App Tracking Transparency and eCommerce Ads

Author: Eric Silberstein

Claps: 90

Date: Mar 3, 2022

Thereâ€™s been a lot of talk recently about how ecommerce ads on Facebook are becoming less effective due to the new Apple / iOS user tracking policies. I was reading the Stratechery post about Shopify last week and realized I donâ€™t understand, at a technical level, why Appleâ€™s App Tracking Transparency system prevents Facebook from attributing ecommerce ads. In the Klaviyo tradition of working transparently, hereâ€™s my record of chasing that question down.

Firstâ€¦is this even a real issue? Seems to be. On Metaâ€™s Q4 earnings call, CFO Dave Wehner said (my bolding):

> But, obviously, as we go into 2022, weâ€™re going to be lapping a period in which in Q1 and Q2, those headwinds were not in place in the year-ago period. So that definitely makes for a tough comp in the first half of the year. **And, you know, we believe the impact of iOS overall as a headwind on our business in 2022 is on the order of $10 billion**, so itâ€™s a pretty significant headwind for our business. And, you know, weâ€™re seeing that impact, you know, in a number of verticals.
>
> **E-commerce was an area where we saw, you know, a meaningful slowdown in growth in Q4.** And similarly, weâ€™ve seen other areas like gaming be a challenge. But, you know, on e-commerce, you know, itâ€™s quite noticeable â€” notable that Google called out, seeing strength in that very same vertical. **And so, you know, given that we know that e-commerce is one of the most impacted verticals from iOS restrictions, it makes sense that those restrictions are probably part of the explanation for the difference between what they were seeing and what we were seeing.**
>
> And if you look at it, you know, we believe those restrictions from Apple are designed in a way that carves out browsers from the tracking prompts Apple requires for apps. And so, you know, what that means is that search ads, you know, could have access to far more third-party data for measurement and optimization purposes than app-based ad platforms like ours. So, you know, when it comes to using data, you can think of it â€” you know, thereâ€™s â€” it is not really apples-to-apples for us. And as a result, you know, we believe Google Search ad business could have benefited relative to services like ours is based a different set of restrictions from Apple.

I asked our VP of Performance Marketing Greg Such about it and hereâ€™s what he slacked back:

> There is a huge component of loss of efficacyâ€¦even beyond if there is a loss of tracking and conversion tracking. If we break down what made Facebook successful was its ability to target on your behalf. Amassing their various data points, they built such an efficient targeting model that the ad buyer basically did nothing. Facebook said put 0 targeting parameters on your campaign. Based on the conversion tag on

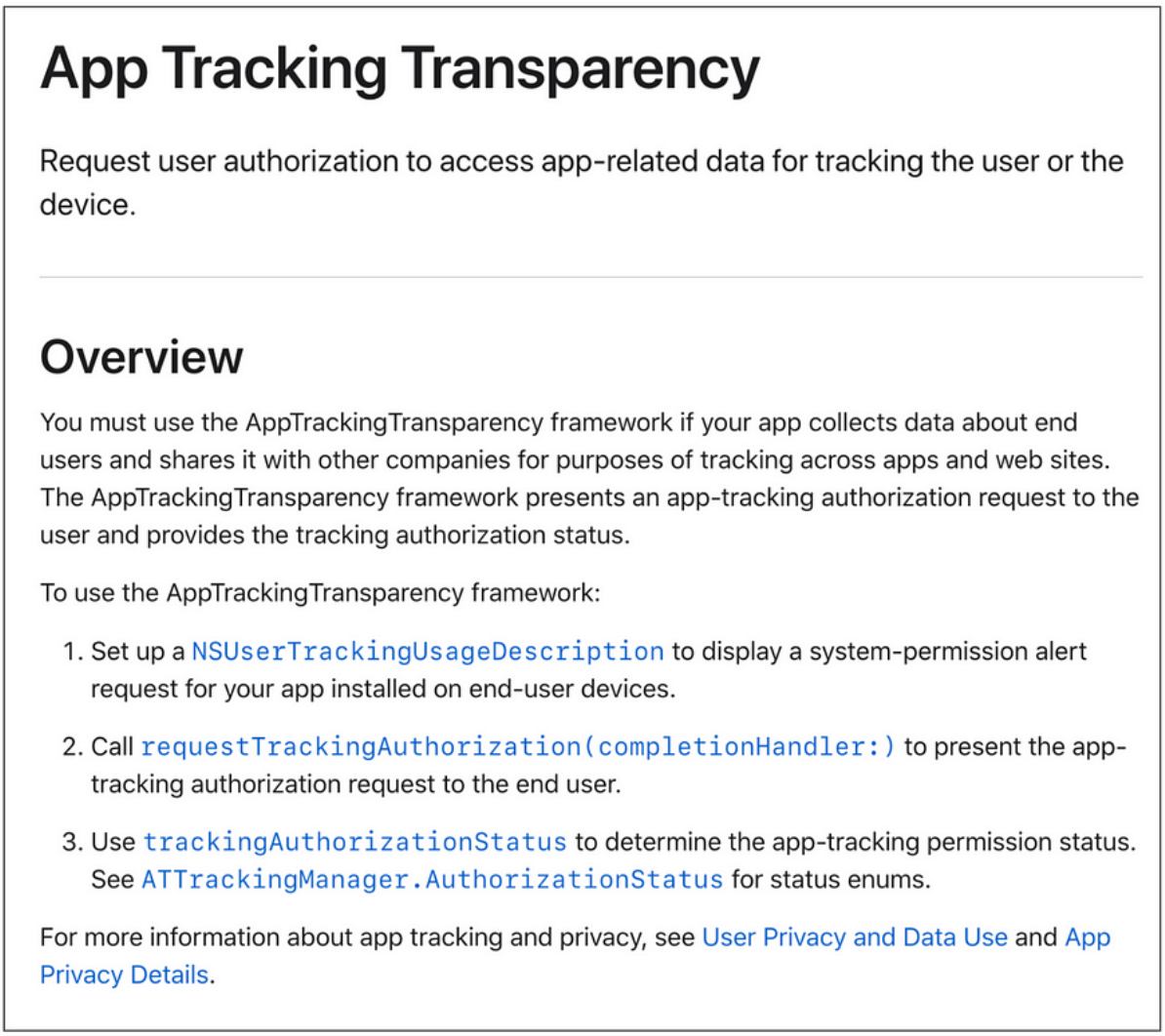
> your website, we will determine who to target based on certain propensities that will make your ad buying as effective as possible. So just tell them the CPA you would like to pay and the budget and it will do the rest. But these user-level data points must have been highly aggregated from usage tracking outside of the FB app â€” now prevented by FB. So now that the targeting has gone to hell, the buying platform is less accurate, costs on ad buyers have gone up â€” it is no longer as reliable. So to me, this is much more than deterministic tracking, but tracking that influenced effectiveness of ad targeting is the culprit.

