in controlled execution environments. We also qualitatively analyzed the apps' reviews in the Google Play Store and their privacy policies. We identified the 16 apps we analyzed from news articles, search engine results, and suggested similar apps in Google Play. We searched for combinations of terms like "smartphone apps," "electronic monitoring," "probation," and "parole" on different search engines. These apps were downloaded in or before August 2021. More details about the apps we studied can be found in Appendix D.

3.1 Static Analysis

To conduct static analysis, we downloaded the apps onto a device and extracted them via Android Debug Bridge. Examining the permissions an app requests, the third-party libraries it uses, and its source code (although obfuscated) can reveal information about the app's data collection practices, who could gain access to the data, and how they might use the data. We analyzed the output of MobSF (Mobile Security Framework), a mobile application static and dynamic analysis tool [22]. Among other things, MobSF presents an app's third-party libraries, decompiled source code, and geo-location (based on server IP address) for any domains detected in the code.

3.2 Limited Dynamic Analysis

Our ability to dynamically analyze the applications under normal operating conditions is, unfortunately, limited, because we either cannot directly create accounts ourselves (n=14) or, in some cases, choose not to do so to avoid agreeing to any terms of service (n=2). In either case, we cannot test the apps as they are used in interaction with EM supervisors. This limitation of our investigation emphasizes again the limited transparency and accountability in this ecosystem.

Nevertheless, we conduct a limited dynamic analysis of pre-login application behaviors. While running each app, we accepted any requested permissions and interacted with the app until we reached a login screen, leaving and returning to the app several times.

To gain visibility into the content and security of the network traffic, we collected network traffic while using the app and conducted a machine-in-the-middle (MITM) attack (when possible) for decryption. Using a Nexus 5X device running Android 8.1 (API 27) with mitmproxy [21], Wireshark [36], and Lumen Privacy Monitor [72, 83], we installed each app on the device and ran it for 10 minutes while capturing network traffic in Seattle, Washington. We collected traffic twice for each app with both a rooted [49] and an unrooted device; some of the apps detected that the device was rooted (and displayed a notification accordingly), and we wanted to know if that detection impacted what network traffic was sent. We instrumented the device with our own root certificate (via mitmproxy) by adding the certificate to its system store. Using Wireshark allowed us to capture network traffic that used protocols aside from the HTTP/S capture supported by mitmproxy; we also used it to verify that our network captures were working properly. Lumen's tracking of DNS transactions allowed us to attribute encrypted network traffic to specific apps, compensating for our lack of visibility into encrypted HTTP headers. After running each app, we deleted it from the device before installing the next one, verifying that it did not modify the phone's state.

3.3 App Review Qualitative Analysis

For the user review analysis, we collected all 257 reviews available in the Google Play Store and conducted qualitative content analysis [68]. Two researchers independently read through all of the reviews, each making a broad list of topics people raised. They discussed the list and jointly created a code book matching topics to closely related themes. They iterated on this code book and reached consensus on the codes to use. Using these codes, one researcher coded all of the reviews and discussed ambiguous reviews with other researchers when necessary. The final codes used are available in Appendix A. Our goal in analyzing app reviews, as with other qualitative work, was not to draw generalizable conclusions about the prevalence of certain issues, but rather to identify and surface the set of issues that people encounter and write reviews about. Consequently we do not attempt to use the review data to make generalizable or statistical claims.

3.4 Privacy Policy Analysis

We collected links to apps' privacy policies from their pages in the Google Play Store. Using an *a priori* code book developed by multiple researchers (building off one used in [34]), one researcher coded the applicable privacy policies; the codes are available in Appendix B. As discussed in Section 5.4, three of the apps did not have privacy policies available online.

3.5 Ethical Considerations

We applied for IRB approval through our institution and received official notification from the IRB that our work does not qualify as human subjects research. Nevertheless, to evaluate the ethics of analyzing public app reviews without author consent, we considered the guidelines created by Buck et al. [17] for ethical treatment of data from online sources. This study focuses on analyzing people's concerns with using these applications and studies discourse rather than the people themselves. Moreover, this collection of reviews does not appear to violate the Google Play Terms of Service [40].

We considered seeking people under EM who use these apps, and asking them if we could experimentally evaluate the properties of their apps while they used them. One of the reasons we chose not to do this is that we considered it too difficult to ethically experiment with the apps of people currently under EM; this could introduce risks to them and cause friction with their EM supervisor.

We found that seven apps in our study (`Sprokit`, `Corrisoft AIR Check-In`, `Community Supervision`, `aCheck`, `BI SmartLINK`, `Omnilink FocalPoint`, `Telmate Guardian`) appeared, at the time of our research, to be in violation of the Google Play Store's user data policies [43]. Three of the apps (`Sprokit`, `Corrisoft AIR Check-In`, `Community Supervision`) requested access to sensitive permissions but did not have privacy policies linked on their respective Google Play pages; four of them (`aCheck`, `BI SmartLINK`, `Omnilink FocalPoint`, `Telmate Guardian`) had links to privacy policies, but the policies did not mention the smartphones applications. We have notified the companies (aside from `Sprokit`, which we discovered was no longer available in the Google Play Store as of February 2022) with a one month deadline by which they must add a privacy policy to their Google Play pages. If the changes are not made by the deadline, we will contact trusted contacts at Google who specialize in vulnerable populations for guidance on next steps. Section 7.4 considers risks associated with simply removing apps from app stores.

3.6 Limitations

Our methods for identifying apps likely did not capture every EM app in use. However, given reports about usage and cumulative number of downloads in Google Play, we believe our findings are representative of these apps.

During our dynamic analysis, we were only able to navigate to the app login screens and could not create accounts. This limited the possible network traffic we could observe, meaning that the findings we report here are a lower bound on what data the apps are sending. Recent work has also taken a similar approach to analyzing some Android apps (albeit for different reasons). In a large-scale analysis of Android apps, Nguyen et al. [64] found that thousands of apps send personal data to third-parties after an app is opened (pre-auth) and potentially violate GDPR due to a lack of explicit consent.

Additionally, we only monitored network traffic from each app for 10 minutes. However, unless we noted otherwise in Section 4 (e.g., if an app had time-driven requests), apps did not send any additional network traffic aside from a burst of traffic when the app was first opened or if an action was taken (e.g., removing the app from the foreground). This indicates that monitoring traffic for a longer period of time likely would not have yielded more network traffic being observed.

We analyzed reviews from these apps in the Google Play Store; this approach has several limitations. Reviews could be from people who do not actually use the apps, to present them in an overly positive or negative light. There is also a potential skew regarding who chose to write a review; people with more negative experiences might be more compelled to write a review. Conversely, someone who had a particularly negative experience with the app might not write it for fear of being identified and facing repercussions. Lastly, four of the 16 apps we analyzed had no public reviews, and could not be included in our analysis.

4 Results: Information Flows, Sources, and Sinks

We analyzed these apps' permissions, network traffic, and third-party library usage. In the following sections, we present general findings for all apps before presenting case studies of the apps we determined to be the most privileged (regarding the data it *can* access), and least privileged.

4.1 Information Sources: Permissions

Permissions determine the types of data apps can collect. To understand the privacy risks to people using these apps, we must first understand what types of data can be collected about them. People under EM are required to accept at least some, if not all, of the permissions requested by these apps. For example, some apps request permissions to offer certain features and continue to function if certain permissions are denied; other apps (such as `Telmate Guardian`) do not allow actions within the app (such as login) until all permissions have been granted.

Smartphone operating system permissions protect access to restricted data and restricted actions. Apps that request more permissions can send more data to supervisors and third-parties. By analyzing the distribution of permissions requested by these apps, we can compare them to the least-privileged app among them. If the least-privileged app has the same (or similar) goals as the other apps, it stands to reason that it may be able to serve as a standard for the "minimum number of permissions" necessary for other apps to function.

