



Should brands ditch Facebook ads as part of a privacy transformation?

By [Ram Prabhakar](#) | March 21, 2022

(Last Updated On: March 22, 2022)



When it comes to online advertising, data is everything. So let's look at some:

More than [230 million Americans are active on Facebook](#). They make up a substantial slice of the \$189bn global mobile marketing industry. Facebook ads drive 32 billion calls per year to American businesses. 26% of users who click a Facebook ad go on to make a purchase. By most metrics, Facebook advertising offers one of the best potential ROIs of any form of direct marketing.

But here's some other data to throw into the mix.

79% of consumers say concerns about data privacy would influence purchasing decisions or impact their connection with a brand. More than 60% of Americans [don't trust Facebook with their data](#).

Until recently, no serious brand would even wonder if they should quit advertising on Facebook. The very fact that the question arises now, is because of data.

Big Data means big concerns

The success of Facebook advertising has been built on its unmatched ability to harvest data at will from almost every corner of the internet. Integration with apps and the use of Facebook tracking Pixels allowed it to track people's behavior, not just on its own platforms but across the whole range of online interactions from websites to apps. Understanding user behaviors in such depth meant Facebook adverts could target consumers at the most granular level and measure impact in exceptional detail. But when data gets that big, it gets noticed.

Data privacy has become a political as well as a business and consumer issue. Legislation such as GDPR in the EU and CCPA in the US has affected every aspect of customer data handling, but in particular marketing. But the real game changer, and one having a measurable impact right now, is the response to the issue from Big Tech itself.

Last year, Apple introduced privacy features in its mobile OS that effectively killed Facebook's ability to track in-app behavior. App users are now specifically asked if they want to allow Facebook to track them. Unsurprisingly, [almost all of them say no](#). The effect on Facebook



advertising has been dramatic, contributing to a \$230bn drop in Facebook/Meta's market value, with some leading industry figures claiming [Facebook advertising has had its day](#).

[Now Google is following suit](#). Over the next two years it will start to limit sharing of user data with third parties and operate without cross-app identifiers, including advertising ID. The third party cookie – the biggest tool in the data harvesting kit – is disappearing.

What does all this mean for Facebook advertising?

In the short term at least, it means a lot. It means an estimated \$10bn drop in advertising revenue for Facebook and that in turn will inevitably mean higher costs for advertisers to make up the shortfall. And it means that you, as a brand, will need to work a lot harder - or certainly a lot smarter - to find your audience on Facebook. Already, the privacy changes mean it is considerably harder to get accurate conversion data, and to retarget users who have interacted with your brand but not actively given consent to be tracked.

Does this mean you should re-consider advertising on Facebook at all?

In a word, no. But it may mean a change of approach.

In many ways, data-gathering by Facebook until recently has been a little like the Wild West – an unruly, seemingly lawless place where fortunes can be made if you turn a blind eye to some less-than-perfectly-ethical practices. But, just like the old West, the coming of law and order might see the end of the quick-buck mentality but usher in a period of sustained and stable growth that is ultimately far more profitable for everyone. It will also be a place where your business can operate without damaging the precious resource of trust you've built up with your customer base.



There will be short-term challenges, but online marketing is too big an industry, and too reliant on data, to step back this far without already having plans to jump forward again.

Facebook, along with Google and other major platforms, is already exploring options to gather data in a more privacy-focused way. [Facebook itself talks about PETs](#) (Privacy Enhancing Technologies) as the driver of “next generation digital advertising”. Technologies such as Secure Multi-Party Computation, where personal data is made shareable while remaining securely depersonalized, will eventually fill the information void left by the current restrictions on data-gathering.



The seismic shock of Apple’s privacy changes are unlikely to repeat with Google. Google is delaying the full implementation of its new privacy policy for two years, and with good reason. It relies on user data as much as Facebook for its multi-billion dollar advertising business. You can be sure Google is confident that, come 2023, new tech will be in place that makes up for the loss of valuable data the new rules cause.



Right now, it is harder than it has been to make advertising pay on Facebook, but the long-term picture is better, both in terms of advertiser reach and, importantly, consumer trust and brand reputation.

So what can brand advertisers do in the meantime?

Be ethical, be smart. Consent is the keyword, and if you are compliant with existing data regulation you will already have this from your key customers. Your customer list is going to become more important than ever.

Use Custom Audiences

Third party data is the sticking point, so you need to leverage first party data more than ever. Facebook gives you the ability to [create your own custom audiences for adverts](#), using data from customer lists, offline activity and web-based activity where your customers have willingly given you their data. For this reason, you may need to focus more of your advertising efforts on email gathering through lead generation or conversion ads.

Use Facebook Data

Much of the data Facebook has on users is considered first party, as users have directly given it to Facebook. This might include: location, demographics, interests etc. Using [Broad Targeting](#) and [Expansion Targeting](#) becomes more important as it utilizes Facebook data effectively to segment audiences around specific personas rather than actual individuals.

Use Server-Side tracking

While Facebook pixels now learn less about customer behavior in browsers, Facebook has introduced its [Conversions API](#), which provides more information about how users interact with your own back-end systems online, such as your CRM or ecommerce platform. While not perfect, in conjunction with pixels, this can make up for a lot of the conversion data that might otherwise be missing.



Diversify into Context Advertising

In the face of all the changes, many leading brands are taking the opportunity to explore other advertising options. There is particular interest in the power of context advertising – targeting content your customers are interested in rather than customers themselves. This can be highly effective: a customer might feel far more positively about your brand if you appeared just when they were actively researching topics related to your products, rather than getting that nagging feeling that you are somehow following them online.

In a nutshell

Your customers care about privacy, and the online environment is moving only in one direction: towards a more data-secure, depersonalized understanding of audiences. Changes, for better or worse, are happening fast and while Facebook remains an essential part of any online advertising strategy, the biggest guarantee that you aren't adversely affected by change means curating your own client data by building direct relationships with them that can be used with, but aren't overly-reliant on, the ever-changing whims of Big Tech.