So whatâ€™s going on technically? I assume App Tracking Transparency controls access to IDFA (ID for Advertisers). Way back, an iOS app could read the MAC address off the phone. Then, to protect privacy, Apple removed that ability, but added IDFA. An app could read the IDFA unless the phone user changed privacy settings, and the phone user could also reset their IDFA. With IDFA, the basic advertising flow must work something like this:

1. Youâ€™re using the Facebook app (or Instagram, Messenger, WhatsApp) on iOS
2. Facebook has your IDFA (they can read it off your device, which they likely did a long time ago and they have a list of all the IDFAs theyâ€™ve ever seen for you)
3. Your feed shows an ad for some other app, letâ€™s say a mobile game called Car Crash
4. Youâ€™re enticed so you tap the ad and install Car Crash
5. Car Crash contains a Facebook iOS SDK
6. The first time you launch Car Crash, the SDK reads your IDFA and tells Facebook
7. You make your first in-app purchase. The app uses the SDK to tell Facebook.

=> Now Facebook can close the attribution loop. They know the ad was served to you, you installed the app, and you made an in-app purchase. This lets them report on ad performance and tune targeting to find more people like you who will install Car Crash and make in-app purchases.

But now Appleâ€™s App Tracking Transparency framework is in useâ€¦



App Tracking Transparency

Request user authorization to access app-related data for tracking the user or the device.

Overview

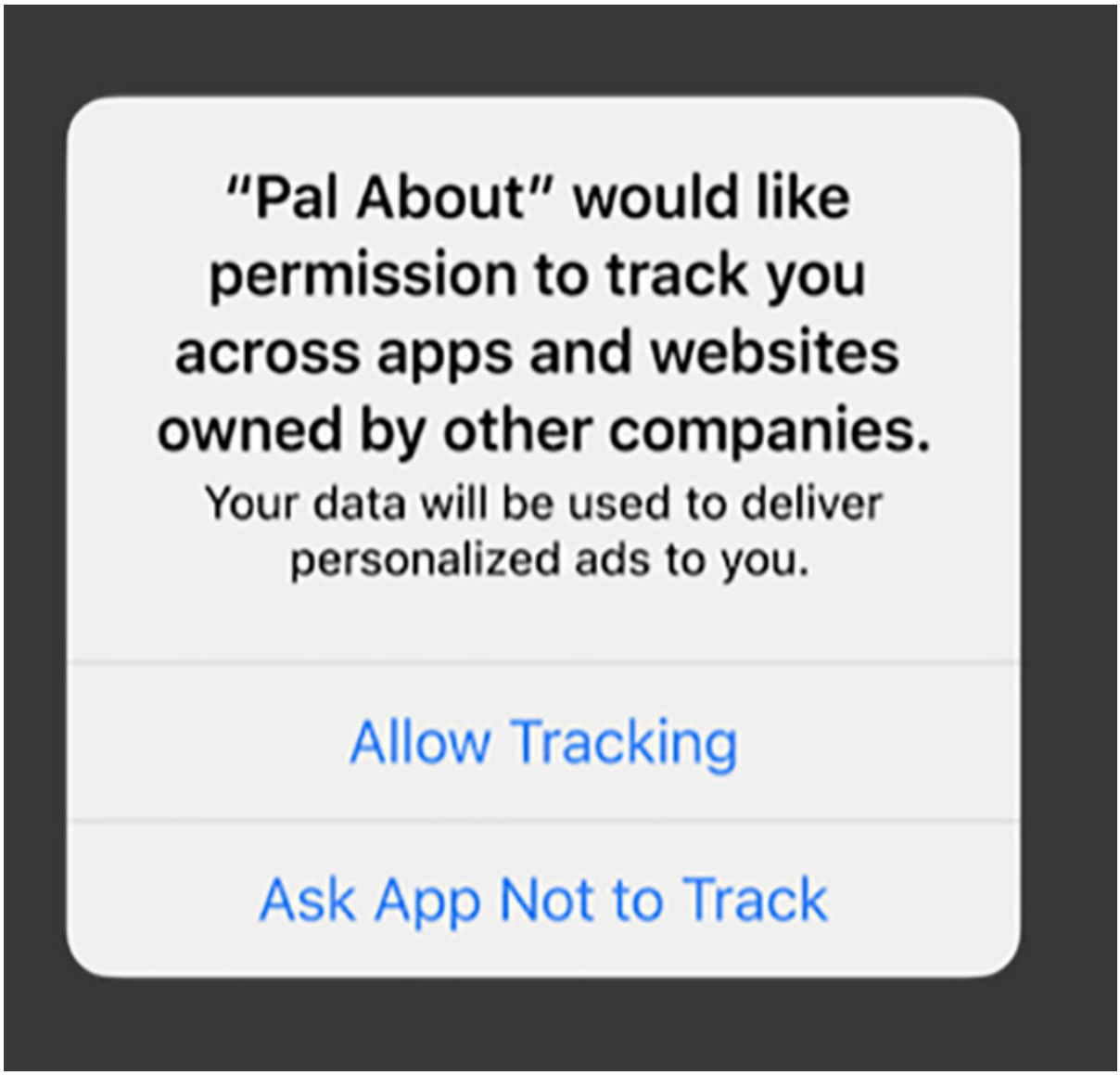
You must use the AppTrackingTransparency framework if your app collects data about end users and shares it with other companies for purposes of tracking across apps and web sites. The AppTrackingTransparency framework presents an app-tracking authorization request to the user and provides the tracking authorization status.