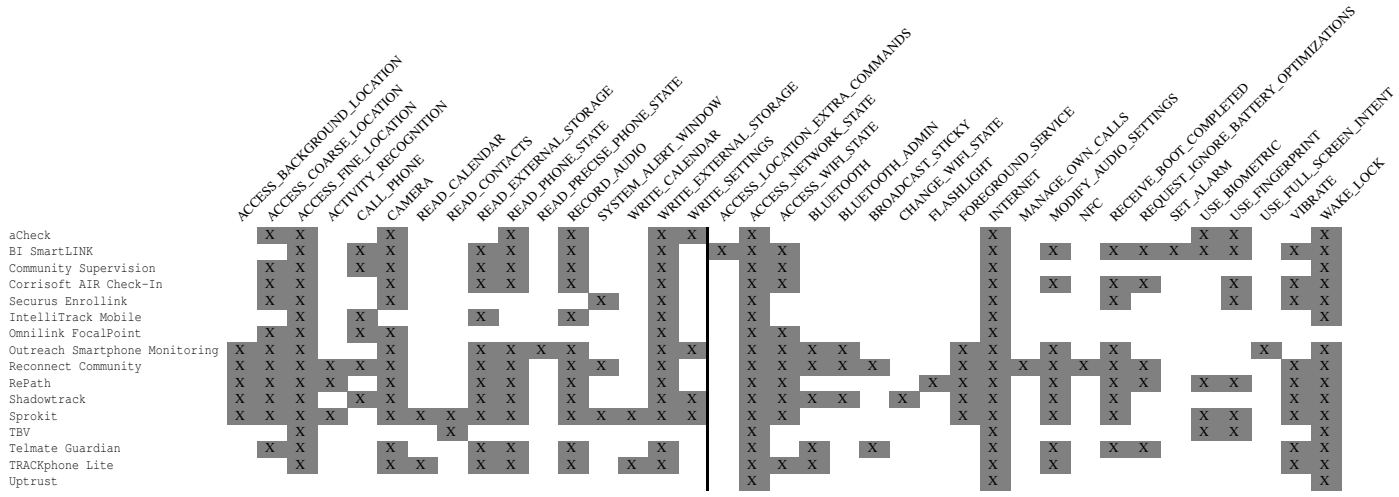

Table 1: Permissions requested by each app. The leftmost permissions are label as "dangerous" by Android.

4.1.1 What is the prevalence of different *dangerous* permissions in these apps?

Table 1 shows the Android permissions requested by the apps. The permissions on the left of the vertical line are labeled as "dangerous" in Android API documentation, while the rest in the table are considered "normal" permissions [25]. Dangerous permissions allow apps to access otherwise restricted data and take otherwise restricted actions. For the purpose of brevity and because they are not relevant to our investigation, we have excluded certain custom permissions, and phone manufacturer specific permissions (e.g., com.huawei.android.launcher.permission.CHANGE_BADGE) from the table.

The most common permission gave apps access to precise location information. All EM apps but one (`Uptrust`) requested ACCESS_FINE_LOCATION, reflecting the centrality of location tracking to these apps' functionality. This permission enables apps to receive a location that is "as accurate as possible, ... sometimes as accurate as within 10 feet (a few meters) or better" [26]. It is notable that beginning with Android 10 (API Level 29, released September 2019), apps that wish to request a phone's location running in the background must request ACCESS_BACKGROUND_LOCATION [26]; only 5/16 monitoring apps did. However, as only 8.2% of Android devices use Android 10 [24], this may not affect these apps' ability to track background location on most devices. Most apps requested CAMERA (13/16) and RECORD_AUDIO (12/16), indicating potential use for biometric face or voice authentication or the use of video and audio data for other purposes.

A few apps requested permissions that did not have widespread use. There were several dangerous permissions that only a few apps requested, indicating that they may not be necessary to offer capabilities similar to those offered by other monitoring apps. For example, only `Outreach Smartphone Monitoring` requests the READ_PRECISE_PHONE_STATE permission, which allows the detailed reading of information about phone state [25]. `TBV` and `Sprokit` are the only monitoring apps that requested the READ_CONTACTS, which—when combined with READ_PHONE_STATE—could allow supervisors to monitor whom someone talks to and how frequently they speak. Similarly, three of the apps request the ACTIVITY_RECOGNITION permission, which reports if someone is in a vehicle, on a bicycle, running, or still [23].

4.2 Information Sinks: Third-Party Libraries

While the presence of permissions reveals what type of data may be collected, the presence of third-party libraries reveals to whom collected data may be sent. Third-party libraries may have access to sensitive data about people using EM apps and may even monetize their use of the app. Smartphone apps typically include third-party libraries, which are sometimes referred to as SDKs (software development kits), although SDKs are broader in scope and often contain more than one library [28].

4.2.1 What type of third-party libraries are included in these apps?

While two apps had no trackers, nearly all of the apps contained one or more Google analytics libraries. MobSF [22], a mobile application analysis tool, uses Exodus [71], a tool to identify trackers in Android applications based on a list of known trackers. According to Exodus, a tracker is software that is meant to collect data about the person using a device or how the device is used; third-party libraries fall under this definition. Table 2 displays

Permission taken or presence of trackers found in static analysis could lead FP if not verified with dynamic analysis. -Vijay

the trackers we found in the apps. Only two of the monitoring apps (`Omnilink FocalPoint` and `Corrisoft AIR Check-In`) contained no trackers at all. All of the remaining apps but `Shadowtrack` contained at least one Google-based analytics tracker.

5 Third party trackers

Tracker	Type	# apps
Google Firebase Analytics	analytics, databases, messaging, crash reporting	12
Google CrashLytics	crash reporting	6
Google Analytics	analytics	2
Microsoft Visual Studio App Center Analytics	analytics, push notifications	2
Microsoft Visual Studio App Center Crashes	crash reporting	2
Facebook Analytics	analytics	2
Facebook Login	login	2
Google AdMob	advertising	1
Facebook Ads	advertising	1
Facebook Share	content sharing	1
Amplitude	analytics, profiling	1
Segment	analytics, profiling	1
OneSignal	push notifications, messaging	1
Branch	analytics	1
Flurry	analytics, advertising	1
New Relic	analytics	1
UrbanAirship	analytics	1

Table 2: Third party trackers in monitoring apps (N=16)

Two apps use ad libraries, indicating the companies behind the apps might profit from the compulsory use of these apps. `Telmate Guardian` contained the Flurry library, but appeared to only use its analytics capabilities and does not implement the code necessary to serve ads in the app. `Sprokit` appeared to contain the code necessary for Google AdMob and Facebook Ads SDKs to serve ads and monetize use of their app.

Two apps use Facebook Analytics and Login SDKs. `Sprokit` and `Uptrust` both use Facebook Analytics and Login SDKs. This means that if someone logs into Facebook in the app, at a minimum the app gets access to their public profile and email address [33]. Additionally, Facebook learns that this person is using the EM app.

Text

5.1 Information Flows: Limited Dynamic Analysis

Unlike permission and libraries, apps' network traffic reveals what they actually do. To understand the data sharing practices of EM apps, we collected data while interacting with the apps. Specifically, we wanted to know what types of data are sent from the apps, to whom those data are sent, and if those data are sent securely. Understanding what types of data are sent allows us to examine the potential risks associated with those data and what data (if any) cross expected or legal bounds. As we mentioned in Section 3.2, while we would prefer to do a thorough dynamic analysis (e.g., collecting network traffic while using a tool to simulate user interaction with the app), our inability to create accounts and the lack of transparency in this ecosystem prevented us from doing so. Although the dynamic analysis was limited, it places a lower bound on what network traffic apps send.

5.1.1 What services do the apps contact?

Apps send traffic to their servers and some of the third-party services detected in their code. Four apps (`Securus Enrollink`, `Omnilink FocalPoint`, `Corrisoft AIR Check-In`, and `TBV`) had no detectable network traffic during our captures. An examination of the domains we detected in network analysis reveals that some of the libraries shown in Table 2 were not contacted. This was likely due to our limited ability to conduct dynamic analysis; we could not get past the account login page on these apps and might not have reached the page(s) that made requests to these libraries.

5.1.2 Are apps transmitting data securely?

Nearly all of the traffic to and from these servers was encrypted using TLS (aside from one font request made by one app). Additionally, based on an IP address-based geolocation tool [59] we used (which are typically accurate on the country-level [56]), all of the servers contacted were located in the United States.

5.1.3 What data do the apps send, and how frequently are they sent?

Using mitmproxy [21] we were able to intercept and decrypt network traffic being sent to some of the apps and observe their contents in clear text. When attempting MITM, two of the monitoring apps (`Telmate Guardian` and `aCheck`) displayed notices indicating they detected the device was rooted and would not permit login. While `Telmate Guardian` contacted the same domains as it did on an unrooted device, `aCheck` did not reach out to its server (gwusacheck.aware.attentigroup.com) when the device was rooted.

