

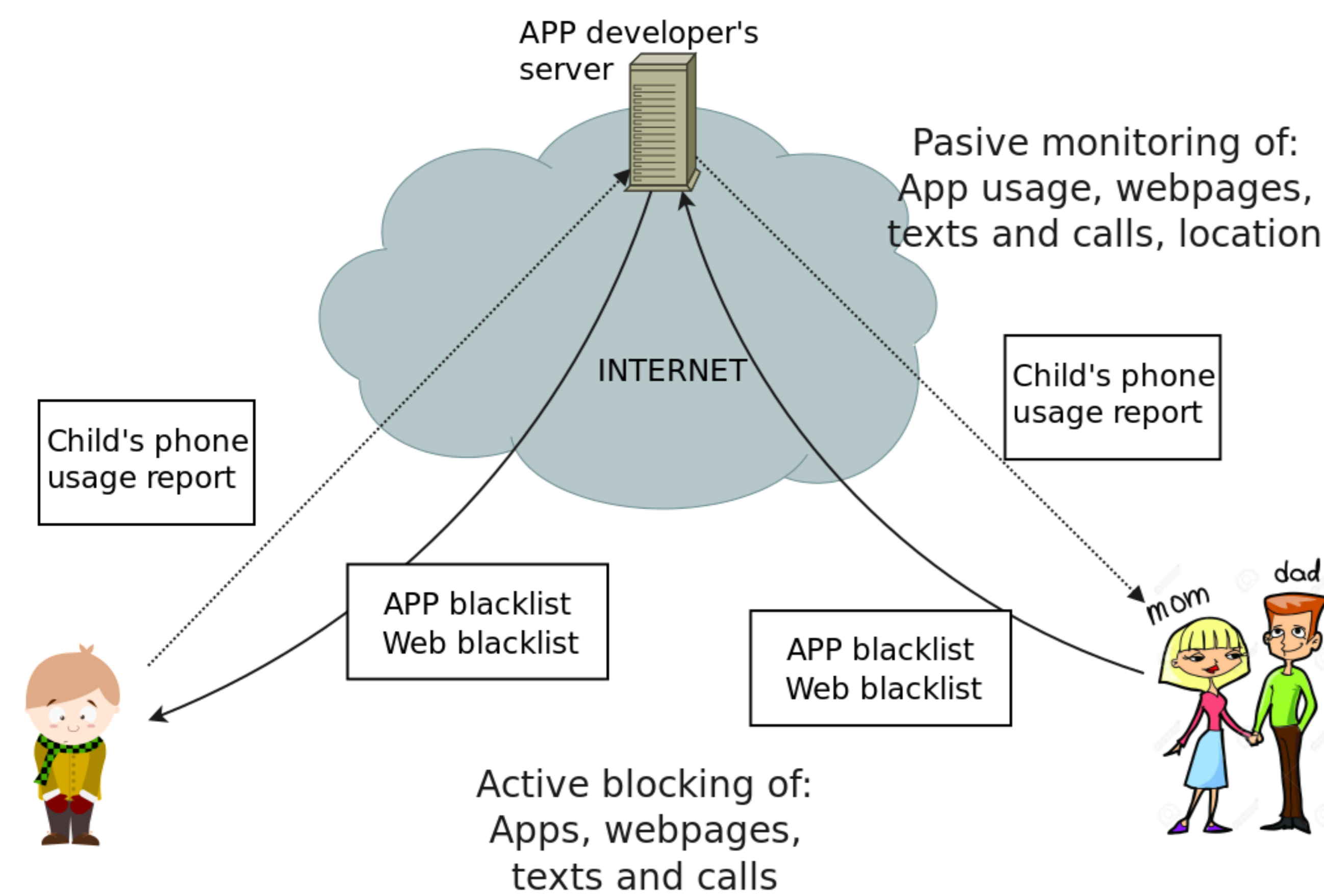
# A Study on the Privacy Implications of Mobile Parental Control Apps

Álvaro Feal(1,2), Julien Gamba(1,2), Narseo Vallina-Rodríguez(1,3), Carmela Troncoso(4), Alessandra Gorla(5), Paolo Calciati(5,6)

(1) IMDEA Networks, (2) Universidad Carlos III de Madrid, (3) ICSI, (4) Spring Lab EPFL, (5) IMDEA Software, (6) Universidad Politécnica de Madrid

## What are parental control apps?

Parents 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 mobile 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 PII 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]
  - Low 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

[1] A. Feal, C. Troncoso, and M. Carro. Privacy study on parental control apps. Master's thesis, UPM, 2017.

[2] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In USENIX OSDI, 2010.

[3] V. Avdiienko, K. Kuznetsov, I. Rommelfanger, A. Rau, A. Gorla, and A. Zeller. Detecting behavior anomalies in graphical user interfaces. In ICSE-C, 2017.

[4] P. Calciati, K. Kuznetsov, X. Bai, and A. Gorla. What did really change with the new release of the app? In MSR, 2018

[5] . Razaghpanah, N. Vallina-Rodríguez, S. Sundaresan, C. Kreibich, P. Gill, M. Allman, and V. Paxson. Haystack: A multi-purpose mobile vantage point in user space. 2016.

[6] H. Harkous, K. Fawaz, R. Leuret, F. Schaub, K. G. Shin, and K. Aberer. Polisis: Automated analysis and presentation of privacy policies using deep learning. USENIX, 2018.