# TrackerControl: Transparency and Choice around App Tracking

Konrad Kollnig ⓘ [1] **and Nigel Shadbolt** ⓘ [1]

1 Department of Computer Science, University of Oxford

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 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, Binns, et al., 2022; 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 used *static analysis*, which tries 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, Lyngs, et al., 2018; Viennot et al., 2014; Wang et al., 2018), but does usually not 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 (Le et al., 2015; Razaghpanah et al., 2018; Shuba et al., 2018; Song & Hengartner, 2015). Most of these operated 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 the generation of factual evidence of what companies apps share data with, and can 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, Zhao, et al., 2018; Kollnig, Binns, Dewitte, et al., 2021; Kollnig, Shuba, Binns, et al., 2022; 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, which is the foundation for tracker blocking in Mozilla Firefox on the web. We further integrate the commonly used StevenBlack hostlist for tracking in apps, as a fallback. Overall, these databases provide information on 1) the *companies* behind tracking on the web and in apps, 2) the *countries* in which these companies are based, 3) and the *purposes* for which tracking is conducted (e.g., analytics or ads). The visualisation of tracking inside TC loosely follows the work by Van Kleek et al. (Van Kleek et al., 2017, 2018).
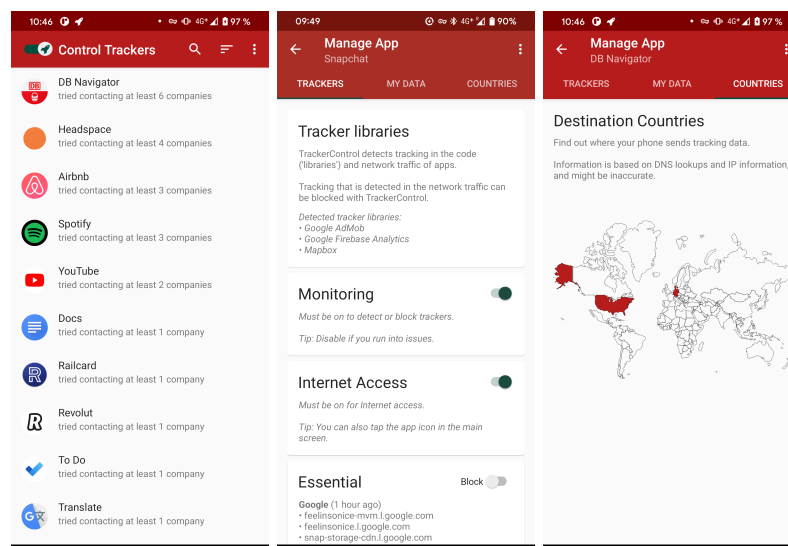
The core of TC builds on the NetGuard app, which is in active use by millions of users worldwide (Bokhorst, 2021). The high maturity of NetGuard ensures the reliability of the tracker analysis while minimising battery impact and supporting the long-term maintainability of TC. In addition to providing insights into app tracking, users of TC can also block unwanted network transmissions, which has contributed to building a vibrant community of tens of thousands of users. This community has helped make TC available in 20 languages.

Use in past and ongoing research

TC has faciliated and inspired academic research at the intersection of policy and privacy technolology (Geier & Herrmann, 2021; Kollnig, Binns, Dewitte, et al., 2021). It has also been used by the Finnish innovation fund Sitra for its 'Digipower investigation' into apps' data practices. As part of this study, leading Finnish politicians and journalists used TC to analyse the practices of Android apps. The results of this investigation will be presented at the Finnish and European Parliament over the course of 2022.

TC is also part of the PlatformControl toolkit (available at https://www.platformcontrol.org/), which forms the foundation of ongoing research efforts into app privacy as part of our research group at the University of Oxford (Kollnig, Binns, Dewitte, et al., 2021; Kollnig, Shuba, Van Kleek, et al., 2022; Kollnig, Binns, Van Kleek, et al., 2021; Kollnig, Shuba, Binns, et al., 2022, 2022).