Although the volume of network traffic was low, apps sent general device information using both event- and time-driven requests. Generally, most apps did not send much data, but those that did sent general device info.

We observed two apps sending time-driven requests. `Telmate Guardian` pinged New Relic once every minute, sending device data and information about domains recently contacted by the app. `Sprokit` contacted Facebook once every five minutes, sending several data. `Telmate Guardian` and `TRACKphone Lite` both sent event-driven requests to third-party libraries (Flurry and Branch, respectively) whenever the apps were moved between the foreground and the background (e.g., if the person using the phone was looking at the app or not). This could be used to calculate the total amount of time someone is using an app or potentially to ensure someone is looking at the app.

5.1.4 Is potentially sensitive information about a monitored person available to any entity able to passively observe the phone's network traffic?

A passive observer on the same Wi-Fi network or an entity such as an ISP may be able to know that the person connected to their network is under EM and using one of these apps based on the domains they observe. Six of the 16 apps (`aCheck`, `BI SmartLINK`, `Community Supervision`, `IntelliTrack Mobile`, `RePath`, and `Telmate Guardian`) contacted domains that might uniquely identify the apps, meaning that the domains often included the names of the apps or their parent companies; a list of these domains is available in the appendix. For example, `Telmate Guardian` contacted domain `api.telmateguardian.com`. This information could allow passive observers—e.g., coffee shops, airports, schools, employers, Airbnb hosts—to know if someone is under EM.

5.2 Case Studies of Apps

We present case studies of the most privileged and least privileged apps to 1) understand the spectrum of potential invasiveness of the apps and 2) derive a minimum set of permissions that might be needed by these apps. This comparison assumes the apps have similar goals and requirements; we discuss the limitations of this assumption in Section 7.2. While it might be preferable to holistically identify the "best" and "worst" apps, the asymmetric information available for each app (e.g., some have no reviews while others have dozens) made such comparisons challenging. Consequently, we compared the apps on the dimensions we could access universally (i.e., the number of permissions).

5.2.1 Which app was the most privileged?

`Sprokit` was the most privileged app and potentially the most invasive because it requested the most dangerous permissions, had the most third-party libraries, and was the only app we observed sending sensor (accelerometer) data *prior to login*. `Sprokit` requested most dangerous permissions of any app we analyzed (14/16 of the permissions shown in Table 1). `Sprokit` had nine third-party libraries, the highest number for any app we analyzed: Google Analytics, Google Firebase Analytics, Google AdMob, Facebook Analytics, Facebook Login, Facebook Ads, Facebook Share, Amplitude, and Segment.

`Sprokit` contacted Facebook at `https://www.facebook.com/adnw_sync2` once every five minutes, sending several data including, but not limited to: if the device is rooted, current accelerometer readings, the amount of total/free device memory, battery stats, general device info, and a flag indicating if the app requires compliance with the Children's Online Privacy Protection Act (COPPA). We did not observe any other apps sending mobile sensor (e.g., accelerometer, gyroscope, barometer) data. We also did not observe web requests to any of the other, non-Facebook libraries we observed during static analysis.

`Sprokit` has 101-500 downloads in the Google Play Store. Its website [77] does not contain a list of entities using the app, indicating that its reach might still be quite small. If these install numbers are not accurate, the discrepancy could be explained if the apps are side-loaded [78].

5.2.2 Which app was the least privileged?

`Uptrust` was the least privileged app because it requested the fewest permissions, and it was the only app that did not request any location permissions. `Uptrust` is the only app in our analysis that did not request any dangerous permissions; it also requested the fewest normal Android permissions of the apps we analyzed. Our static analysis detected that `Uptrust` included three third-party libraries: Google Firebase Analytics, Facebook Analytics, and Facebook Login.

While conducting MITM, we observed network traffic being sent to Google Firebase and at least one of the Facebook libraries. Specifically, a POST request to `https://firebaseinstallations.googleapis.com` logged that the `Uptrust` app was installed and sent back an authentication token. Several requests sent to `graph.facebook.com` appeared to log the installation of the `Uptrust` app (`event: MOBILE_APP_INSTALL`) and other custom events (`event: CUSTOM_APP_EVENTS`), including `fb_sdk_settings_changed` and `fb_sdk_initialize`. Each request to Facebook contained an anonymous id (`anon_id`) and an advertiser ID (`advertiser_id`), along with an `advertiser_tracking_enabled` flag set to true and some device information (such as phone type and Android API version).

Although `Uptrust`'s website lists 104 states & local agencies that have used its app, it only has between 501-1000

installs in the Google Play Store [82].

5.2.3 Takeaways

While `Sprokit` and `Uptrust` both state that their apps do no track its users [77, 82], there is a wide discrepancy regarding the permissions they request, the number of third-party libraries they include, and the amount and type of network traffic we observed in our limited dynamic analysis. It is worth noting that although we determined `Sprokit` was the most privileged app, its website suggests that it does not track people: "We Strive to Prevent E-Carceration; No tracking; No recording; Non-stigmatizing" [77].

5.3 Concerns in the App Reviews

Because the data collection and sharing practices of the apps ultimately impact the people required to use them, it is important to understand what concerns they have about these practices—providing more depth to our understanding of people's actual experiences with these apps in ways that a strictly technical analysis cannot.

To understand the concerns of people using these apps, we qualitatively coded reviews of these apps in the Google Play Store. Twelve of the 16 apps had visible reviews (N = 257) in the Google Play Store; `aCheck`, `Sprokit`, `TRACKphone Lite`, and `Uptrust` were the exceptions.

5.3.1 What were the general sentiments towards the apps in the reviews?

While there were some positive reviews, widespread lack of functionality, these apps' disruptiveness, and dissatisfaction with the *proper function* of these apps caused the reviews to be overwhelmingly negative (n=165). While some of the negative reviews did not contain an explanation for the negative review—e.g., R94: "*Worst app ever*"—the majority of them (n=104) mentioned a malfunction in the app. Some of the most common malfunctions were not being able to perform a successful check-in in the app, not receiving a notification for a check-in, or an app no longer working after an update. Several reviews also mentioned not knowing how to log in to the app or make an account, since most of the apps do not allow account creation. Among the negative reviews that provided more context, some (n=41) described dissatisfaction with a *properly-functioning* app, often raising issues with the performance of the app or the fact that they have to use the app at all.

There were also several positive reviews (n=75). Some of them (n=33) provided no explanation for the positive review (e.g., R8: "*Very good*") while others (n=42) described how the app is good for communication, staying on track with the conditions of their supervision, or avoiding having to physically go into an office to meet with their supervisor—e.g., R172: "*The best app for Offender Report in. No more need to drive down to see your probation officer. Make payments right from your phone.*"

5.3.2 What types of malfunctions were mentioned?

Malfunctions discussed by the reviewers of were mostly related to an inability to use the app to successfully perform a check-in—an important requirement of community supervision. This inability to check-in was often attributed to failures in the apps' facial recognition, voice recognition, or location detection systems. Some failed check-ins were attributed to general lack of functionality (e.g., R189: "*app [won't] let me check in,it has been having problems all day today*") or not receiving notifications that a check-in was being requested (e.g., R32: "*Does not do notifications. Causes of problem with PO [probation/parole officer]*").