To use the AppTrackingTransparency framework:

1. Set up a `NSUserTrackingUsageDescription` to display a system-permission alert request for your app installed on end-user devices.
2. Call `requestTrackingAuthorization(completionHandler:)` to present the app-tracking authorization request to the end user.
3. Use `trackingAuthorizationStatus` to determine the app-tracking permission status. See `ATTrackingManager.AuthorizationStatus` for status enums.

For more information about app tracking and privacy, see User Privacy and Data Use and App Privacy Details.

â€¦which means an iOS app canâ€™t read the IDFA unless the user agrees to be tracked through a prompt like this:



At a purely technical level (i.e. ignoring policies, terms of service, etc.), this means that in step 6 above, Car Crash is unlikely to be able to read your IDFA. (If youâ€™re installing a game why would you think â€" yes, I want it to track me.) In step 2 above, if you had just installed Facebook, it too would not be able to get your IDFA. (Presumably Facebook already has billions of IDFAs, but over time, as people get new phones, they wonâ€™t be able to read the new ones for people who opt out.) Overall, the ad attribution loop canâ€™t be closed, at least not easily and with certainty.

(Now if Car Crash was also owned/published by Facebook, they could use IDFV = ID for Vendors, and they could close the loop. This gives a hint as to why there is consolidation in the app gaming space.)

I believe app advertising is a huge business for Facebook (although not immediately finding numbers on that), and I now get why App Tracking Transparency would throw off app advertising, but what does that have to do with ecommerce? In ecommerce the funnel (e.g. browse, add to cart, purchase) takes place on a web site. What does IDFA have to do with that?

Hereâ€™s a version of the flow above for ecommerce:

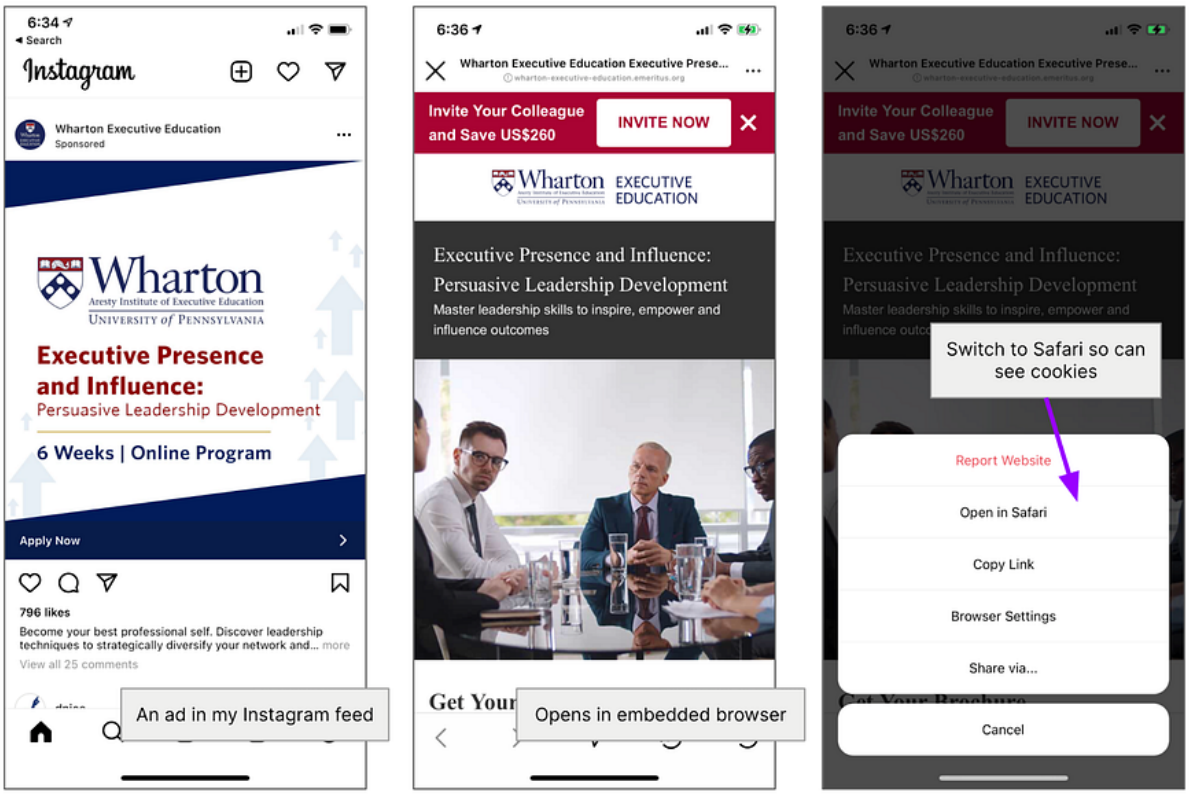
1. Youâ€™re using the Facebook app (or Instagram, Messenger, WhatsApp) on iOS (wow â€" 94% of Metaâ€™s ad revenue is from mobile)

2. Your feed shows an ad for a sweater from Yarn and Thread
3. Youâ€™re enticed so you tap â€œBuy Nowâ€
4. Now youâ€™re on the Yarn and Thread website, probably on the browser embedded in Facebook, Facebookâ€™s â€œpixelâ€ javascript is running on the page, and it knows who you are and/or about the ad you tapped because that information was passed through URL query params
5. Facebookâ€™s javascript sets a cookie identifying you, or reads one it set earlier
6. You buy the sweater
7. Facebookâ€™s javascript sends Facebook an event indicating you purchased

