# Extended Abstract: Privacy Threats in Online Advertising

Maximilian Wittig
*University of Regensburg*

Doğan Kesdoğan
*University of Regensburg*

**Abstract** Today's market for digital advertising fails to protect the right to informational self-determination. We present a privacy threat model that explains at the process level the systematic debilitation of the user and its impact on society. Previous work has limited its analysis to the attacker's tracking capabilities. Our work adds to this literature by broadening the view of a system that *is* processing excessive amounts of user data. To this end, we explore the ability of the 'market' to control users' opinions, as they are technically unable to protect their personal data. The market is optimizing the personalization of advertising because it is more profitable than context-based advertising. This focus on individualization raises the privacy concern that users' perception and creativity will be limited by a lack of information, which in turn poses a risk to democracy. This threat arises from the interaction between technology and the business model.

**Introduction** On the Internet, a majority of services such as visiting websites, using mobile applications or e-mail services are free of charge, although the providers incur costs for development and maintenance. According to the free mentality, consumers are not willing to pay for digital products or services. Therefore, their business model is cross-financed by advertising, as alternative revenue models are not competitive. At the same time, the demand for online advertising (and thus ad space) is huge, since it leverages the internet's vast reach and targeting capabilities to connect with specific audiences. To choose a target, tracking services provide the market profiling information about the user's demographic data (age, gender, ethnicity) and habits (interests in certain topics). It is evident that the business model of online advertising, and therefore its infrastructure, is based on collecting as much information about users as possible.

**Threat Model** The goal of technical privacy is to ensure self-determination in the virtual world. It aims to recognize asymmetries of power when analyzing existing or planned systems. The aim is also to uncover undesirable developments

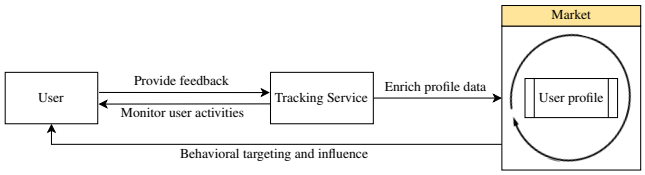


Figure 1: Privacy threat model in programmatic advertising

in the design of services and to make it more difficult for adversaries to realize their intentions to control and influence. However, the user's role in the ad-delivery process is limited due to a lack of knowledge and control. As society shifts towards digitizing lifestyles and managing their everyday tasks online, the ability of trackers to map online activities to interests and real-world behaviors is becoming more sophisticated. Consequently, the user can be more effectively influenced with targeted ads over time. As ad personalization increases conversion rates, user data has inevitably become an asset that is now exchanged throughout the online advertising infrastructure [11]. Within this convoluted ecosystem, a multitude of stakeholders exist, making it difficult for users to enforce their right to control their personal data. For example, which tracking company is authorized to collect data and for what purpose, and how can previously given consent be withdrawn and the data deleted? Prior work has shown the huge prevalence of tracking services on the Internet [4–7] and has shed light on how the tracking mechanisms work [1–3].

Fig. 1 shows the interactions between the main players. The market is responsible for the selection of targeted ad. With programmatic advertising, user impressions are automatically sold to the highest bidder in a real-time auction. Bidders may choose to target users of a specific application or website (contextual targeting), users who have previously interacted with products (re-targeting), users of specific areas (geotargeting), or users who seem to be interested in certain topics (behavioral targeting). To enable these targeting strategies, tracking services monitor the user's online activities to create a user profile that is shared with the market. Tracking services

collaborate with publishers in exchange for money to place their own scripts into the source code of the product. However, the user generally has no economic relationship with them or interest in exchanging data (nor is he aware of it). The goal of the promotional marketing message is to influence the user's opinion on a particular topic. By interacting (or not) with the product or an ad, the user gives feedback to the market, enabling it to select even more personalized ads in the future. As Google's Topic API on Web shows, the feedback does not have to be apparent to the user.

Overall, this opens two risks. First, it has been shown in the past that the tracking software can introduce technical errors into the original product, such as malvertising [8] and leaky HTTP forms [9]. Second, by learning the user's personality, the attacker can carry out more intelligent and targeted attacks. Here, the user's perception of information is selectively restricted in a self-learning loop. Limiting the choice of information threatens the creativity and innovative power of a society, as the freedom of personal development is hindered.

Our privacy threat model can be used to analyze solutions and their impact on the system at a meta level. For example, there are technical solutions that block the collection of data by tracking services and thus stop the learning process of the user profile, but also damage the market economically. Another approach attempts to reconcile the Internet's dominant business model and user privacy by creating behavioral profiles within the user domain, so that personal information is only disclosed to third parties on permission, which represents a more transparent form of feedback [10].

## References


[1] ACAR, G., EUBANK, C., ENGLEHARDT, S., JUAREZ, M., NARAYANAN, A., AND DIAZ, C. The web never forgets: Persistent tracking mechanisms in the wild. Association for Computing Machinery, pp. 674–689.

[2] BEKOS, P., PAPADOPOULOS, P., MARKATOS, E. P., AND KOURTELLIS, N. The hitchhiker's guide to facebook web tracking with invisible pixels and click ids.

[3] ECKERSLEY, P. How unique is your web browser? M. J. Atallah and N. J. Hopper, Eds., Springer Berlin Heidelberg.

[4] ENGLEHARDT, S., HAN, J., AND NARAYANAN, A. I never signed up for this! privacy implications of email tracking. *Proceedings on Privacy Enhancing Technologies* (2018).

[5] ENGLEHARDT, S., AND NARAYANAN, A. Online tracking: A 1-million-site measurement and analysis. p. 1388–1401.

[6] FOUAD, I., BIELOVA, N., LEGOUT, A., AND SARAFIJANOVIC-DJUKIC, N. Missed by filter lists: Detecting unknown third-party trackers with invisible pixels. *Proceedings on Privacy Enhancing Technologies 2020* (2020), 499–518.

[7] KOLLNIG, K., SHUBA, A., KLEEK, M. V., BINNS, R., AND SHADBOLT, N. Goodbye tracking? impact of ios app tracking transparency and privacy labels. Association for Computing Machinery, p. 508–520.

[8] SAKIB, M. N., AND HUANG, C.-T. Automated collection and analysis of malware disseminated via online advertising. vol. 1, pp. 1411–1416.

[9] SENOL, A., ACAR, G., HUMBERT, M., AND BORGESIUS, F. Z. Leaky forms: A study of email and password exfiltration before form submission. USENIX Association, pp. 1813–1830.

[10] TOUBIANA, V., NARAYANAN, A., BONEH, D., NISSENBAUM, H., AND BAROCAS, S. Adnostic: Privacy preserving targeted advertising.

[11] ZENG, E., MCAMIS, R., KOHNO, T., AND ROESNER, F. What factors affect targeting and bids in online advertising? a field measurement study. Association for Computing Machinery, pp. 210–229.