Some reviews (n=33) also mentioned failures that involved smartphone sensors (e.g., camera, microphone, location). Several apps require people to send a picture, send a video, or hold the phone to their face while facial recognition happens. Common problems related to camera usage included inability to take a picture or record a video and not being recognized by facial recognition algorithms. Regarding facial recognition, R37 wrote "*The facial recognition needs to be refined since I didn't have makeup on when I took the first pictures, however when I put on makeup, facial recognition becomes much harder, even in adequate lighting*," and R41 said "*Facial recognition is terrible. I've given up.*" Research by Buolamwini and Gebru [18] showed that facial analysis algorithms have significantly higher error rates on darker-skinned people; this could cause facial recognition problems to disproportionately impact Black (or other darker-skinned) people under EM. A review added by R93 during the international COVID-19 pandemic read "*Can be very inconvenient when I am out in public and have to take my mask off to check in ...*"

R198 expressed frustration with the location sensor: "*Hate it.. it goes off for nothing and it supposed to be gps but can't even detect the right location..... STUPID APP...*" Another reviewer (R150) described their troubles with using the microphone for voice recognition: "*It keeps locking up. I have never gotten past the voice analysis. It truly sucks.*"

5.3.3 What types of disruptions did EM apps cause in people's lives?

Disruptions caused by the apps included 1) loud alerts in inappropriate settings (e.g., work or church) or at inappropriate times (e.g., they were asleep), 2) taking up significant resources on their smartphones, such as space and battery, and 3) causing the entire smartphone to crash or freeze, potentially jeopardizing an EM condition that their phone is always running and available. These

disruptions could violate the information security principles of availability (if the app causes the phone's OS to crash) and confidentiality (because of privacy leakage when loud notifications happen). The reviews contained descriptions of disruptions they cause in the reviewers' lives, particularly the notifications from the apps and the problems the apps cause on their smartphones. Regarding the volume of the notifications from the app, R129 wrote "*... Raises all media to maximum volume when the notification goes off (even on silent) which is incredibly harmful to your ears with ear buds in*." Another reviewer (R133) wrote "*... the notification overrides my phone's silent/vibrate function which is a nuisance for certain places (e.g. church, work etc.). When I first started the program I could keep it silent, then it started overriding about a month into it.*" The reviewers also mentioned how the timing of the notifications can be disruptive, sometimes going off while they are asleep—e.g., R184: "*it has costed me a job already because they ping you in the middle of the night while you are asleep. cant wake up on time to get to work*," R180: "*It goes off all night and keeps me awake ...*"

Several reviewers mentioned how the apps they use constantly draining battery from their phones. To remedy this, one reviewer described purchasing an external battery to ensure that their phone always had power. Other complaints were about the amount of memory these apps take up and how using these apps can cause their entire phones to glitch and freeze. Regarding the memory requirements of an app, R228 wrote "*This is b.s. man.. gotta update every few weeks bcuz they keep thinkin of new ways to keep their boots on our necks.. it ends up taking so much space, you gotta buy a phone JUST FOR THIS ONE APP!!!! ZERO STARS*."

Discussing crashes and battery, R64 wrote "*App constantly crashes in the background, no response from support. Drains battery from constantly reopening and crashing*" and R87 wrote "*Freezing up phone and causes a lot of glitches along with consuming battery life*."

5.3.4 What comparisons did the reviews make to alternatives?

EM apps were compared to ankle monitors and prisons in a few reviews; EM apps were described as better than prison, and both better and worse than ankle monitors. Reviewers of the apps sometimes compared them to other methods of EM, namely ankle monitors. Two reviewers described using an app as better or more tolerable than using an ankle monitor (R91: "*... it's one hundred percent more livable than an ankle bracelet ...*"). Conversely, one reviewer said they preferred using an ankle monitor to using an app, after listing a myriad of problems they encountered with the app—R129: "*... Ridiculous waste of money for something that does nothing but frustrate you. Ankle monitor > [`Outreach Smartphone Monitoring`] ANY DAY.*" Similarly, another reviewer suggested that people under EM should use a different method for location tracking if they have other options available to them—R179: "*It's a horrible app and if you have a choice of some other gps options take it.*".

Reviewers also compared using the apps to being incarcerated. Unsurprisingly, while they described using the apps as inefficient and dysfunctional, some reviewers still thought using the apps was much better than being in prison or jail. R187 wrote "*Horrible app. Constant network problems, won't let me pay on the app ... extremely inefficient all around. but... it is better [than] prison...*"

5.3.5 What did the reviews say about concerns of people using EM apps and the risks they faced?

Reviewers described a general sense of injustice by being required to use these apps. They also raised privacy concerns, and felt that using this apps would lead to more problems with their EM supervisors and potentially imprisonment. Some reviewers (n=9) explicitly mentioned surveillance or privacy concerns that they have with the apps they were using. For example R217 wrote "*It's ok. I don't trust it because it is very intrusive but have no choice in the matter because I am on state probation.*"

Reviewers (n=23) raised the risk of them getting a violation because of the app malfunctioning. R37 wrote "*I've been having trouble with the check-ins not alerting my phone which causes my probation officer to call and threaten to file a warrant for my arrest because I missed the check-ins, which is incredibly frustrating and distressing.*" Similarly, R192 said "*This app has a very bad default in it ... when trying to report to your parole officer it has a tendency to not allow you to report ... when it says that you need to report it is not logging it in so therefore if you have this app you are going to go to jail because it's going to make you fail ...*"

More generally, 57 reviews mentioned a broad sense of injustice or being wronged. One reviewer (R209), who used an app as part of a drug treatment program, pleaded with the app's developers to fix its problems:

> "l'm a drug court client in phase 5 been in the program over a year done very well[,] worried about this app it doesn't work not very well[,] the developer's should be ashamed of themselves[,] this is my sobriety and freedom that's at stake this app has the ability to destroy all l have work so hard for[,] please fix it or take it down[,] your money is not worth my freedom !!!!"

5.4 Privacy Policies

We inspected the privacy policies of these apps 1) to understand their described data collection and sharing practices, 2) to observe what regulatory limits on these practices they raised, and 3) to determine if the behavior we observed during

our technical analysis was covered (explicitly or implicitly) by statements in the policies.

Three apps did not have a privacy policy available in the Google Play Store, indicating that they may be in violation of the Google Play Store's user data policies. Every app in the Google Play Store "must post a privacy policy in both the designated field in Play Console and within the app itself" [43]. Out of the 16 apps we analyzed, three of them (`Community Supervision`, `Corrisoft AIR Check-In`, `Sprokit`) had links that did not actually point to a privacy policy. `Corrisoft AIR Check-In` even had the words "Privacy Policy" on its website but there was no hyperlink to click on [20]. This means these three apps appear to be in violation of the Google Play Store's user data policies [43].

Only 9 apps had a privacy policy that explicitly addresses the apps' usage, and one of them may have taken down a relevant privacy policy in response to public scrutiny. Although 3 apps did not have a privacy policy linked the Google Play Store, we were able to find one of the policies on the app's website, bringing the number of policies we found to 14. Of the 14 privacy policies that we were able to locate, four of them do not reference the EM apps, with three of them specifically referring only to the "Site" where the privacy policy was hosted. It could be argued that these four policies also violate Google Play's policy because they do not address their respective apps; however, this violation is less straightforward than the aforementioned one. `BI SmartLINK`'s Google Play page had a link that appeared to be to an app-specific privacy policy (`https://bi.com/products-and-services/bi-smartlink-privacy-policy/`), but the URL forwarded to a generic privacy privacy with no mention of the app (`https://bi.com/privacy/`). Interestingly, as recently as May 2021, the app-specific `BI SmartLINK` URL was active and contained relevant information [48]. Later that month, a report critiquing the app and referencing its privacy policy ("*... SmartLINK's privacy policy indicates that the application can share virtually any information collected through the application, even beyond the scope of the monitoring plan, with the supervising officer*") was published [61]; as of October 2021 that privacy policy is no longer reachable. This means that only 9/16 apps currently have privacy policies that appear to be applicable to their respective apps; we describe these nine apps' policies in more detail below.

5.4.1 Data collection & sharing

While the level of details regarding data collection vary, almost all the apps said that they share data with third-parties, sometimes for marketing or advertising purposes. While some apps' privacy policies gave very detailed description of what data they collected—`RePath` even explicitly mentioned the sensitive permissions requested in the app and provided a use case for each one [29]—other apps were quite vague, with text like "we may require you to provide us with certain personally identifiable information" [58].

Eight of the nine policies had language about sharing data with law enforcement, a supervisor, or a court-based entity. Although these policies state that they will comply with warrants, they also outline other reasons they might share data with one of these entities without a warrant, such as to "protect and defend the rights or property of [the company]" [41]. Eight of the nine policies also described their data sharing practices with third-parties. These practices appeared to be similar across the policies; one's personal data is typically shared with affiliates, subsidiaries of the companies, or a service provider. The service providers include companies that do web hosting, marketing, analytics, and advertising.

Regarding selling data, five of the policies said explicitly that they do not sell one's data. Seven of the policies mention that data will be used for marketing, sometimes for marketing the company's own product and advertisements.

5.4.2 Regulations

Apps mentioned regulations but may consider themselves exempt from complying with certain portions of them. The privacy policies may be relevant if people under EM bring legal challenges against third-party data disclosures or retention. For example, the California Consumer Privacy Act (CCPA) created certain rights for California residents to request deletion of personal information by private business and permits civil penalties for violations [1]. However, the Act only applies to companies of a certain size or revenue [2], and it is unclear whether the businesses producing EM apps would qualify. Additionally, prior research on prison technology companies indicates CCPA may have little impact, even if it applies, due to broad exceptions within privacy policies [66].

