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

Kentrell Owens, Anita Alem (Harvard Law School), Franziska Roesner, and Tadayoshi Kohno

Presented at USENIX Security 2022

SECURITY & PRIVACY RESEARCH LAB
UNIVERSITY of WASHINGTON

You are at a protest

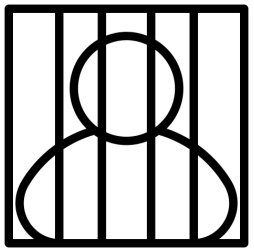
Something is thrown at police

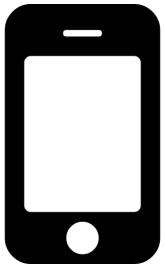
You are arrested and taken to jail

You see a judge within 24 hrs

Instead of bail, you install an app

Copyright: Pepsi

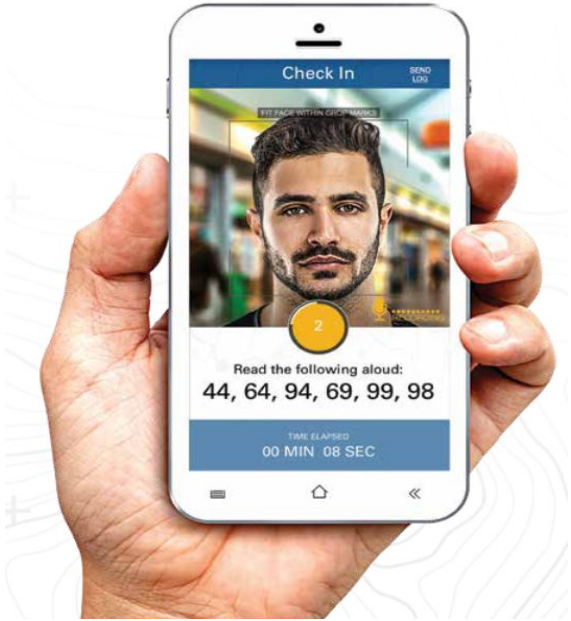




Apps are a new type of electronic monitoring (EM)

- EM is a subset of community supervision (~4.5 million)
  - Probation, parole, immigrant/juvenile/pre-trial detention, etc.
- Normally must comply with several conditions such as curfews, visits, drug tests, supervision fees, etc.
- Historically EM tech was ankle monitors
- EM smartphone apps are increasingly being deployed
  - Immigrant detention by ICE (~95k as of March 2022)
  - Probation in Virginia state prisons (~11k as of March 2021)

EM apps are used for “check-ins” with supervisor



Copyright: Telmate Guardian

- In addition to or in lieu of in-person meetings
- Check-ins might use: location, facial/voice recognition, breathalyzer
- Failure to successfully check-in can lead to incarceration

Problem: These high-stakes apps have not been audited to evaluate their data practices or what (privacy) risks they may have on people coerced to use them.

Research Questions

RQ1: What are the **experiences and concerns of people** coerced to use these apps?

Method: Qualitative analysis of Google Play Store app reviews

RQ2: What are the privacy-related **technical properties** of apps?

Method: Static & limited dynamic analysis of Android apps (N=16); Case studies of some apps

RQ3: Do the apps' **privacy policies** align with our observations?

Method: Qualitative analysis of privacy policies

RQ4: What **legal privacy protections** (if any) exist for people under EM?

Method: Collaboration with a legal scholar

RQ1: What are the **experiences and concerns of people** coerced to use these apps?

Method: Qualitative analysis of Google Play Store app reviews

RQ2: What are the privacy-related **technical properties** of apps?

Method: Static & limited dynamic analysis of Android apps (N=16); Case studies of some apps

RQ3: Do the apps' **privacy policies** align with our observations?

Method: Qualitative analysis of privacy policies

RQ4: What **legal privacy protections** (if any) exist for people under EM?

Method: Collaboration with a legal scholar

Ethical Considerations

- Sought IRB approval and were deemed exempt
- Followed guidelines (Buck and Ralston 2021) for analyzing data from online sources
- Seven apps appeared to violate Google Play Store's User Data policies
- We reached out to these companies with a 1 month deadline after which we notified Google

What are the experiences and concerns of people coerced to use these apps?

