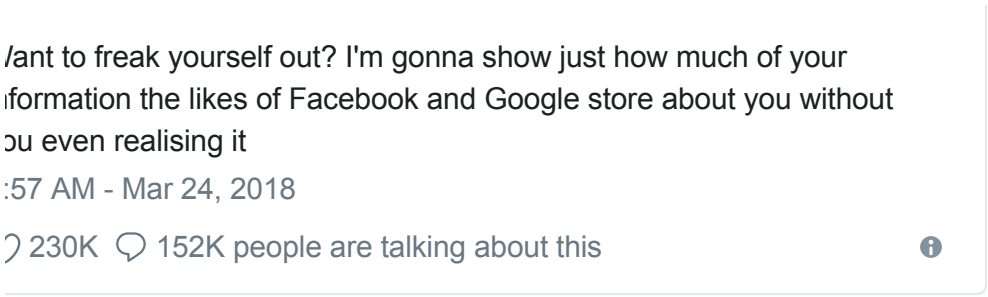
With Facebook and Google It was not consent, it was concealment

Natasha Lomas @riptari /

Comment

Facebook's response to the clutch of users who are suddenly woke — triggered to delve into their settings by the Facebook data misuse scandal and #DeleteFacebook backlash — to the fact the social behemoth is, quietly and continuously, harvesting sensitive personal data about them and their friends tells you everything you need to know about the rotten state of tech industry ad-supported business models.

Dylan Curran



“People have to expressly agree to use this feature,” the company wrote in a defensively worded blog post at the weekend, defending how it tracks some users’ SMS and phone call metadata — a post it had the impressive brass neck to self-describe as a “fact check”.

“Call and text history logging is part of an opt-in feature for people using **Messenger** or Facebook Lite on **Android**. This helps you find and stay connected with the people you care about, and provides you with a better experience across Facebook.”

So, tl;dr, if you’re shocked to see what Facebook knows about you, well, that’s your own dumb fault because you gave Facebook *permission* to harvest all that personal data.

Not just Facebook either, of course. A fair few Android users appear to be having a similarly rude awakening about how **Google’s** mobile platform (and apps) slurp location data pervasively — at least unless the user is very, very careful to lock everything down.

But the difficulty of A) knowing exactly what data is being collected for what purposes and B) finding the cunning concealed/intentionally obfuscated master setting which will nix all the tracking is by design, of course.

Privacy hostile design.

No accident then that Facebook has just given its settings pages a haircut — as it scrambles to rein in user outrage over the still snowballing Cambridge Analytica data misuse scandal —

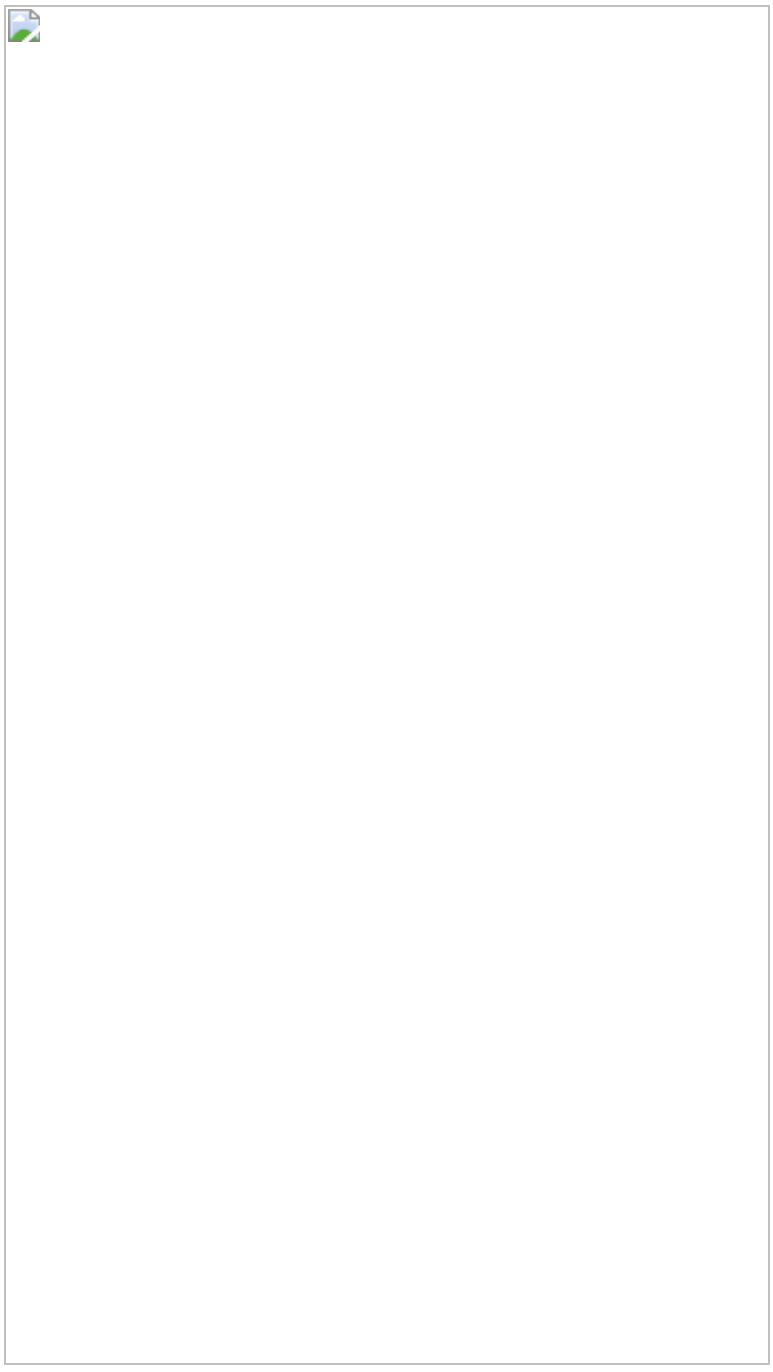
consolidating user privacy controls onto one screen instead of the full TWENTY they had been scattered across before.

ehem

Insert your ‘stable door being bolted’ GIF of choice right here.