Five policies mentioned CCPA, and four mentioned Children's Online Privacy Protection Act (COPPA). One app (`IntelliTrack Mobile`) described itself as exempt from CCPA's data deletion clause and that the community supervisor should be contacted, saying it is "generally exempt from the Right to Delete requirements of CCPA. All Right to Know, Right to Receive and Right to Delete requests should be directed to your corresponding Supervising Authority" [41]. Another policy mentioned that "monitored users" may have limited deletion rights [57]. Similarly, while five policies contained text about data deletion and retention, only one (`Shadowtrack`) named a fixed duration after which data would be deleted: "All facial recognition data is stored for a period of **up to seven years** after the Enrollee is removed from the program. This retention time period is dictated by the supervising agency" [79].

Two app policies included the possibility that data might be stored or processed outside of the U.S., bringing into question

how the privacy laws abroad may conflict with those of the U.S. and if that affects the monitored individual's data rights.

6 Putting Our Results in Legal Context

To understand the legal ramifications of these apps and what protections exist for people on EM, we examined the legal context for EM apps. The Constitution and its interpretation by the Supreme Court set the baseline of protection against invasive community supervision practices. Existing protections often arise from *legal challenges* alleging unconstitutional practices; these rulings, if favorable for the people on EM, can set limits on the scope of certain invasive practices.

However, legal challenges to EM of individuals under supervision face three significant hurdles. First, constitutional precedent is unfavorable, particularly when "public safety" is balanced against the privacy rights of a disfavored group like people convicted or accused of a crime. Second, individuals under supervision are already subject to strict conditions infringing the right to privacy, freedom of speech, and religion; arguably, smartphone EM is no different [45]. Third, advocates may be hesitant to challenge EM because they believe its alternative would be greater incarceration, rather than abolition; we discuss this third point in more detail in Section 7.3.

Courts disagree on the limits of continuous EM of supervised individuals, and the Supreme Court has yet to decide the issue [87]. The most relevant constitutional protection against government EM is the Fourth Amendment right to be free from unreasonable searches and seizures. Smartphone apps present a search of phone data as well as location data [6]. "The touchstone of the Fourth Amendment is reasonableness" based on the degree of intrusion into an individual's privacy [4]. The Supreme Court, however, has held that probationers and parolees have a diminished expectation of privacy [5], since criminal convictions necessarily "curtail an offender's freedoms" [4]—although, as previously discussed, not everyone under EM has been convicted of a crime (e.g., people on pretrial release or release from immigrant detention). The court balances this diminished expectation of privacy against government interests that include "integrating probationers back into the community, combating recidivism, and protecting potential victims" [5]. Against such vague state interests, "searches are almost always deemed reasonable" [85].

The breadth and continuous nature of smartphone surveillance raises the question: **at some point, surely *some* kind of search must be unreasonable?** However, the government may circumvent the reasonableness requirement altogether by invoking a questionable notion of consent. Some circuit courts have held that because the criminal defendant agreed to warrantless searches in their supervision conditions to avoid incarceration, they have consented to the search and forfeit the right to raise a Fourth Amendment claim [85]—regardless of the obvious issues of coercion (i.e., if you must use the app or go to jail) [45]. Notably, the relevant consent in such a case is not to the privacy policy of the smartphone application, but to the conditions of supervision imposed by a court or administrative body [7]. As a result of both the Fourth Amendment "reasonableness" analysis and consent arguments, groundbreaking Supreme Court cases such as *Riley v. California* and *United States v. Carpenter*, which imposed greater protections on smartphone searches or location data [6, 8], have generally not been applied to individuals on probation or parole [85].

Private companies may face legal challenges as well. Although the Fourth Amendment generally only applies to government actors [3], it may also apply to private actors who are sufficiently involved in a public action such as administering criminal punishment [32, 73]. Constitutional law aside, private contractors are still subject to statutory, contractual, and regulatory requirements as well as tort law [60], all of which can be used to challenge faulty monitors [31, 38].

Advocates face an uphill battle in distinguishing smartphone EM from other conditions of supervision that have been deemed legally permissible. For example, one district court, in responding to an ICE detainee's claim that 24/7 smartphone monitoring encroached on his individual liberty, noted "far more onerous" conditions such as mandatory lifetime sex offender registry or prohibiting a parolee from leaving the state for four years are legally valid; EM seems tame in comparison [11].

Ultimately, it is difficult for anyone to bring legal challenges if they are faced with a false choice of opting in to EM when the alternative is incarceration. It is necessary to move beyond "alternatives," as discussed in Section 7.3.

7 Discussion

7.1 EM Apps Introduce New Harms & Risks

Due to their multipurpose use, EM smartphone apps introduce new risks to people, relative to both typical community supervision and ankle monitors. Because of the range of mobile OS permissions and sensors on smartphones, apps can collect and share significantly more data than ankle monitors (even ones that may have microphones). These data can be shared digitally with third-parties used within the app but also can be shared by EM supervisors with police or other prosecutorial entities.

Using EM apps also means that entities that might not otherwise be aware that an individual is under EM now know this. For example, network service providers (e.g., ISPs) observing network traffic may be able to telling that someone is using an EM app based on a domain. Mobile operating systems (e.g., iOS, Android) log whenever someone downloads these apps. Third-party libraries (e.g., Facebook) can learn that an individual is using an app, and they may have additional personal data about this individual.

As discussed in Section 5.3, the apps are often unreliable and dysfunctional. Many reviews discussed a variety of malfunctions within the app. Other reviews described how the apps affected the performance of their entire device, causing it to crash. These issues could cause people using EM apps to be more likely to fail a check-in; some reviews mentioned how people felt that these apps were setting them up to fail. Given that people might not be able to successfully check-in, and they need to have their devices on and charged as a condition of EM, it can be argued that the use of the apps is likely to increase interactions between people under EM and their supervisor and increase the likelihood that they might be incarcerated.

Our results indicate that some apps request permissions that let them access audio and video data, and may periodically send data to servers (e.g., `Sprokit` contacting Facebook every five minutes). The amount of data sent by these apps may create financial burdens for people using them. Given that the poorest people are overrepresented in community supervision [51], and poorer people are more likely to use prepaid phone plans [67], apps that send significant video or audio data for biometric verification could be costly. The cost of mobile data plans necessary to use the apps can be burdensome, especially in addition to the fees that may be required as an EM condition [35, 86].

It is worth noting that while we believe EM smartphone apps introduce new risks and harms to people on community supervision, we do not seek to imply that these new risks and harms are more significant or important than those already imposed by the conditions of community supervision. The restrictive conditions of community supervision (and the predictable failures to comply with these stringent conditions [27]) "can lead to job loss, housing instability, difficulty caring for children, interruptions in healthcare, and a host of other collateral consequences" [30, 52, 70]. Using EM apps adds to an already onerous list of things people under community supervision must manage.

7.2 Examining the "Least Privileged" App

We observed a potentially wide discrepancy along multiple dimensions between the least privileged (`Uptrust`) and the most privileged apps (`Sprokit`). This discrepancy raises the question: what permissions are necessary for these apps to accomplish their goals? In computer security & privacy, the principle of least privilege states that a system "should operate using the least set of privileges necessary to complete the job" [74]; this principle has relevance in this ecosystem. If an app's goal is rehabilitation, it may focus more on features like court date reminders and request the minimum permissions necessary to support those features. If its goal is surveillance, it will likely request as many permissions as possible to collect the widest range of data, and may share that data widely.

That said, we acknowledge that although the apps can be used for similar purposes, they may have different goals (e.g., enforcing a home curfew versus daily breathalyzer readings) and consequently need different permissions. There is no existing standard for what functionality EM apps should or should not include nor what permissions EM apps should request, and from a legal perspective there is no burden (that we are aware of) on the government to choose a less privileged app over one that might be more privileged. Nonetheless, it is still helpful for us to identify the least privileged app to inform policymakers who can develop regulatory limits for EM apps and may use the least privileged permissions access as a model. Our paper provides empirical data for a multi-stakeholder conversation to potentially develop a model to determine what permissions are necessary and how much data collection is "too much" (if these apps are to continue to be used).