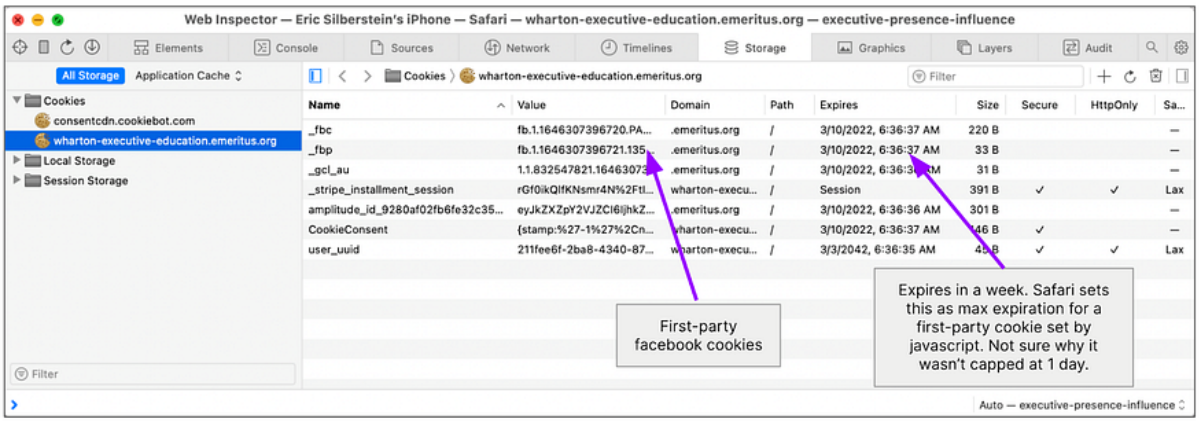
=> Now Facebook can close the attribution loop. They know the ad was served to you and it resulted in a conversion.

(Even this simple flow raises questions. For example, if you initially view the product in the embedded browser, but donâ€™t buy, and later you go directly to the page in mobile Safari and buy, does Facebook know who you are and will they attribute the ad? There are many, many ways Facebook can stitch things together. For example, they might have earlier set a first-party cookie on the â€œYarn and Threadâ€ site. Or, if not Safari, they could set a third-party cookie on the site. They could be using probabilistic technology based on clues like IP address, browser type, etc. to figure out that youâ€™re you. With over $110B in advertising revenue last year, the ROI is probably there to engineer all of this stitching together technology for even obscure cases.)

Hereâ€™s an ad in my Instagram feed:



And here are the cookies that get set by Facebook:



Thatâ€™s all consistent with the flow I outlined above.

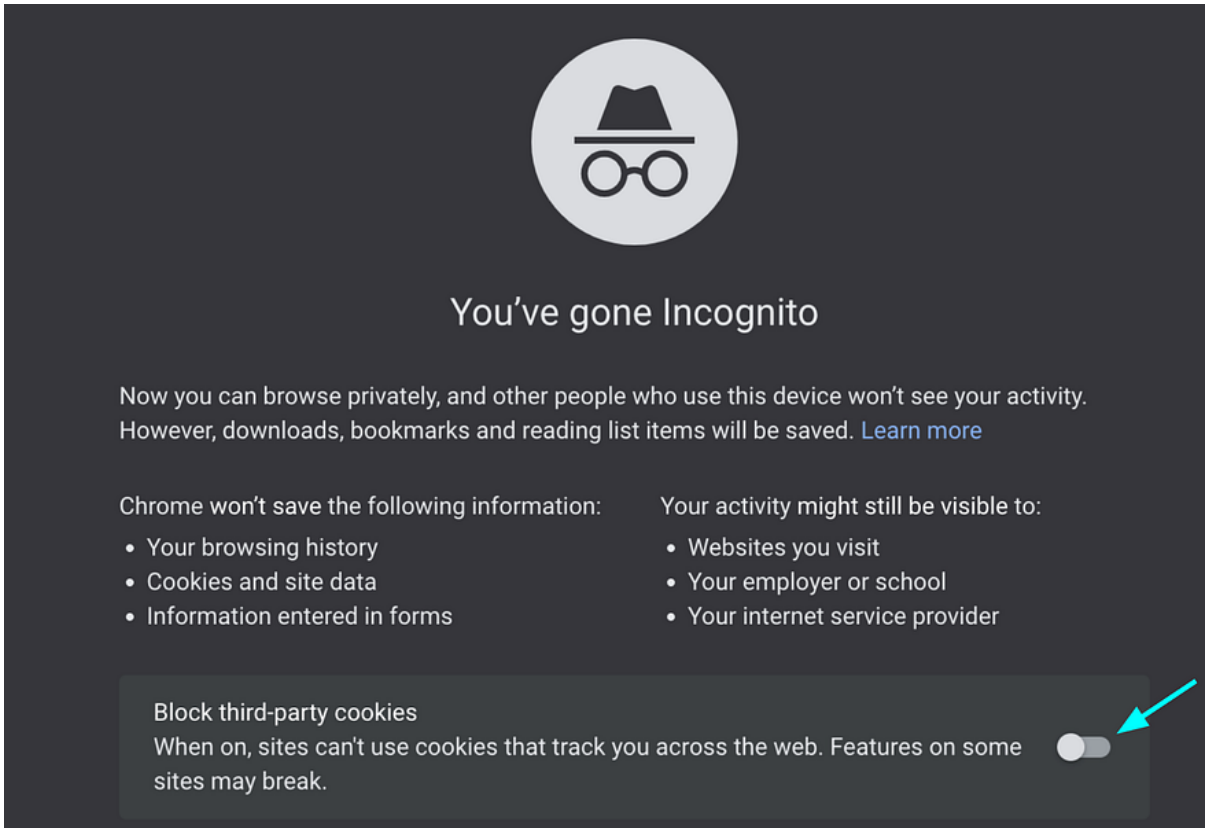
Letâ€™s create a toy example to see some of this tracking from the Facebook side.

