

Facebook knows literally everything about you

Behind every feature, Facebook is collecting data

10 months ago



Cambridge Analytica may have [used](#) Facebook's data to influence your political opinions. But why does least-liked tech company **Facebook** have all this data about its users in the first place?

Let's put aside Instagram, WhatsApp and other Facebook products for a minute. Facebook has built the world's biggest social network. But that's not what they sell. You've probably heard the internet saying "if a product is free, it means that you are the product."

And it's particularly true in this case because Facebook is the world's

second biggest advertising company in the world behind Google. During the last quarter of 2017, Facebook [reported](#) \$12.97 billion in revenue, including \$12.78 billion from ads.

That's 98.5 percent of Facebook's revenue coming from ads.

Ads aren't necessarily a bad thing. But Facebook has reached [ad saturation](#) in the newsfeed. So the company has two options — creating new products and ad formats, or optimizing those sponsored posts.

This isn't a zero-sum game — Facebook has been doing both at the same time. That's why you're seeing more ads on Instagram and Messenger. And that's also why ads on Facebook seem more relevant than ever.

Facebook has reached ad saturation in the newsfeed

If Facebook can show you relevant ads and you end up clicking more often on those ads, then advertisers will pay Facebook more money.

So Facebook has been collecting as much personal data about you as possible — it's all about showing you the best ad. The company knows your interests, what you buy, where you go and who you're sleeping with.

You can't hide from Facebook

Facebook's terms and conditions are [a giant lie](#). They are purposely misleading, too long and too broad. So you can't just read the company's terms of service and understand what it knows about you.

That's why some people have been downloading their Facebook data. You can do it too, it's quite easy. Just head over to your [Facebook settings](#) and click the tiny link that says "Download a copy of your Facebook data."

In that archive file, you'll find your photos, your posts, your events, etc. But

if you keep digging, you'll also find your private messages on Messenger (by default, nothing is encrypted).

And if you keep digging a bit more, chances are you'll also find your entire address book and even metadata about your SMS messages and phone calls.

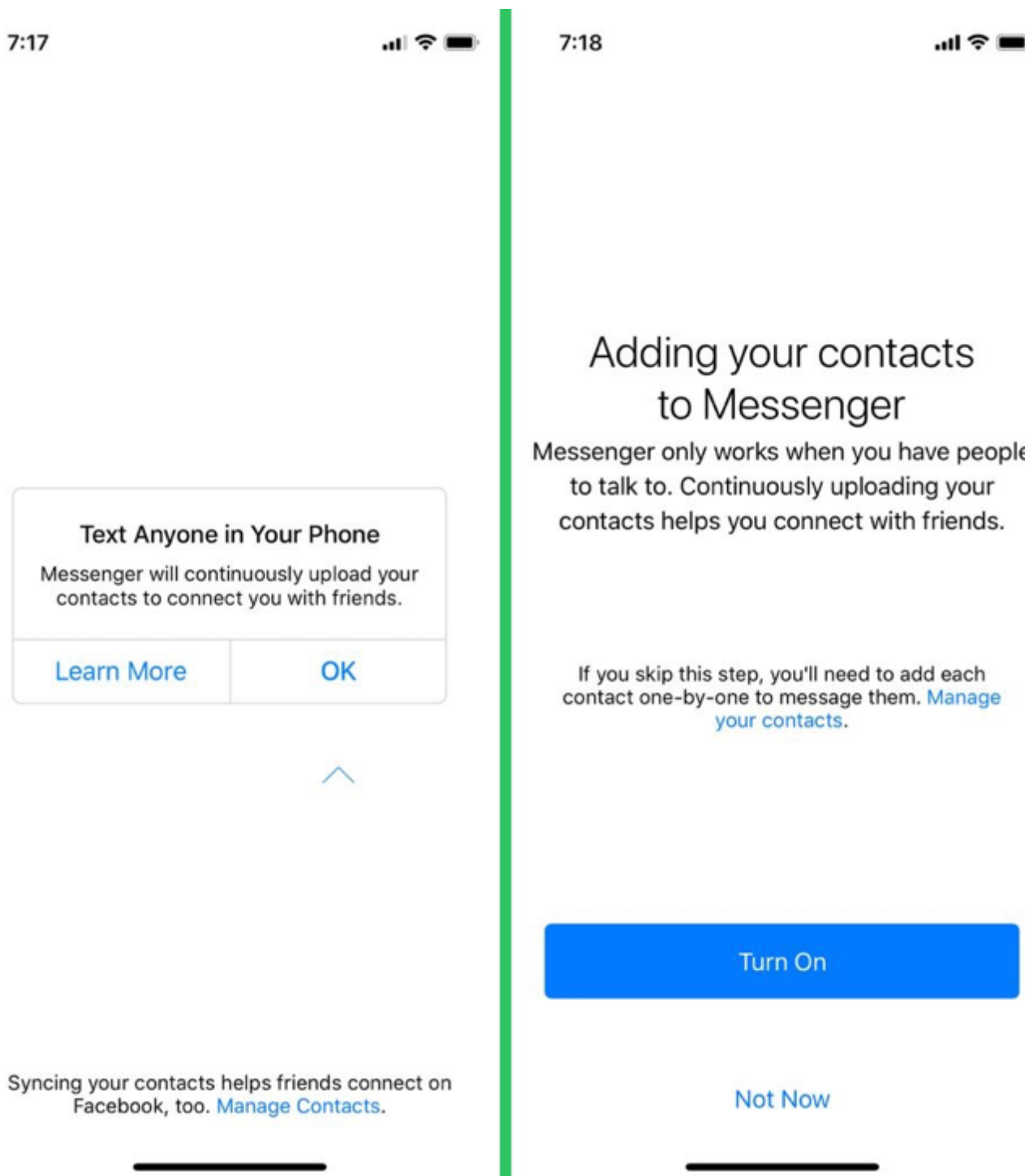
All of this is by design and you agreed to it. Facebook has unified terms of service and share user data across all its apps and services (except WhatsApp data in Europe [for now](#)). So if you follow a clothing brand on Instagram, you could see an ad from this brand on Facebook.com.