Malfunctions caused issues with performing check-ins

- Check-ins are typically a requirement of using these apps
- Caused by apps' faulty facial/voice recognition or location
- Loud alerts (at work or church), consumed significant battery/space, and causing OS crashes/freezes
- Crashes could cause a violation of EM conditions

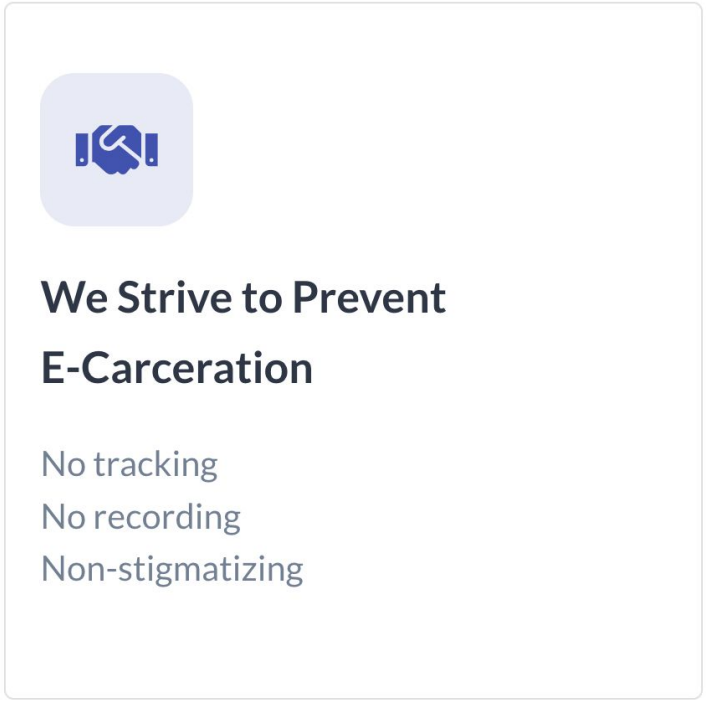
People described a general sense of injustice

R209: “*I'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 I have work so hard for[,] please fix it or take it down[,] your money is not worth my freedom !!!!*”

What are the privacy properties of the most & least privileged apps?

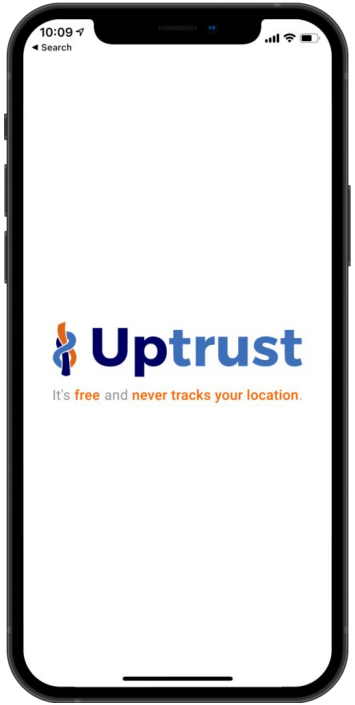
SPROKIT was the most privileged app

- Requested the most runtime permissions (14)
- Had the most 3rd-party libraries (nine, including ad and social media)
- Sent Facebook data every 5 min



Copyright: SPROKIT

Uptrust was the least privileged app



Copyright: Uptrust

- Requested zero runtime permissions
- Had three third-party libraries (analytics & social media)
- “...doesn't geolocate or have a user-funded model…”

Conclusion and looking forward

- EM apps introduce new harms & risks
- There are few limits on what these apps can do
- Their proliferation is not inevitable
- CS researchers can do good in this space

What can S&P researchers do to help?

- Lots of other carceral tech impacting people
  - Ankle monitors, wearables for recidivism prediction, mental health prediction tools targeting incarcerated people
- We can audit these technologies and collaborate with legal scholars, policy makers & community organizations
- Understanding how things work isn't necessary to understand harm… but it helps!

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

Kentrell Owens
kentrell@cs.washington.edu

Anita Alem
aalem@jd23.law.harvard.edu

Franziska Roesner
franzi@cs.washington.edu

Tadayoshi Kohno
yoshi@cs.washington.edu

- Analyzed 16 EM Android apps
- EM apps introduce new harms & risks
- Legal protections are minimal
- Their proliferation is not inevitable
- More details in the paper!

Twitter: @KentrellOwens
Full paper: https://tinyurl.com/em-apps