# Targeted Advertising With Total User Privacy

Morgan Saville

CAUSE

morgan@cause.cx

**Abstract**

**It is common for free platforms on the internet to use targeted advertising as a revenue stream, but this usually comes at the cost of user privacy. In this paper we propose a method of targeting advertising to users of an online platform without any of their data being collected or accessible. Broadly, this technique combines deep reinforcement learning (to learn user preferences) with cryptography (to prevent others, including the platform administrators, from accessing any private user data). Furthermore, we propose an algorithm which allows multiple platforms to benefit from these learned preferences while still maintaining user privacy.**

## 1 Introduction

This paper solves two main problems. The first is maximising the revenue of an individual platform without sacrificing user privacy. The second is generalising this technique such that it can be used across multiple platforms.

With respect to the first problem, we will define our criteria for success.

(1) No private user data should be accessible to other users of the platform, attackers, advertisers, or the platform itself.

(2) Subject to criterion (1), platform revenue must be maximised.

(3) Skeptical users must be able to verify criterion (1) if they so wish.

The success criteria for the second problem are as follows:

(4) Targeting technqiues acquired for a user on one participating platform must be usable for targeting on any other participating platform.

(5) Criterion (1) must hold across and within all participating platforms.

(6) Skeptical users must be able to verify criterion (5) if they so wish.

(7) No malicious agent can interfere with the targeting techniques for a general user (e.g., an advertiser making their ad show up more frequently than it should).

It is important to define what is meant by "private user data" in criterion (1). For the remainder of this paper, this term refers to any and all of the following:

- Any information which indicates which advertisements a given user has seen or interacted with.

- Any information about a given user's activities on a given platform.

In addition to these, we will use the term "private user data" to capture the intuitive notion of any data which a particularly privacy-concerned user might not want/expect anybody else to have access to.

Note that it is up to the individual platforms to decide how and why they store data when it comes to other parts of their platform. In this paper we are simply ensuring that no private user data is collected by the targeted advertising system itself. This is to say that just because a platform participates in the targeted advertising scheme described herein, it does not provide a guarantee that the platform maintains the same level of privacy across its other features.

An example of data which *must* be collected when advertising is when a user clicks on an ad which redirects them to the advertiser's website, the advertiser does need to know the platform from which the click originated (or something to this effect). This is necessary for the purpose of billing. However, we do not consider this a violation of privacy so long as the advertiser can not connect that interaction to a specific user account on the platform.

Furthermore, such an interaction may well result in the advertiser being able to associate the click with the IP address of the user. Particularly cautious users might consider using a VPN while browsing, or indeed the platform might want to provide

ads in forms other than hyperlinks. Suffice it to say that workarounds for this problem exist, but are beyond the scope of this paper. Instead we will focus only on ensuring privacy in the process of *deciding* which ads to show.