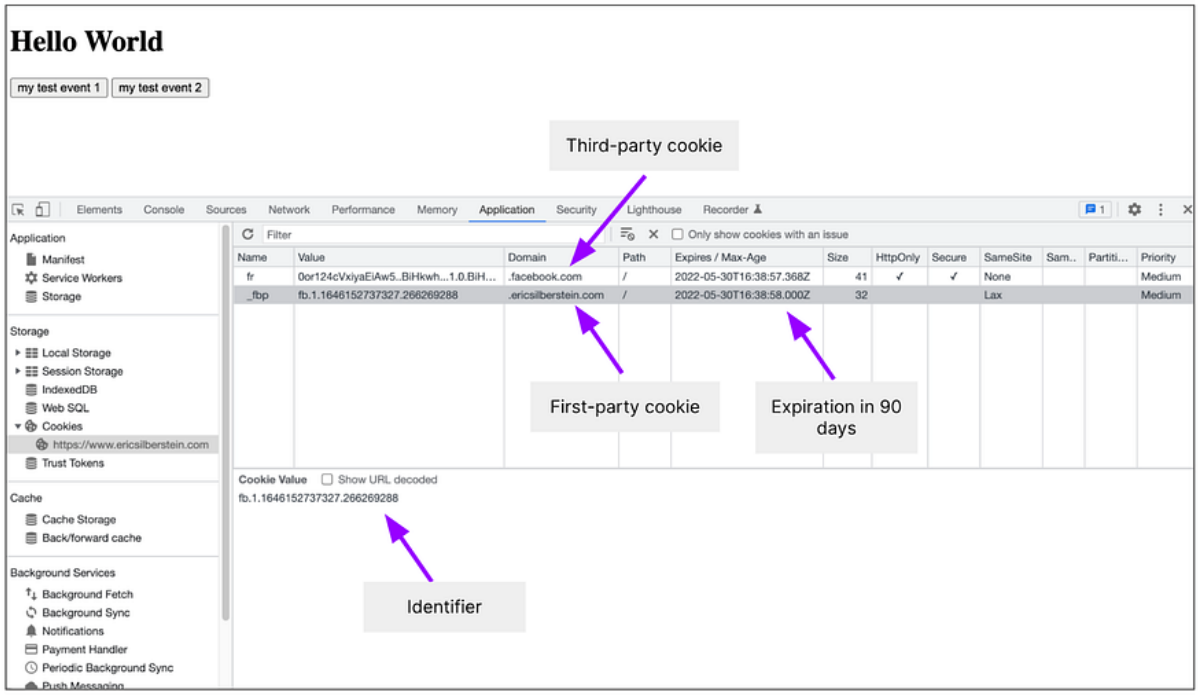
Using a Facebook ad account I created for something else last year, Iâ€™m â€œinstallingâ€ the Facebook pixel on this page.

(Why are these snippets of javascript called pixels? It dates back to earlier when you placed a one-by-one pixel blank jpg or gif on your page with a URL from an analytics or ad site. The GET request for that image would tell the ad server that the page was loaded, and the third-party cookie the ad server set/received in the HTTP header would tell who was doing the loading.)