7.3 Moving Beyond "Alternatives"

As we note in Section 6, legal precedent is not favorable to parolees and probationers, or to challenges regarding consent, since people under EM may "agree" to the conditions to avoid incarceration. Since they consent to the general conditions of EM rather than the terms and conditions of an app, people under EM may be subject to whatever data practices the app vendor itself desires (as long as these practices are not disagreeable to the EM supervisor and do not violate contract terms). EM app vendors can force updates and change their privacy policies (if they have one) at any time, and the people coerced to use these apps may not have a successful pathway to legally challenging any of its practices because they "consented."

Regardless of what legal arguments may be raised to challenge EM, it is important to know that the choice is not just "EM or incarceration," as judges and prosecutors may present it; there is also effective community-based rehabilitation. As Chaz Arnett has noted, "the narrow comparison between jail and electronic monitoring" provides an incomplete choice when a variety of abolitionist alternatives may be explored [13]. Most importantly, as Kate Weisburd wrote, "[t]here is no empirical evidence ... that monitoring is used as an alternative; and that in a world without monitors the same people would (or should) remain incarcerated" [13]; a recent report examining pretrial electronic monitoring in Los Angeles County supports this [84].

7.4 Recommendations

In light of our findings, we direct our recommendations to technology companies and the computer security and privacy research community.

Mobile app marketplaces. Mobile app marketplaces (e.g., the Google Play Store) should realize that they are not neutral

actors and that they have a place in the future of EM apps. They can enforce their terms of use and require apps that collect sensitive data to have a privacy policy that describes how the app functions or be taken down from the marketplace; this could cause up to several apps in this study to be removed. However if they are immediately removed, people who are required to use them or to newly enroll may be unable to do so and may face immediate harm as a result. A similar risk exists if a company removes their app from the Google Play Store (like `Sprokit`) while it continues to be used. EM apps being removed from app marketplaces could lead to supervisors sideloading [78] these apps onto people's devices (instead of downloading them from app marketplaces), and this ecosystem would become more opaque. However, another possibility is that the usage of EM apps would become untenable; the labor required from EM supervisors (managing app updates and complaints) might lead to a decline in their usage.

Relatedly, app marketplaces could also modify their terms of use to limit the use of apps in their marketplace in carceral contexts. App marketplaces could have special rules for EM apps. Just as incarcerated people and people on probation/parole may be considered a "special population" by an IRB, one could imagine a flag that app developers are required to set if their app is used for electronic monitoring. This flag could trigger additional rules, including increased transparency requirements. The Google Play Store already prohibits apps that block ads and apps that allow people to cheat at games [39]. They could similarly prohibit EM apps. In allowing EM apps and banning others, they are making a set of value judgements; our work calls on them to consider whether these value judgements are appropriate.

Computer security & privacy researchers. EM apps exist within a broader ecosystem of carceral technologies. This ecosystem includes technologies like ankle monitors, recidivism risk-assessment tools, and mental health prediction targeted at incarcerated people. These same technologies are often administered by private companies on behalf of public sector entities, meaning that they may not be subject to the same public records requirements as governments. Despite the severe impact that these technologies may have on people affected by them, many of their internal parameters and controls are unknown. While understanding the inner workings of these technologies is not necessary to understand the harm they may cause, it may benefit the public by exposing faulty or discriminatory inputs and the harms that they *do* cause. Given our skills for understanding complex systems and frequently interdisciplinary methods, the computer security & privacy research community is particularly well-positioned to make a positive impact in this space by increasing transparency and, consequently, accountability.

Future work in this space could determine how to more thoroughly study EM apps and overcome the significant ethical concerns and structural challenges. To actually understand usage one needs to have an app that is paired with an account run by an EM supervisor; we do not currently have the structures in place to conduct these experiments.

Other recommendations. Regarding recommendations for legislators, judges, prosecutors, state and county community corrections organizations, or activists, we will defer to the recommendations of those organizations and people actively working in these sectors. We refer the readers to the work of Kate Weisburd [85, 86], Just Futures Law & Mijente [61], and James Kilgore [54, 55] for detailed recommendations for each of these actors.

8 Related Work

8.1 Electronic Monitoring

Weisburd compiled and analyzed almost 300 state and local policies governing people on EM [86], the largest such compilation [30]. In addition to providing detailed background on the characteristics of different EM technologies (including smartphone apps), Weisburd also found that these technologies (deemed "punitive surveillance") are invasive and restrictive and argues that their use is itself a *form of punishment*, rather than rehabilitative, as they are often presented.

Just Futures Law & Mijente published a report in May 2021 on how ICE's Alternatives to Detention (ATD) program expands mass surveillance [61]. They discuss in-depth the different surveillance technologies ICE uses at different stages of its ATD program; these technologies include GPS tracking with an ankle monitor, voice recognition & verification over the phone, and `BI SmartLINK` and the facial recognition it uses. The report describes how the app functions, what its usage was at the time of publication, and how the usage of EM apps is likely evolve to include biometric wearables. The authors point out how biometric wearables, such as wrist bands or head pieces, are already being used in carceral systems in the U.K. [63] and Hong Kong [69], and in 2019 the DOJ funded a project at Purdue University leveraging smartphones, wearables, and AI "to identify risky behaviors, stressful situations and other behavioral and physiological factors correlated with those individuals at risk of returning to their criminal behavior" [46].

James Kilgore wrote a survey paper covering literature on EM [53], concluding that there is "no serious, rigorously executed research that proves that EM has a positive impact on the person being monitored." Kilgore argues that using smartphone apps for EM is part of a larger EM research agenda that aims to either justify EM's use or making it more efficient.

In human-computer interaction (HCI) literature, Troshynski et al. [81] conducted focus groups with ten people in California who were required to wear ankle monitors as a condition of their parole. They found that the places that par-

ticipants were able to occupy had both spatial (e.g., exclusion zones) and temporal dimensions (e.g., device battery life). The authors argued that privacy researchers should adopt a new view of location privacy (which they called "accountabilities of presence") that focused on social and cultural participation rather than traditional economic cost/benefit analyses (e.g., *trading* one's privacy to use a platform).

8.2 Android Application Analysis

Researchers have previously conducted similar privacy-focused analyses of Android apps. Feal et al. [34] conducted a privacy study of 46 parental control apps (aka "parentware") using similar static, dynamic, and privacy policy analysis techniques as in our work. They also provided legal context for their research (COPPA). Overall they found that the apps lacked transparency and did not comply with regulatory requirements, even apps recommended by government-affiliated entities. Han et al. [42] conducted a similar analysis comparing the privacy of pairs of free and paid versions of consumer apps. They found that despite popular belief otherwise, paid and free versions of apps had similar collection and sharing practices regarding sensitive data.

9 Conclusion

We analyzed 16 Android apps used for electronic monitoring. We found that these apps include numerous trackers, the permissions requested by them vary widely (with the most common one being location), and reviews indicate that their users find them invasive and frequently dysfunctional. This is the first work to systematically analyze apps in this ecosystem that desperately needs transparency and accountability. Our results call for all stakeholders (including app stores, security researchers, and legal stakeholders) to rethink what, if anything, these apps should look like.

Acknowledgments

The authors would like to thank the paper shepherd Tara Whalen and the anonymous reviewers for their insightful comments. We would also like thank Aurelia Augusta for her help developing an earlier iteration of the reviews codebook, Gennie Gebhart for brainstorming in the early stages of this project, Lassana Magassa for early conversations that led to this project, Sudheesh Singanamalla for his helpful comments on the methodology, Mason Kortz for reviewing the legal portion of this paper, Christine Geeng & David Kohlbrenner for reviewing a draft of this paper, and Nancy Garland for providing feedback on our methods and our disclosure process. This work was supported in part by the University of Washington Tech Policy Lab, which receives support from: the William and Flora Hewlett Foundation, the John D. and Catherine T. MacArthur Foundation, Microsoft, the Pierre and Pamela Omidyar Fund at the Silicon Valley Community Foundation; it was also supported by the US National Science Foundation (Awards 156525 and 2114230).

References

[1] Cal. Civ. Code §§ 1798.100-.199 (West 2018).

[2] Cal. Civ. Code §§ 1798.140(1) (West 2018).

[3] United States v. Jacobsen, 466 U.S. 109, 129-30. 1984.

[4] United States v. Knights, 534 U.S. 112, 119. 2001.

