Sample op-ed

**You Gave Facebook Your Number For Security. They Used It For Ads.**

By Gennie Gebhart, Sept 27, 2018

Published by Electronic Frontier Foundation

<https://www.eff.org/deeplinks/2018/09/you-gave-facebook-your-number-security-they-used-it-ads>

Add “a phone number I never gave Facebook for targeted advertising” to the list of deceptive and invasive ways Facebook makes money off your personal information. Contrary to user expectations and Facebook representatives’ own previous statements, the company has been using contact information that users explicitly provided for security purposes—or that users *never provided at all*—for targeted advertising.

A group of academic researchers from [Northeastern University and Princeton University](https://mislove.org/publications/PII-PETS.pdf), along with [Gizmodo reporters](https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051), have used real-world tests to demonstrate how Facebook’s latest deceptive practice works. They found that Facebook harvests user phone numbers for targeted advertising in two disturbing ways: two-factor authentication (2FA) phone numbers, and “shadow” contact information.

### Two-Factor Authentication Is Not The Problem

First, when a user gives Facebook their number for security purposes—to [set up 2FA](https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts), or to receive alerts about new logins to their account—that phone number can become fair game for advertisers within weeks. (This is not the first time Facebook has [misused 2FA phone numbers](https://gizmodo.com/facebook-turned-its-two-factor-security-feature-into-th-1823006334).)

But the important message for users is: **this is not a reason to turn off or avoid 2FA.** The problem is not with two-factor authentication. It’s not even a problem with the inherent [weaknesses of SMS-based 2FA in particular](https://krebsonsecurity.com/2016/09/the-limits-of-sms-for-2-factor-authentication/). Instead, this is a problem with how Facebook has handled users’ information and violated their reasonable security and privacy expectations.

There are [many types of 2FA](https://www.eff.org/deeplinks/2017/09/guide-common-types-two-factor-authentication-web). SMS-based 2FA requires a phone number, so you can receive a text with a “second factor” code when you log in. Other types of 2FA—like authenticator apps and hardware tokens—do not require a phone number to work. However, until just [four months ago](https://www.facebook.com/notes/facebook-security/two-factor-authentication-for-facebook-now-easier-to-set-up/10155341377090766/), Facebook required users to enter a phone number to turn on *any* type of 2FA, even though it offers its authenticator as a more secure alternative. Other companies—[Google notable among them](https://www.eff.org/deeplinks/2016/12/2017-wishlist)—also still follow that outdated practice.

Even with the welcome move to no longer require phone numbers for 2FA, Facebook still has work to do here. This finding has not only validated users who are suspicious of Facebook's repeated claims that we have “[complete control](https://www.eff.org/deeplinks/2018/04/facebook-not-what-complete-user-control-looks)” over our own information, but has also seriously damaged users’ trust in a foundational security practice.

Until Facebook and other companies do better, users who need privacy and security most—especially those for whom using an authenticator app or hardware key is not feasible—will be forced into a corner.

### Shadow Contact Information

Second, Facebook is *also* grabbing your contact information from your friends. Kash Hill of *Gizmodo* provides [an example](https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051):

...if User A, whom we’ll call Anna, shares her contacts with Facebook, including a previously unknown phone number for User B, whom we’ll call Ben, advertisers will be able to target Ben with an ad using that phone number, which I call “shadow contact information,” about a month later.

This means that, even if you never directly handed a particular phone number over to Facebook, advertisers may nevertheless be able to associate it with your account based on your friends’ phone books.

Even worse, none of this is accessible or transparent to users. You can’t find such “shadow” contact information in the “contact and basic info” section of your profile; users in Europe can’t even get their hands on it despite [explicit requirements under the GDPR](https://gdpr-info.eu/art-15-gdpr/) that a company give users a “[right to know](https://www.eff.org/deeplinks/2018/07/new-rules-protect-data-privacy-where-focus-what-avoid)” what information it has on them.

As Facebook attempts to salvage its reputation among users in the wake of the [Cambridge Analytica scandal](https://www.eff.org/deeplinks/2018/04/what-we-want-learn-zuckerbergs-congressional-testimonies-week), it needs to put its money [where its mouth is](https://www.facebook.com/zuck/posts/10104712037900071). Wiping 2FA numbers and “shadow” contact data from non-essential use would be a good start.