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <!-- Facebook Pixel Code -->
    <script>
    !function(f,b,e,v,n,t,s)
    {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
    n.callMethod.apply(n,arguments):n.queue.push(arguments)};
    if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
    n.queue=[];t=b.createElement(e);t.async=!0;
    t.src=v;s=b.getElementsByTagName(e)[0];
    s.parentNode.insertBefore(t,s)}(window, document,'script',
    'https://connect.facebook.net/en_US/fbevents.js');
    fbq('init', 'XXXXXXXXXXXXXXX');
    fbq('track', 'PageView');
    </script>
    <noscript><img height="1" width="1" style="display:none"
    src="https://www.facebook.com/tr?id=244380074197461&ev=PageView&noscript=1"
    /></noscript>
    <!-- End Facebook Pixel Code -->
  </head>
  <body>
    <h1>Hello World</h1>
    <button onClick="fbq('track', 'my-test-event-1');">my test event 1</button>
    <button onClick="fbq('track', 'my-test-event-2');">my test event 2</button>
  </body>
</html>
```

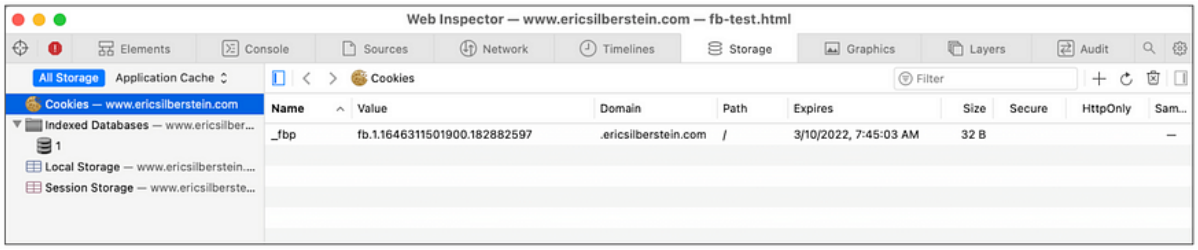
Letâ€™s access this page in Chrome with third-party cookies turned on.



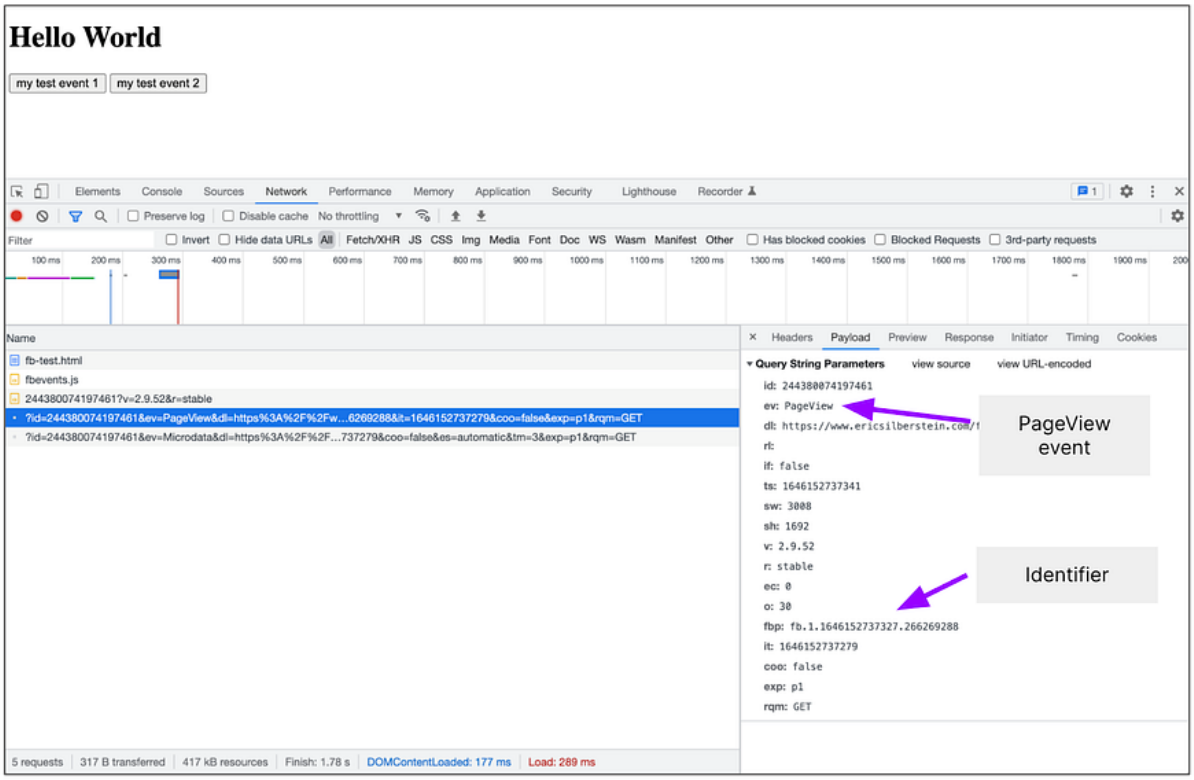


The Facebook javascript sets a first-party cookie and a third-party cookie. Both are set to expire in 90 days. Both contain identifiers.

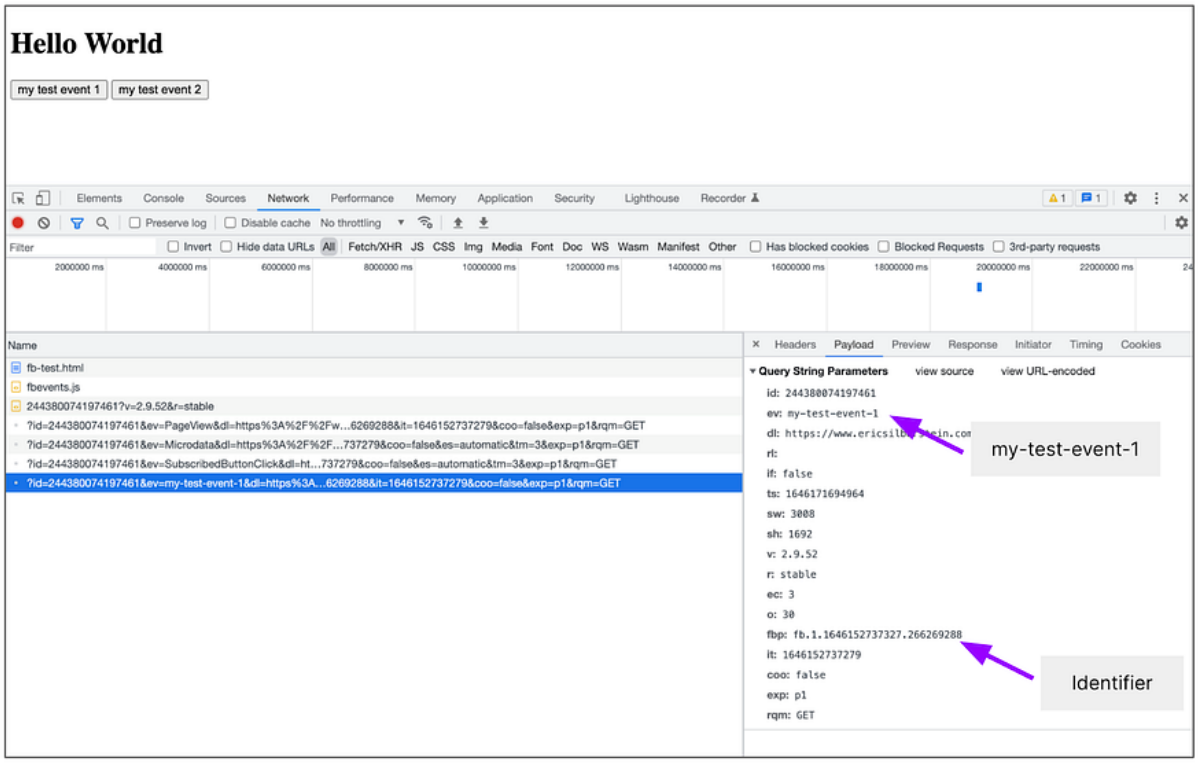
(In Safari, it can only set a first-party cookie and that cookie expires in a week.)



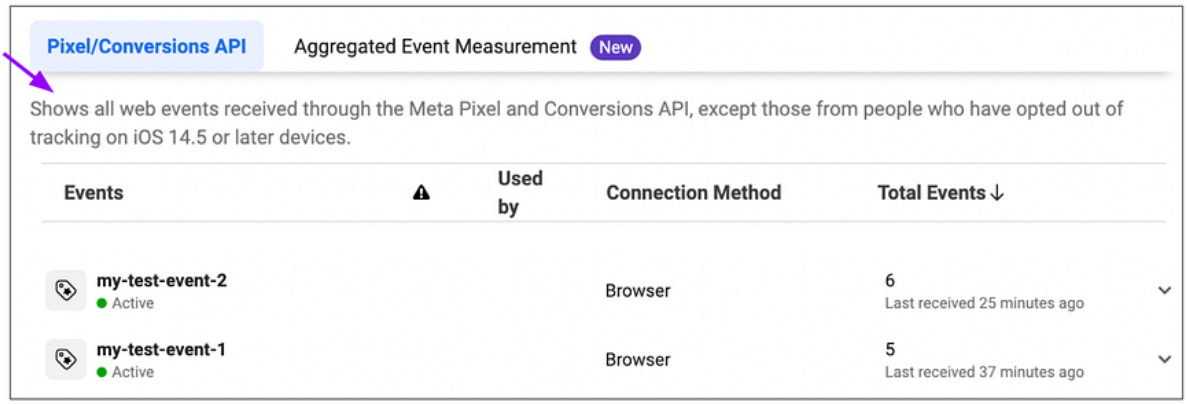
Javascript told Facebook about the page load:



And when I click the â€œmy test event 1â€ button (think of that like add to cart), as expected, it tells Facebook:



Now letâ€™s look at the Facebook page that shows incoming events:



Aha! What jumps out right away is the message â€œShows all web events received through the Meta Pixel and Conversions API, except those from people who have opted out of tracking on iOS 14.5 or later devices.â€

So first, this has nothing to do with IDFA â€” nothing about IDFA would block javascript from sending events from a web page.

Second, what exactly does â€œpeople who have opted outâ€ mean? People who are using a browser embedded in an app in which the user opted out of tracking? Anyone who ever opted out of tracking from any Meta app (Facebook, Instagram, Messenger, etc.) regardless of if they are currently on mobile or desktop?

What seems clear is the inability to close the attribution loop for ecommerce, unlike for apps, is **not enforced by technology.**

Letâ€™s look at the terms of App Tracking Transparency. From the Apple developer page on User Privacy and Data Use (my bolding):

> **Asking Permission to Track**
>
> With iOS 14.5, iPadOS 14.5, and tvOS 14.5 and later, you need to receive the userâ€™s permission through the AppTrackingTransparency framework in order to track them or access their deviceâ€™s advertising identifier. **Tracking refers to the act of linking user or device data collected from your app with user or device data collected from other companiesâ€™ apps, websites, or offline properties for targeted advertising or advertising measurement purposes.** Tracking also refers to sharing user or device data with data brokers.

This seems pretty clear. The flow described above links user device data from the Facebook app to websites from another company. Itâ€™s really as simple as Apple is prohibiting what used to be standard practice. Here are some other things that were standard practice that are also prohibited (my bolding):

> Examples of tracking include, but are not limited to:
>
> **Displaying targeted advertisements in your app based on user data collected from apps and websites owned by other companies.**