[5] Samson v. California, 547 U.S. 843, 848-49. 2006.

[6] Riley v. California, 573 U.S. 373, 401-02. 2014.

[7] United States v. Barnett, 415 F.3d 690, 691-93. 2015.

[8] Carpenter v. United States, 138 S. Ct. 2206, 2221. 2018.

[9] A.N. v. Ind. Dep't of Child Servs., No. 18A-JT-2147, 2019 Ind. App. Unpub. LEXIS 883, at *4, *14. 2019.

[10] Poll shows strong cross-ideological support for dramatically reducing jail and prison populations to slow the spread of coronavirus. http://thejusticecollaborative.com/2020/03/new-report-poll-jail-prison-coronavirus/, Mar 2020.

[11] Ndiaye v. Adducci, No. 4:19CV712, 2020 U.S. Dist. LEXIS 252421. 2020.

[12] ACLU. 91 percent of americans support criminal justice reform, aclu polling finds. https://www.aclu.org/press-releases/91-percent-americans-support-criminal-justice-reform-aclu-polling-finds, Nov 2017.

[13] Chaz Arnett. From Decarceration to E-carceration. *Cardozo L. Rev.*, 41:641, 2019.

[14] Patricio G. Balona. More eyes being fixed on volusia-flagler juveniles on probation. https://www.news-journalonline.com/news/20170625/more-eyes-being-fixed-on-volusia-flagler-juveniles-on-probation, Jun 2017.

[15] Nikki Trautman Baszynski. States should abolish technical violations of probation and parole. *The Point by the Appeal*, Apr 2021.

[16] Ryan Briggs. Krasner: "mass supervision" is the "evil twin" of mass incarceration. https://stoneleighfoundation.org/krasner-mass-supervision-is-the-evil-twin-of-mass-incarceration/, Mar 2019.

[17] Amber M. Buck and Devon F. Ralston. I didn't sign up for your research study: The ethics of using "public" data. *Computers and Composition*, 61:102655, 2021. Rhetorics of Data: Collection, Consent, & Critical Digital Literacies.

[18] Joy Buolamwini and Timnit Gebru. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, Feb 2018.

[19] Ronald P Corbett Jr. Burdens of leniency: The changing face of probation. *Minn. L. Rev.*, 99:1697, 2014.

[20] Corrisoft. Home. https://web.archive.org/web/20211012183449/https://corrisoft.com/, 2021.

[21] A Cortesi, M Hils, T Kriechbaumer, and contributors. mitmproxy. https://mitmproxy.org/, 2010.

[22] Henry Dalziel and Ajin Abraham. *Automated security analysis of android and iOS applications with mobile security framework*. Syngress, 2015.

[23] Google Developers. Detect when users start or end an activity. https://developer.android.com/guide/topics/location/transitions.

[24] Google Developers. Distribution dashboard. https://developer.android.com/about/dashboards.

[25] Google Developers. Manifest.permission. https://developer.android.com/reference/android/Manifest.permission.

[26] Google Developers. Request location permissions. https://developer.android.com/training/location/permissions.

[27] Shaila Dewan. Probation may sound light, but punishments can land hard. *The New York Times*, Aug 2015.

[28] DIGIDAY Editors. Explainer: SDKs vs Libraries. https://digiday.com/media/explainer-sdks-vs-libraries/, Apr 2011.

[29] eHawk Solutions. Repath privacy policy. https://web.archive.org/web/20210927232836/https://ehawksolutions.com/repathprivacypolicy/.

[30] Bhadha et al. Electronic prisons: The operation of ankle monitoring in the criminal legal system. *George Washington University Law School*, page 54, 2021.

[31] Lauren Etter. What's the maker of post-it notes doing in the ankle monitor business? struggling. *Bloomberg.com*, Apr 2017.

[32] Brian B Evans. Private prisons. *Emory LJ*, 36:253, 1987.

[33] Facebook. Permissions - facebook login - documentation. https://developers.facebook.com/docs/facebook-login/android/permissions/.

[34] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proceedings of Privacy Enhancing Technologies (PoPETS)*, 2020.

[35] Todd Feathers. 'They track every move': how US parole apps created digital prisoners. http://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners, Mar 2021.

[36] The Wireshark Foundation. Wireshark. https://www.wireshark.org/.

[37] Sidney Fussell. Apps are now putting the parole agent in your pocket. https://www.wired.com/story/apps-putting-parole-agent-your-pocket/, Nov 2020.

[38] Robert S Gable. Left to Their Own Devices: Should Manufacturers of Offender Monitoring Equipment be Liable for Design Defect? *U. Ill. JL Tech. & Pol'y*, page 333, 2009.

[39] Google. Device and network abuse. https://support.google.com/googleplay/android-developer/answer/9888379#zippy=%2Cexamples-of-common-violations.

[40] Google. Google play terms of service. https://play.google.com/about/play-terms/index.html, Oct 2020.

[41] Track Group. Track group privacy policy. https://web.archive.org/web/20210927153055/http://trackgrp.com/privacy-policy/, Jun 2020.

[42] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Narseo Vallina-Rodriguez, Amit Elazari, Kenneth A. Bamberger, and Serge Egelman. The Price is (Not) Right: Comparing Privacy in Free and Paid Apps. *Proceedings on Privacy Enhancing Technologies*, 2020(3):222–242, Jul 2020.

[43] Play Console Help. User data. https://support.google.com/googleplay/android-developer/answer/10144311.

[44] Kelly Hoffman. *Use of Electronic Offender-Tracking Devices Expands Sharply*. Sep 2016.

[45] Andrew Horwitz. Coercion, pop-psychology, and judicial moralizing: Some proposals for curbing judicial abuse of probation conditions. *Wash. & Lee L. Rev.*, 57:75, 2000.

[46] Brian Huche. Artificial intelligence examines best ways to keep parolees from recommitting crimes. https://www.purdue.edu/newsroom/releases/2020/Q3/artificial-intelligence-examines-best-ways-to-keep-parolees-from-recommitting-crimes.html, Aug 2020.

[47] U.S. Immigration and Customs Enforcement. Detention management—detention stastitics. https://www.ice.gov/detain/detention-management. Updated October 1, 2021.

[48] BI Incorporated. Bi smartlink™ privacy policy. https://web.archive.org/web/20210526234349/https://bi.com/products-and-services/bi-smartlink-privacy-policy/.

[49] IT Info. Root a device (rooting) – what does it mean? https://webllena.com/root-a-device-rooting-what-does-it-mean/, Feb 2018.

[50] Charles Koch Institute. What is community supervision? https://charleskochinstitute.org/stories/what-is-community-supervision/, Jan 2019.

[51] Deborah Johnson. Connections among poverty, incarceration, and inequality. https://www.irp.wisc.edu/resource/connections-among-poverty-incarceration-and-inequality/, May 2020.

[52] Alexi Jones. Correctional control 2018: Incarceration and supervision by state. https://www.prisonpolicy.org/reports/correctionalcontrol2018.html, Dec 2018.

[53] James Kilgore. Survey of EM Literature. https://www.challengingecarceration.org/survey-of-em-literature/, Jun 2018.

[54] James Kilgore. Let's fight for freedom from electronic monitors and e-carceration. https://truthout.org/articles/lets-fight-for-freedom-from-electronic-monitors-and-e-carceration/, Sep 2019.

[55] James Kilgore. As the u.s. scrambles to slow coronavirus, we should be wary of increased surveillance. https://theappeal.org/coronavirus-covid-19-surveillance-electronic-monitoring/, Mar 2020.

[56] Dan Komosny, Miroslav Voznak, and Saeed Ur Rehman. Location accuracy of commercial ip address geolocation databases. *Information Technology And Control*, 46(3):333–344, Sep 2017.

[57] Outreach Smartphone Monitoring LLC. Privacy policy. https://web.archive.org/web/20210929230231/https://app.osmnow.com/privacy_policy.pdf, Feb 2020.

[58] TRACKtech LLC. Privacy policy. https://web.archive.org/web/20210921161420/https://app.tracktechllc.com/privacy_policy.html.

[59] MaxMind. Geoip2 precision web service demo. https://www.maxmind.com/en/geoip2-precision-demo.

[60] Gillian E Metzger. Privatization as delegation. *Colum. L. Rev.*, 103:1367, 2003.