Messaging apps are privacy traps

But Facebook has also been using this trick quite a lot with Messenger. You might not remember, but the on-boarding experience on Messenger is really aggressive.

On iOS, the app shows you a fake permission popup to access your address book that says "Ok" or "Learn More". The company is using a fake popup because you can't ask for permission twice.

There's a *blinking arrow* below the OK button.



If you click on “Learn More”, you get a giant blue button that says “Turn On”. Everything about this screen is misleading and Messenger tries to manipulate your emotions.

“Messenger only works when you have people to talk to,” it says. Nobody wants to be lonely, that’s why Facebook implies that turning on this option will give you friends.

Even worse, it says “if you skip this step, you’ll need to add each contact one-by-one to message them.” This is simply a lie as you can automatically talk to your Facebook friends using Messenger without adding them one-by-one.

If you tap on “Not Now”, Messenger will show you a fake notification every now and then to push you to enable contact syncing. If you tap on yes and disable it later, Facebook [still keeps all your contacts](#) on its servers.

On Android, you can let Messenger [manage your SMS messages](#). Of course, you guessed it, Facebook uploads all your metadata. Facebook knows who you’re texting, when, how often.

Even if you disable it later, Facebook will keep this data for later reference.

But Facebook doesn’t stop there. The company knows a lot more about you than what you can find in your downloaded archive. The company asks you to share your location with your friends. The company tracks your web history on nearly every website on earth using embedded JavaScript.

But my favorite thing is probably peer-to-peer payments. In some countries, you can [pay back your friends](#) using Messenger. It’s free! You just have to add your card to the app.

It turns out that Facebook also buys data about your [offline purchases](#). The next time you pay for a burrito with your credit card, Facebook will learn

The next time you pay for a burrito with your credit card, Facebook will learn about this transaction and match this credit card number with the one you added in Messenger

about this transaction and match this credit card number with the one you added in Messenger.

In other words, Messenger is a great Trojan horse designed to learn everything about you.

And the next time an app asks you to share your address book, there's a 99-percent chance that this app is going to mine your address book to get new users, spam your friends, improve ad targeting and sell email addresses to marketing companies.

I could say the same thing about all the other permission popups on your phone. Be careful when you install an app from the Play Store or open an app for the first time on iOS. It's easier to enable something if a feature doesn't work without it than to find out that Facebook knows everything about you.

GDPR to the rescue

There's one last hope. And that hope is GDPR. I encourage you to read TechCrunch's Natasha Lomas excellent [explanation of GDPR](#) to understand what the European regulation is all about.

Many of the misleading things that are currently happening at Facebook will have to change. You can't force people to opt in like in Messenger. Data collection should be minimized to essential features. And Facebook will have to explain why it needs all this data to its users.

If Facebook doesn't comply, the company will have to pay up to 4 percent of its global annual turnover. But that doesn't stop you from actively reclaiming your online privacy right now.

You can't be invisible on the internet, but you have to be conscious about what's happening behind your back. Every time a company asks you to tap OK, think about what's behind this popup. You can't say that nobody told

you.