

Facebook slammed for 'cheap trick' to defraud people to accept privacy policy

By News.com.au

[Facebook slammed for 'cheap trick' to get people to accept privacy policy.](#)

Shutterstock

ORIGINALLY PUBLISHED BY:



As digital companies grapple with new data protection laws for consumers in Europe, Facebook has been slammed for a cheap trick it used in an apparent attempt to get users to hastily accept a privacy policy that didn't comply with the new laws.

Social media sites use all sorts of methods to hold your attention and keep you coming back. You haven't been on LinkedIn in a while? All of a sudden you get an email telling you a recruiter was looking at your page. You haven't opened Instagram for some time? You soon find yourself getting a lot more push notifications about videos your friends are posting.

Other tricks are more subtle like when you log onto Twitter and there's a brief pause before your notifications pop up — that's designed to keep you in suspense the same way the final reel of a pinball machine can take an extra second to fall into place.

These sorts of things are part and parcel of using such services. But when you're used to manipulating users, it can be easy to



M

O

d

a

l

T

ri

g

g

e

r

overstep the mark — and Facebook appears to have done just that.

The European Union's much-touted General Data Protection Regulation (GDPR) came into effect in May, prompting people's **inboxes to fill** with emails from companies about updates to their privacy policy and how they use customer data, in order to comply with the new rules.

But according to a complaint filed by the European Center for Digital Rights on behalf of an anonymous complainant, Facebook used deceptive pressure tactics to get people to accept its privacy policy in violation of the GDPR.

The complaint alleges that Facebook blocked users' accounts if they did not consent and used "tricks" to get people to agree in the form of enticing them with fake message notifications to pressure them to click through so they could see the notifications.

"[Facebook] used additional 'tricks' to pressure the users: For example, the consent page included two fake red dots ... that indicated that the user has new messages and notifications, which he/she cannot access without consenting — even if the user did not have such notifications or messages in reality," the complaint reads.

Facebook has been contacted for comment on the complaint.

Facebook actually put *fake red dots* to try and make you think you have messages even if you don't, so you agree to their tracking more hastily. Read full complaint against Facebook: <https://t.co/uI5fYairtK> – with tricks like that, sorry Facebook, you deserve to be hit hard. pic.twitter.com/inThjgPoov

— Francis Irving (@frabcus) **May 28, 2018**

The company has only just recovered from a **global privacy scandal** and the reaction on social media was damning.

“This is disappointing, Facebook. You are losing users’ trust for a reason,” wrote Tristan Harris, founder of Center for Humane Technology who has been **described by The Atlantic** as the “closest thing Silicon Valley has to a conscience.”

Harris spent three years as a Google design ethicist developing a framework for how technology should ethically steer the thoughts and actions of billions of people.

Others who don’t spend their days grappling with such pertinent tech issues were equally admonishing of Facebook’s newest boondoggle.

“Wow. That’s disgustingly devious. But brilliant, as idea,” **wrote one Twitter user.**

Facebook is the second biggest digital advertiser and in the world and more data equals more money, so naturally it wants as few restrictions around how it uses that data as possible.

The company recently **moved the physical location of its servers** holding user data outside of the EU as a way to skirt the GDPR for non-EU residents.

What does the GDPR mean for you?

Years in the making, the GDPR rules are prompting companies to rewrite their privacy policies and in some cases (like Microsoft announced) apply the European Union’s tougher standards in other regions where privacy laws are weak. Although they take effect as Facebook faces an enormous privacy crisis, that timing is largely coincidental.

The regulation has little relevance for the United States, but any company with customers in the EU, if they offer goods and services in the EU, or if they monitor the behavior of individuals in the EU will be affected.

Ultimately not much will change for you. Companies will keep on collecting and analyzing personal data from your phone, the apps you use and the sites you visit. The big difference is that now the companies will have to justify why they're collecting and using that information. And they're prevented from using data for a different purpose later, the Associated Press reported.

FILED UNDER DIGITAL PRIVACY, FACEBOOK, SOCIAL MEDIA