[61] Just Futures Law & Mijente. Ice digital prisons. https://www.flipsnack.com/JustFutures/ice-digital-prisons-1u8w3fnd1j.html, May 2021.

[62] Mike Nellis. "Better than Human"? Smartphones, Artificial Intelligence and Ultra-Punitive Electronic Monitoring. *Challenging E-Carceration*, page 20, 2019.

[63] BBC News. "sobriety ankle tags" rolled out across england. https://www.bbc.com/news/uk-politics-56583153, Mar 2021.

[64] Trung Tin Nguyen, Michael Backes, Ninja Marnau, and Ben Stock. Share First, Ask Later (or Never?) Studying Violations of GDPR's Explicit Consent in Android Apps. In *30th USENIX Security Symposium*, August 2021.

[65] Molly Osberg and Dhruv Mehrotra. When your freedom depends on an app. https://gizmodo.com/when-your-freedom-depends-on-an-app-1843109198, Apr 2020.

[66] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In *CHI '21*, May 2021.

[67] PaymentsJournal. Prepaid card trends by age and income:. https://www.paymentsjournal.com/prepaid-card-trends-by-age-and-income/, Nov 2020.

[68] Alan Peshkin. The goodness of qualitative research. *Educational researcher*, 22(2):23–29, 1993.

[69] Katya Pivcevic. Biometrics, drones and robotic guards: Inside hong kong's first 'smart prison'. https://www.biometricupdate.com/202012/biometrics-drones-and-robotic-guards-inside-hong-kongs-first-smart-prison, Dec 2020.

[70] Mark Pogrebin, Mary Dodge, and Paul Katsampes. The collateral costs of short-term jail incarceration: The long-term social and economic disruptions. *Corrections Management Quarterly*, 5:64–69, 2001.

[71] Exodus Privacy. εxodus: The privacy audit platform for android applications. https://reports.exodus-privacy.eu.org/en/.

[72] Abbas Razaghpanah, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Christian Kreibich, Phillipa Gill, Mark Allman, and Vern Paxson. Haystack: In situ mobile traffic analysis in user space. *arXiv preprint arXiv:1510.01419*, pages 1–13, 2015.

[73] Jed Rubenfeld. Privatization and state action: Do campus sexual assault hearings violate due process. *Tex. L. Rev.*, 96:15, 2017.

[74] Jerome H Saltzer and Michael D Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[75] Wendy Sawyer and Peter Wagner. Mass incarceration: The whole pie 2020. https://www.prisonpolicy.org/reports/pie2020.html, Mar 2020.

[76] Vincent Schiraldi. Explainer: How 'technical violations' drive incarceration. https://theappeal.org/the-lab/explainers/explainer-how-technical-violations-drive-incarceration/, March 2021.

[77] SPROKIT. Sprokit (successful prisoner re-entry opportunities & knowledge interactive tool). https://www.sprokit.net/.

[78] Cameron Summerson. How to sideload apps on android. https://www.howtogeek.com/313433/how-to-sideload-apps-on-android/, Jan 2018.

[79] Shadowtrack Technologies. Privacy policy. https://web.archive.org/web/20210528161904/https://www.shadowtrack.com/about_us/privacy/.

[80] Telmate. Telmate guardian: A new frontier in smartphone-based location monitoring; the case for telmate guardian and "community corrections," including parole, probation, pre-trial & work release. https://web.archive.org/web/20210511011316/https://www.telmate.com/wp-content/uploads/2015/07/TEL-WhitePaper-Guardian-NonBleed-r6.pdf, Jul 2015.

[81] Emily Troshynski, Charlotte Lee, and Paul Dourish. Accountabilities of presence: Reframing location-based systems. In *CHI '08*, 2008.

[82] Uptrust. Impact. https://uptrust.co/impact/, Feb 2021.

[83] Narseo Vallina-Rodriguez. Lumen privacy monitor. https://www.icsi.berkeley.edu/icsi/projects/networking/haystack.

[84] Alicia Virani. *Pretrial Electronic Monitoring in Los Angeles County*. Feb 2022.

[85] Kate Weisburd. Sentenced to surveillance: Fourth amendment limits on electronic monitoring. *NCL Rev.*, 98:717, 2019.

[86] Kate Weisburd. Punitive surveillance. *Virginia Law Review*, 108, 2021.

[87] Daniel Yeager. Certain certiorari: The digital privacy rights of probationers. *Conn. L. Rev. CONNtemplations*, 50:1, 2017.

A Review Qualitative Analysis Codes

- Sentiment: Positive, with explanation
- Sentiment: Positive, no explanation

- Sentiment: Negative, proper function
- Sentiment: Negative, with malfunction
- Sentiment: Negative, no explanation or unclear explanation
- Sentiment: Neutral or unclear
- Justice: Felt wronged, injustice
- Sensors: Problem with camera
- Sensors: Problem with microphone
- Sensors: Problem with location
- Sensors: Problem with external device
- Authentication: Unable to login
- Malfunctions: Problems after update
- Malfunctions: Check-in or monitoring features not working
- Malfunctions: Faulty notification behavior
- Risks: Getting a violation because of faulty app
- Risks: Surveillance/privacy
- Comparison to alternatives: Better than traditional alternatives
- Comparison to alternatives: Worse than traditional alternatives
- Comparison to alternatives: Better than Prison
- Disruptions: Device limitations
- Disruptions: Loud alerts
- Misc: Technical Support Requests/Issues
- Misc: Took screenshots to capture check-ins that were logged
- Misc: Billing issues
- Misc: Forced to remove mask to check-in

B Privacy Policy Qualitative Analysis Codes

- Mentions their mobile app?
- Mentions Mobile Data collection? E.g., location, contacts, camera
- Mentions sharing with law enforcement (without warrant)?
- Mentions sharing with 3rd parties?
- Mention any regulations?
- Mentions processing data on servers worldwide?
- Software updates mentioned?
- Do they sell your data?
- Do they mention "marketing purposes"?
- Mentions Retention? / Deletion?

C Summary of Network Traffic Analysis

App Name	Potentially Identifying Domain(s) Contacted	Third Party Libraries
Telmate Guardian	api.telmateguardian.com	Flurry, New Relic, Urban Airship
BI SmartLINK	{bicdn, services, services.tn}.bi.com	Google Firebase Analytics, Microsoft Visual Studio App Center Analytics
RePath	app-version-log.repathportal.com	Google CrashLytics, Google Firebase Analytics
IntelliTrack Mobile	intellitrack-api.trackgrp.com	Google CrashLytics, Google Firebase Analytics
Community Supervision	api.globalsupervision.net	Xamarin
aCheck	gwusacheck.aware.attentigroup.com	
Reconnect Community		Google Firebase Analytics, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes
Uptrust		Facebook, Google Firebase Analytics
Outreach Smartphone Monitoring		Google CrashLytics, Google Firebase Analytics
Shadowtrack		Google CrashLytics, Google Firebase Analytics
TRACKphone Lite		Branch
Sprokit		Facebook

Table 3: Summary of network traffic analysis.

D App Information

App Name	App ID	Installs	Additional usage information
aCheck	com.attenti.acheck.us	100+	
BI SmartLINK	com.biinc.mobile.client	100,000+	In 2020, the BI SmartLINK app was used by Immigration & Customs Enforcement (ICE) to monitor approx. 24,000 people; as of May 8, 2021, this number is 34,445 people [35, 47].
Community Supervision	com.supervision.community	500+	
Corrisoft AIR Check-In	com.corrisoft.air.core	1,000+	
Securus Enrollink	com.stopllc.offendermobile	1,000+	
IntelliTrack Mobile	com.trackgrp.intellitrackmobile	100+	
Omnilink FocalPoint	com.numerex.focalpoint	1,000+	
Outreach Smartphone Monitoring	com.osmnow	1,000+	
Reconnect Community	org.call2test.connectcomply	10,000+	
RePath	com.ehawk.repath	1,000+	
Shadowtrack	com.shadowtrack.shadowtrackview	10,000+	The Shadowtrack app is being used by approx. 11,000 people on probation in Virginia [35].
Sprokit	com.sprokit.Sprokit	100+	No longer available as of February 2022.
TBV	com.tbv.totalrecovery	100+	
Telmate Guardian	com.telmate.prod	10,000+	
TRACKphone Lite	com.tracktechllc.trackphonelite	100+	
Uptrust	com.uptrust.enduser	100+	

Table 4: EM app details, including Google Play Store installs and additional usage information.