Another example of Facebook’s privacy hostile design: As my TC colleague Romain Dillet pointed out last week, the company deploys misleading wording during the Messenger onboarding process which is very clearly intended to push users towards clicking on a big blue “turn on” (data-harvesting) button — inviting users to invite the metaphorical Facebook vampire over the threshold so it can perpetually suck data.

Facebook does this by implying that if they don’t bare their neck and “turn on” the continuous contacts uploading they somehow won’t be able to message any of their friends…



An image included with Facebook's statement.

That's complete nonsense of course. But opportunistic emotional blackmail is something Facebook knows a bit about — having been previously caught experimenting on users without their consent to see if it could affect their mood.

Add to that, the company has scattered its social plugins and tracking pixels all around the World Wide Web, enabling it to expand its network of surveillance signals — again, without it being entirely obvious to Internet users that Facebook is watching and recording what they are doing and liking outside its walled garden.

According to pro-privacy search engine DuckDuckGo Facebook's trackers are on around a quarter of the top million websites. While Google's are on a full ~three-quarters.

So you don't even have to be a user to be pulled into this surveillance dragnet.

In its tone-deaf blog post trying to defang user concerns about its SMS/call metadata tracking, Facebook doesn't go into any meaningful detail about exactly why it wants this granular information — merely writing vaguely that: "Contact importers are fairly common among social apps and services as a way to more easily find the people you want to connect with."

It's certainly not wrong that other apps and services have also been sucking up your address book.

But that doesn't make the fact Facebook has been tracking who you're calling and messaging — how often/for how long — any less true or horrible.

This surveillance is controversial not because Facebook gained permission to data mine your phone book and activity — which, technically speaking, it will have done, via one of the myriad socially engineered, fuzzily worded permission pop-ups starring cutesy looking cartoon characters.

But rather because the consent was not informed.

Or to put it more plainly, Facebookers had no idea what they were agreeing to let the company do.

Which is why people are so horrified now to find what the company has been routinely logging — and potentially handing over to third parties on its ad platform.

Phone calls to your ex? Of course Facebook can see them. Texts to the number of a health clinic you entered into your phonebook? Sure. How many times you phoned a law firm? Absolutely. And so on and on it goes.

This is the rude awakening that no number of defensive 'fact checks' from Facebook — nor indeed defensive tweet storms from current CSO **Alex Stamos** — will be able to smooth away.

"There are long-standing issues with organisations of all kinds, across multiple sectors, misapplying, or misunderstanding, the provisions in data protection law around data subject consent," says data protection expert Jon Baines, an advisor at UK law firm Mishcon de Reya LLP and also chair of NADPO, when we asked what the Facebook-Cambridge Analytica data misuse scandal says about how broken the current system of online consent is.

"The current European Data Protection Directive (under which [the UK] Data Protection Act sits) says that consent means any **freely given specific and informed** indication of their wishes by which a data subject signifies agreement to their personal data being processed. In a situation under which a data subject legitimately later claims that they were unaware what was happening with their data, it is difficult to see how it can reasonably be said that they had "consented" to the use."

Ironically, given recent suggestions by defunct Facebook rival Path's founder of a latent reboot to cater to the #DeleteFacebook crowd — **Path** actually found itself in an uncomfortable privacy hotseat all the way back in 2012, when it was discovered to have been uploading users' address book information without asking for permission to do so.

Having been caught with its fingers in the proverbial cookie jar, Path apologized and deleted the data.

The irony is that while Path suffered a moment of outrage, Facebook is only facing a major privacy backlash now — after it's spent so many years calmly sucking up people's contacts data, also without them being aware because Facebook nudged them to think they needed to tap that big blue 'turn on' button.

Exploiting users' trust — and using a technicality to unhook people's privacy — is proving pretty costly for Facebook right now though.

And the risks of attempting to hoodwink consent out of your users are about to step up sharply too, at least in Europe.

Baines points out that the EU's updated privacy framework, GDPR, tightens the existing privacy standard — adding the words "clear affirmative act" and "unambiguous" to consent requirements.

More importantly, he notes it introduces "more stringent requirements, and certain restrictions, which are not, or are not explicit, in current law, such as the requirement to be able to **demonstrate** that a data subject has given (valid) consent" (emphasis his).

"Consent must also now be separable from other written agreements, and in an intelligible and easily accessible form, using clear and plain language. If these requirements are enforced by data protection supervisory authorities and the courts, then we could well see a significant shift in habits and practices," he adds.

The GDPR framework is also backed up by a new regime of major penalties for data protection violations which can scale up to 4% of a company's global turnover.

And the risk of fines so large will be much harder for companies to ignore — and thus playing fast and loose with data, and moving fast and breaking things (as Facebook used to say), doesn't sound so smart anymore.