

Meta charging European users to remove ads is a privacy red herring

December 19 2023, by Ignacio Cofone



Credit: Unsplash/CC0 Public Domain

This November, Meta rolled out a new subscription model for Facebook

and Instagram users in the European Union, where they could pay a fee in exchange for [an ad-free browsing experience](#) on Facebook and Instagram. Referred to by critics as a "Pay or Okay" model, and [charging 9.99 to 12.99 euros monthly](#), the option is already an object of controversy.

Meta, among [many others](#), presented the new policy as a [privacy-preserving measure](#). Meta explains it responds to EU [privacy](#) regulations.

And opponents of this approach only partially disagree. The [Austrian Data Protection Authority](#), together with activist and lawyer Max Schrems and the [advocacy group NOYB](#), filed a complaint against Meta's new model. They argue that paying for privacy [breaches privacy as a fundamental right](#).

The European Consumer Organization also filed [an equivalent complaint](#). Asking to pay for privacy is wrong, the complaint argues, and asking to pay so much for it is worse.

But both those who are excited about privacy-preserving Facebook and Instagram versions, and the organizations that filed these complaints, miss the point: Meta doesn't provide any option to pay for privacy—in the EU or anywhere else.

Meta's business model relies on personal data

The issue is that users who choose the new option still have their information collected by Meta. The company declared that people who pay for the service will not have their information processed for [renting advertising spots on their accounts](#). It never promised that they wouldn't have their information collected or processed for other purposes.

Meta's objective isn't just to display ads to many people but also to make

its ads more effective through precise targeting. To do this, Meta collects information about its users, from their location and likes to their [browsing outside of the platform](#).

Meta's most valuable resource isn't your attention while you use Facebook for an hour or two, but what the accumulation of thousands of those hours provides. Your attention is valuable for a second, but [your information is useful forever](#); Meta can predict how likely a user is to buy a product when others with similar demographics clicked on it before.

It is unlikely that Meta will offer pay-for-privacy because it would lose enormous profits from advertisers if it stopped collecting data from paying users. If it did that and EU users opted for a payment-supported Facebook as opposed to an ad-supported one, it would miss out on ad accuracy for its non-EU users too. The monthly payments received would be unlikely to compensate for that large loss.

An additional revenue stream

Avoiding ads can make scrolling through Facebook and Instagram more enjoyable, but paying to avoid them doesn't change Meta's privacy problem. The privacy problem with Meta's business model isn't that it shows ads but rather what it does to make them valuable: collecting [personal information](#) and subjecting it to Meta's data practices.

Although ads are the public face of Meta's business model, the real profit and potential harms lie in its data practices. Renting ad spots generates revenue, but the heart of both Meta's business model and its privacy problem is what it does to improve them. In that context, Facebook's paid version is an additional revenue stream rather than a commitment to more ethical data practices or a breach of fundamental rights.

A more pleasant, ad-free browsing experience is a convenience that, in fact, may increase the amount of time people spend on the platform, allowing for more [personal data](#) to be collected.

Beyond Facebook

Facebook is one example of a ubiquitous business model in the information economy.

The real cost of services in the information economy isn't their monthly fee. Whether we send money to paid services that also collect our data like Amazon Prime, Netflix, Spotify and Uber, or we instead see ads, doesn't change our harm exposure. There's nothing wrong, from a privacy perspective, with paying to remove ads. What entities do with our data poses long-term risks [beyond our immediate browsing experience](#).

So users who opt for paid alternatives aren't exempt from most of the cost. The Cambridge Analytica scandal, where personal information from millions was exploited for political purposes, illustrates one of the long-term risks of data accumulation. Facebook's data practices had consequences far beyond ad targeting. The risk of data misuse and data breaches grows as [more information is gathered](#).

More robust rules

Ultimately, it's not the ads, but the way companies [obtain, use, and share personal data](#) that needs attention and reform. Relying on individual users to opt out, whether paying or for free, is insufficient. It places the burden on each of them to navigate [complicated and technical yet ambiguous privacy settings on countless platforms](#).

Rather than by supporting or opposing new options to pay to avoid targeted ads, the way to reduce harm in the data economy is to develop [more robust rules](#) to govern the collection and processing of people's data. Useful protections are those that apply [regardless of what options users click](#).

The takeaway from the controversy shouldn't be to stop the new—and currently Meta-specific—business model in which people can pay for ad removal. Rather, it should be to stop the old, internet-wide, business model in which companies collect and use people's data with insufficient commitments to keep them safe.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Meta charging European users to remove ads is a privacy red herring (2023, December 19) retrieved 29 April 2024 from <https://techxplore.com/news/2023-12-meta-european-users-ads-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.