What are parental control apps?
Parent’s can monitor the phone usage of their children as well as set rules

Private information harvesting
- Highly intrusive apps by definition
- Must have parental consent
- Must not share private information

Goals
- Report possible COPPA and GDPR violations
- Map privacy policy to actual behavior
- Shed light on a highly intrusive yet not studied type of mobiles apps

Motivation
- Previous work: dynamic analysis using Taintdroid[1,2]
- We analyzed 7 apps and found:
  - One app gathers private data before policy acceptance
  - Two apps disseminate private data already stored on the device
  - Two apps share location and web history with third parties
  - Four apps send PIIs over an insecure channel (no TLS)

Methodology
- Static analysis:
  - Backstage and Cartographer[3,4]
  - We extract information flows, URLs, libraries and UI elements
- Dynamic analysis:
  - Lumen Privacy Monitor[5]
  - Lowe bound on data leaks
- Privacy policy analysis:
  - Polisis[6]
  - Semiautomatic analysis of privacy policies

Early results
- Private data flows in 33 apps
- Non COPPA compliant libraries in 8 apps
- 12 weeks of privacy policies stored

Ethical considerations
- At no point in this study have we gathered private data from real users
- All data is generated using fake accounts controlled by us

Reference