




TrackerControl: Transparency and Choice around App Tracking

Konrad Kollnig¹ and Nigel Shadbolt¹

¹ Department of Computer Science, University of Oxford

DOI: [10.xxxxxx/draft](https://doi.org/10.xxxxxx/draft)

Software

- [Review](#) 
- [Repository](#) 
- [Archive](#) 

Editor: [Sebastian Benthall](#) 

Reviewers:

- [@gradvohl](#)
- [@gcdeshpande](#)

Submitted: 05 February 2022

Published: unpublished

License

Authors of papers retain copyright and release the work under a Creative Commons Attribution 4.0 International License ([CC BY 4.0](#)).

Summary

Third-party tracking allows companies to collect users' behavioural data, track their activity across digital devices, and potentially share this data with third-party companies. This can put deep insights into private lives into the hands of strangers, and often happens without the awareness of end-users. In light of this, we have developed TrackerControl, which aims to provide the interested individuals with real-time evidence of tracking.

Statement of need

In the past, the analysis of app tracking often used *off-device network analysis*, e.g. with Charles Proxy or mitmproxy ([Kollnig, Shuba, et al., 2021](#); [Ren et al., 2016](#); [Van Kleek et al., 2017](#)). Such analysis usually comes with the limitation that background system-level communication may be wrongly assigned to an app and taint the analysis results.

Other past studies have used *static analysis*, trying to gain insights into apps' data practices without executing them ([Egele et al., 2011](#); [Han et al., 2013](#)). Such static analysis has enabled the analysis of apps in the millions ([Binns et al., 2018](#); [Viennot et al., 2014](#); [Wang et al., 2018](#)), but usually does not to generate evidence of actual data transmission to trackers taking place, since apps are never run.

In response, past research has developed on-device network analysis tools ([Razaghpanah et al., 2018](#); [Shuba et al., 2018](#); [Song & Hengartner, 2015](#)). Most of these used to operate at a domain-level and provided limited insights into what companies actually receive data from end-users, or to what countries data is sent and for what purpose. Furthermore, none of the previous on-device network analysis tools had been deployed at scale and most remained research prototypes.

TrackerControl

To improve the quality of tracking analysis and make it available to a wide audience, we developed the Android app TrackerControl (TC). This app provides users with real-time evidence of app tracking. TC analyses the network traffic of other apps, by establishing a local VPN on the Android phone and matching all observed network traffic against a database of known tracking domains. This allows to generate factual evidence of what companies apps share data with, and support research (both academic and non-academic) on app privacy.

The tracking database behind TC is a unique feature of the app. The core of this database is the X-Ray 2020 database that is the product of significant research efforts over the past years ([Binns et al., 2018](#); [Kollnig, Binns, et al., 2021](#); [Kollnig, Shuba, et al., 2021](#); [Van Kleek et al., 2017](#)). This database has been created from analysing more than 2 million Android apps. The X-Ray 2020 is complemented by the Disconnect.me database, that is the foundation for tracker

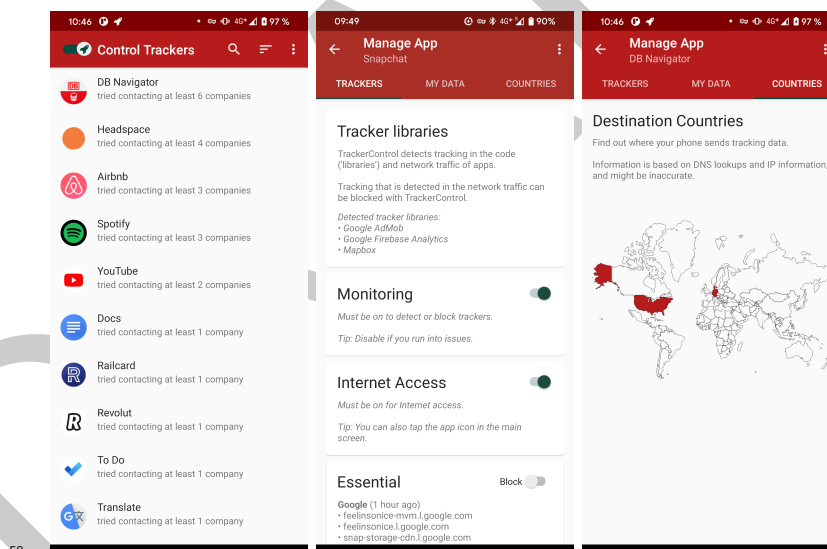
39 blocking in Mozilla Firefox on the web. We further integrate the commonly used StevenBlack
40 hostlist for tracking in apps, as a fallback. Overall, these databases provide information on
41 1) the *companies* behind tracking on the web and in apps, 2) the *countries* in which these
42 companies are based, 3) and the *purposes* for which tracking is conducted (e.g. Analytics or
43 Ads).

44 The core of TC builds on the NetGuard app, which is in active use by millions of users worldwide
45 (Bokhorst, 2021). The high maturity of NetGuard ensures reliability of tracker analysis whilst
46 minimising battery impact and supporting the long-term maintainability of TC.

47 In addition to providing insights into app tracking, users of TC can also block unwanted
48 transmissions, which has contributed to building a vibrant community of tens of thousands of
49 users. This community has helped make TC available in 19 languages.

