

## **Google's AI advertising revolution: More privacy, but problems remain**

April 2 2021, by David Murakami Wood and David Eliot



Credit: Google DeepMind from Pexels



In March 2021, Google announced that it was ending support for thirdparty cookies, and moving to "<u>a more privacy first web</u>." Even though the move was expected within the industry and by academics, there is still confusion about the new model, and cynicism about whether it truly constitutes the kind of revolution in online privacy that Google claims.

To assess this, we need to understand this new <u>model</u> and what is changing. The current advertising technology (adtech) approach is one in which platform corporations give us a "free" service in exchange for our data. The data is collected via third-party cookies downloaded to our devices, that allow a browser to record our internet activity. This is used to create profiles and predict our susceptibility to specific ad campaigns.

Recent advances have allowed digital advertisers to use deep learning, a form of artificial intelligence (AI) wherein humans do not set the parameters. Although more powerful, this is still consistent with the old model, relying on collecting and storing our data to train models and make predictions. Google's plans go further still.

## Patents and plans

All corporations have their <u>secret sauce</u>, and Google is more secretive than most. However, patents can reveal some of what they're up to. After an exploration of Google patents, we found U.S. patent <u>US10885549B1</u>, "Targeted advertising using temporal analysis of user-specific data": a patent for a system that predicts the effectiveness of ads based on a user's "temporal data," snapshots of what a user is doing at a specific point instead of indiscriminate mass data collection over a longer time period.

We can also make inferences by examining work from other organizations. Research funded by adtech company Bidtellect demonstrated that <u>long-term historical user data is not necessary to</u>



generate accurate predictions. They used deep learning to model users' interests from temporal data.

Alongside contextual advertising—which displays ads based on the content of the website on which they appear—this could lead to more privacy-conscious advertising. And without storing personally identifiable information, this approach would be compliant with progressive laws like the European Union's General Data Protection Regulation (GDPR).

Google has also released some information through the <u>Google Privacy</u> <u>Sandbox (GPS)</u>, a set of public proposals to restructure adtech. At its core are <u>Federated Learning Cohorts (FLoCs)</u>, a decentralized AI system deployed by the latest browsers. <u>As the Google AI blog explains</u>, federated learning differs from traditional machine learning techniques that collect and process data centrally. Instead, a deep learning model is downloaded temporarily onto a device, where it trains on our data, before returning to the server as an updated model to be combined with others.

With FLoCs, the deep learning model will be downloaded to Google Chrome browsers, and analyze local browser data. It then sorts the user into a "cohort," a group of a few thousand users sharing a set of traits identified by the model. It makes an encrypted copy of itself, deletes the original and sends the encrypted copy back to Google, leaving behind only a cohort number. Since each cohort contains thousands of users, Google maintains that the individual becomes virtually unidentifiable.

## **Cohorts and concerns**

In this new model, advertisers don't select individual characteristics to target, but instead advertise to a given cohort, <u>as Google's Github page</u> <u>explains</u>. Although FLoCs may sound less effective than collecting our



individual data, <u>Google claims</u> they realize "95 percent of the conversions per dollar spent when compared with cookie-based advertising."

The bidding process for ads will also take place on the browser, using another system <u>codenamed</u> "<u>Turtledove</u>." Soon, Google adtech will all work this way, contained on a web browser, making constant ad predictions based on our most recent actions, without collecting or storing personally identifiable information.

We see three key concerns. First, this is only part of a much larger AI picture Google is building across the internet. Through <u>Google Analytics</u>, for example, Google continues to use data gained from individual website-based first-person cookies to train machine learning models and potentially build individual profiles.

Secondly, does it matter how an organization comes to "know" us? Or is it the fact that it knows? Google is giving us back legally acceptable individual data privacy, however it is intensifying its ability to know us and commodify our online activity. Is privacy the right to control our individual data, or for the essence of ourselves to remain unknown without consent?

The final issue concerns AI. The limitations, biases and injustice around AI are now <u>a matter of widespread debate</u>. We need to understand how <u>deep learning</u> tools in FLoCs group us into cohorts, attribute qualities to cohorts and what those qualities represent. Otherwise, <u>like every</u> <u>previous marketing system</u>, FLoCs could further entrench socio-economic inequalities and divisions.

This article is republished from <u>The Conversation</u> under a Creative Commons license. Read the <u>original article</u>.



## Provided by The Conversation

Citation: Google's AI advertising revolution: More privacy, but problems remain (2021, April 2) retrieved 26 April 2024 from https://techxplore.com/news/2021-04-google-ai-advertising-revolution-privacy.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.