Screenshots

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

Acknowledgements

References

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. *Proceedings of the 10th ACM Conference on Web Science - WebSci '18*, 23–31. https://doi.org/10.1145/3201064.3201089

Binns, R., Zhao, J., Kleek, M. V., & Shadbolt, N. (2018). Measuring third-party tracker power across web and mobile. *ACM Transactions on Internet Technology*, *18*(4), 1–22. https://doi.org/10.1145/3176246

Bokhorst, M. (2021). NetGuard: A simple way to block access to the internet per app. In *GitHub repository*. GitHub. https://github.com/M66B/NetGuard

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011, January). PiOS: Detecting privacy leaks in iOS applications. *Proceedings of NDSS 2011*.

Geier, O., & Herrmann, D. (2021). *The AppChk crowd-sourcing platform: Which third parties are iOS apps talking to?* (pp. 228–241). https://doi.org/10.1007/978-3-030-78120-0_15

Han, J., Yan, Q., Gao, D., Zhou, J., & Deng, R. H. (2013). Comparing mobile privacy protection through cross-platform applications. *Proceedings 2013 Network and Distributed System Security Symposium*, 16.

Kollnig, K., Binns, R., Dewitte, P., Kleek, M. V., Wang, G., Omeiza, D., Webb, H., & Shadbolt, N. (2021). A fait accompli? An empirical study into the absence of consent to third-party tracking in Android apps. *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 181–196. ISBN: 978-1-939133-25-0

Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C., & Shadbolt, N. (2021). Before and after GDPR: Tracking in mobile apps. *Internet Policy Review*, *10*(4). https://doi.org/10.14763/2021.4.1611

Kollnig, K., Shuba, A., Binns, R., Kleek, M. V., & Shadbolt, N. (2022). Are iPhones really better for privacy? A comparative study of iOS and Android apps. *Proceedings on Privacy Enhancing Technologies*, *2022*(2), 6–24. https://doi.org/10.2478/popets-2022-0033

Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., & Shadbolt, N. (2022). Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. *2022 ACM Conference on Fairness, Accountability, and Transparency*, 508–520. https://doi.org/10.1145/3531146.3533116

Le, A., Varmarken, J., Langhoff, S., Shuba, A., Gjoka, M., & Markopoulou, A. (2015). AntMonitor: A system for monitoring from mobile devices. *Proceedings of the 2015 ACM SIGCOMM Workshop on Crowdsourcing and Crowdsharing of Big (Internet) Data - C2b(1)D '15*, 15–20. https://doi.org/10.1145/2787394.2787396

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018, February). Apps, trackers, privacy, and regulators: A global study

---

of the mobile tracking ecosystem. *Proceedings of NDSS 2018*. https://doi.org/10.14722/ndss.2018.23009

Ren, J., Rao, A., Lindorfer, M., Legout, A., & Choffnes, D. (2016). ReCon: Revealing and controlling PII leaks in mobile network traffic. *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '16*, 361–374. https://doi.org/10.1145/2906388.2906392

Shuba, A., Markopoulou, A., & Shafiq, Z. (2018). NoMoAds: Effective and efficient cross-app mobile ad-blocking. *Proceedings on Privacy Enhancing Technologies 2018*, 125–140. https://doi.org/10.1515/popets-2018-0035

Song, Y., & Hengartner, U. (2015). PrivacyGuard: A VPN-based platform to detect information leakage on Android devices. *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, 15–26. https://doi.org/10.1145/2808117.2808120

Van Kleek, M., Binns, R., Zhao, J., Slack, A., Lee, S., Ottewell, D., & Shadbolt, N. (2018). X-Ray Refine: Supporting the exploration and refinement of information exposure resulting from smartphone apps. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–13. https://doi.org/10.1145/3173574.3173967

Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., & Shadbolt, N. (2017). Better the devil you know: Exposing the data sharing practices of smartphone apps. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, 5208–5220. https://doi.org/10.1145/3025453.3025556

Viennot, N., Garcia, E., & Nieh, J. (2014). A measurement study of Google Play. *The 2014 ACM International Conference on Measurement and Modeling of Computer Systems*, 221–233. https://doi.org/10.1145/2591971.2592003

Wang, H., Liu, Z., Liang, J., Vallina-Rodriguez, N., Guo, Y., Li, L., Tapiador, J., Cao, J., & Xu, G. (2018). Beyond Google Play: A large-scale comparative study of Chinese Android app markets. *Proceedings of the Internet Measurement Conference 2018*, 293–307. https://doi.org/10.1145/3278532.3278558