50 TC has facilitated and inspired academic research at the intersection of policy and privacy
51 technology (Geier & Herrmann, 2021; Kollnig, Binns, et al., 2021). It has also been used by
52 the Finnish innovation fund Sitra for its 'Digipower investigation' into apps' data practices. As
53 part of this study, leading Finnish politicians and journalists used TrackerControl to analyse
54 the practices of Android apps. The results of this investigation will be presented at the Finnish
55 and European Parliament over the course of 2022. Both studies underline that TC can support
56 research into app privacy.

57 Screenshots



58
59 The left-hand screenshot shows the app overview. The middle screenshot shows the observed
60 tracking companies, domains and purposes for one app. The right-hand screenshot shows the
61 destinations of tracking data, obtained from the contacted IP addresses.

62 Acknowledgements

63 Konrad Kollnig was funded by the UK Engineering and Physical Sciences Research Council
64 (EPSRC) under grant number EP/R513295/1.

65 The underlying network analysis functionality is provided by the NetGuard Firewall, developed
66 by Marcel Bokhorst (Bokhorst, 2021).

67 TrackerControl would not have been possible without the help of many outstanding individuals,
68 including Max Van Kleek, Katherine Fletcher, George Chalhoub, and numerous app testers

69 and friends.

70 References

- 71 Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third
72 party tracking in the mobile ecosystem. *Proceedings of the 10th ACM Conference on Web*
73 *Science - WebSci '18*, 23–31. <https://doi.org/10.1145/3201064.3201089>
- 74 Bokhorst, M. (2021). NetGuard: A simple way to block access to the internet per app. In
75 *GitHub repository*. GitHub. <https://github.com/M66B/NetGuard>
- 76 Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011, January). PiOS: Detecting privacy leaks
77 in iOS applications. *Proceedings of NDSS 2011*.
- 78 Geier, O., & Herrmann, D. (2021). *The AppChk crowd-sourcing platform: Which third parties*
79 *are iOS apps talking to?* (pp. 228–241). https://doi.org/10.1007/978-3-030-78120-0_15
- 80 Han, J., Yan, Q., Gao, D., Zhou, J., & Deng, R. H. (2013). Comparing Mobile Privacy Pro-
81 tection through Cross-Platform Applications. *Proceedings 2013 Network and Distributed*
82 *System Security Symposium*, 16.
- 83 Kollnig, K., Binns, R., Dewitte, P., Kleek, M. V., Wang, G., Omeiza, D., Webb, H., &
84 Shadbolt, N. (2021). *A fait accompli? An empirical study into the absence of consent*
85 *to third-party tracking in android apps*. *Seventeenth Symposium on Usable Privacy and*
86 *Security (SOUPS 2021)*, 181–196. ISBN: 978-1-939133-25-0
- 87 Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., & Shadbolt, N. (2021). Are iPhones
88 really better for privacy? A comparative study of iOS and android apps. *arXiv Preprint*
89 *arXiv:2109.13722*.
- 90 Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich,
91 C., & Gill, P. (2018, February). Apps, trackers, privacy, and regulators: A global study
92 of the mobile tracking ecosystem. *Proceedings of NDSS 2018*. [https://doi.org/10.14722/](https://doi.org/10.14722/ndss.2018.23009)
93 [ndss.2018.23009](https://doi.org/10.14722/ndss.2018.23009)
- 94 Ren, J., Rao, A., Lindorfer, M., Legout, A., & Choffnes, D. (2016). ReCon: Revealing
95 and Controlling PII Leaks in Mobile Network Traffic. *Proceedings of the 14th Annual*
96 *International Conference on Mobile Systems, Applications, and Services - MobiSys '16*,
97 361–374. <https://doi.org/10.1145/2906388.2906392>
- 98 Shuba, A., Markopoulou, A., & Shafiq, Z. (2018). NoMoAds: Effective and efficient cross-
99 app mobile ad-blocking. *Proceedings on Privacy Enhancing Technologies 2018*, 125–140.
100 <https://doi.org/10.1515/popets-2018-0035>
- 101 Song, Y., & Hengartner, U. (2015). PrivacyGuard: A VPN-based platform to detect information
102 leakage on android devices. *Proceedings of the 5th Annual ACM CCS Workshop on Security*
103 *and Privacy in Smartphones and Mobile Devices*, 15–26. [https://doi.org/10.1145/2808117.](https://doi.org/10.1145/2808117.2808120)
104 [2808120](https://doi.org/10.1145/2808117.2808120)
- 105 Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., & Shadbolt, N. (2017).
106 Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps.
107 *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI*
108 *'17*, 5208–5220. <https://doi.org/10.1145/3025453.3025556>
- 109 Viennot, N., Garcia, E., & Nieh, J. (2014). A measurement study of Google Play. *The*
110 *2014 ACM International Conference on Measurement and Modeling of Computer Systems*,
111 221–233. <https://doi.org/10.1145/2591971.2592003>
- 112 Wang, H., Liu, Z., Liang, J., Vallina-Rodriguez, N., Guo, Y., Li, L., Tapiador, J., Cao,
113 J., & Xu, G. (2018). Beyond Google Play: A large-scale comparative study of Chinese

114 android app markets. *Proceedings of the Internet Measurement Conference 2018*, 293–307.
115 <https://doi.org/10.1145/3278532.3278558>

DRAFT