>
> Sharing device location data or email lists with a data broker.
>
> **Sharing a list of emails, advertising IDs, or other IDs with a third-party advertising network that uses that information to retarget those users in other developersâ€™ apps or to find similar users.**
>
> Placing a third-party SDK in your app that combines user data from your app with user data from other developersâ€™ apps to target advertising or measure advertising efficiency, even if you donâ€™t use the SDK for these purposes. For example, using an analytics SDK that repurposes the data it collects from your app to enable targeted advertising in other developersâ€™ apps.

There is also an FAQ section on that page and these questions are relevant:

> **If a user provides permission for tracking via a separate process on our website, but declines permission in the app tracking transparency prompt, can I track that user across apps and websites owned by other companies?**
>
> Developers must get permission via the app tracking transparency prompt for data thatâ€™s collected in the app and used for tracking. Data collected separately, outside of the app and not related to the app, is not in scope.
>
> **What identifiers or data are governed by the â€œtrackingâ€ policy?**
>
> Any user or device level identifier that is used to join data from your app with data from third parties (including SDKs used in your app) for purposes of advertising or ad measurement or sharing with a data broker. This includes, but is not limited to, the deviceâ€™s advertising identifier, session ID, fingerprint IDs, and device graph identifiers. If your app receives or shares any of these identifiers for the above listed purposes, you must use the AppTrackingTransparency framework to obtain user consent.

Further down on that same page Apple talks about Private Click Measurement:

> Apple supports Private Click Measurement for iOS and iPadOS apps, in addition to websites. Advertising networks can now measure the effectiveness of advertisement

clicks within iOS or iPadOS apps that navigate to a website. This information can be used to understand which advertisements drive conversions (such as purchases or signups) â€” while maintaining user privacy.

Described here, the idea is to allow enough information to be passed back for an advertiser or algorithm to measure the conversions from an ad and, for example, tell which creative does better, without allowing so much information to be passed back that conversions can be linked to individuals.

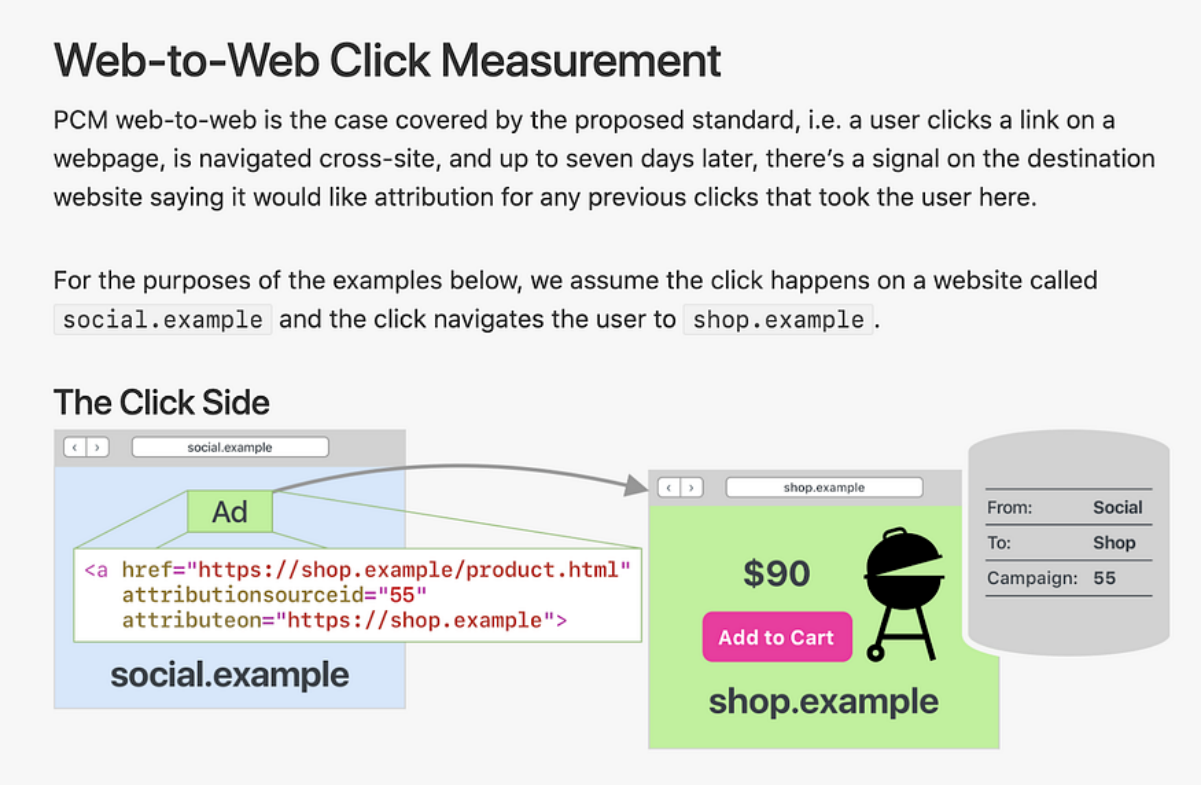


Diagram from the WebKit blog post linked above showing how PCM works

In this approach, the userâ€™s web browser (Safari/WebKit only at least for now I imagine) retains certain tracking information and later passes an attribution report back to the ad serving site. The content and timing of the report are such that the ad system will not usually be able to tie the conversion event to an individual. The system will work for web-to-web and app-to-web. The app to web example is what we want in the ecommerce flow outlined above. Not sure if app developers who had this capability for over a decade would be as excited as John Wilander who wrote the blog post: â€œThis is exciting â€” weâ€™re adding the capability to measure ad clicks from iOS and iPadOS apps to Safari!â€

Does Facebook already support this? It seems like they are supporting something that follows the same rules (i.e. has the same limitations) but perhaps is not actually using WebKit Private Click Management. The Meta article How the Apple iOS 14 Release May Affect Your Ads and Reporting says (my bolding):

> Specifically, Apple requires that apps in the App Store that engage in what Apple defines as â€œtrackingâ€ to show a prompt on iOS 14.5 or later devices, in accordance with their AppTrackingTransparency framework. Appleâ€™s policy prohibits certain data collection and sharing unless people opt into tracking on iOS 14.5 or later devices via the prompt. As a result, ads personalization and performance reporting may be limited for both app and web conversion events.

> In response to these changes, we are processing pixel conversion events and app events from iOS 14.5 or later devices using **Aggregated Event Measurement**. This will help support your efforts to preserve user privacy and help you run effective campaigns.

The Meta article About Aggregated Event Measurement says:

> Metaâ€™s Aggregated Event Measurement is a protocol that allows for measurement of web and app events from people using iOS 14.5 or later devices. Aggregated Event Measurement limits domains and mobile apps to 8 conversion events that can be configured and prioritized for Aggregated Event Measurement reporting. At this time, only prioritized events can use Aggregated Event Measurement data to help improve conversion optimization.
>
> â€¦
>
> Our solution is meant to limit the amount of personal data used to facilitate conversion reporting and ads optimization, **but itâ€™s designed to solve for key advertiser use cases not addressed by Appleâ€™s Private Click Measurement tool**. Aggregated Event Measurement will continue to evolve with upcoming browser changes to help our advertisers support consumer privacy.

And there are even more details about how this all works in this article: Meta Pixel Updates for Appleâ€™s iOS 14 Requirements.

Circling back to my original question about why Appleâ€™s App Tracking Transparency system prevents Facebook from attributing ecommerce ads, the answer turns out to be simple â€” **Appleâ€™s new policies prohibit it unless the user agrees to be tracked**.

Two other observations from this exploration:

First, yes, I donâ€™t like being tracked, but these rules create some unfortunate incentives. If you think about the rules from the standpoint of a merchant, the merchant is no longer allowed to say to the place theyâ€™re advertising, â€œHey, you know that person Xavier Kim you sent my way. He liked what he saw and he boughtâ€¦so if you see other people like Xavier tell them about me.â€ But if the sale happens in the same location as where the ad is shown, say within Instagram, then Facebook has complete information, and can therefore optimize advertising. This will push merchants away from the open internet where interactions and transactions happen on owned sites, and toward selling their products on the big guys. Do we really want even more stuff to happen on Facebook? And from a merchant standpoint, in a few years, theyâ€™ll have the same problem as with business pages. They spent all this effort getting people to â€œlikeâ€ their pages, but now they have to pay Facebook to communicate with those people.

Secondâ€¦this stuff is way more complicated than I thought. I spent a day or two on this. You could easily spend months understanding the regulations, policies, standards, techniques, and workarounds for tracking and ad attribution. And itâ€™s getting way more complicated as the world figures out how to balance privacy with ad measurement and optimization. Advertising is importantâ€¦but is it *that* important? It feels like way too much brain power is going into this areaâ€¦I now better understand that quote â€œThe best minds of my generation are thinking about how to make people click ads.â€