NEW YORK POST

The right way to fix Facebook

Julian Sanchez

March 23, 2018

As anyone who's uploaded an ill-advised photo from a college party knows, Facebook is where your old mistakes come back to haunt you years later. That turns out to hold just as true for the company itself — a fact executives at the behemoth social network have been discovering to their chagrin this week, amid international furor over the political strategy firm Cambridge Analytica's illicit access to a vast trove of Facebook user data.

Facebook's mistake, in this case, was a classic case of taking a good idea too far. The idea was that the company's massive map of users' social connections could be put to innovative uses if that data were opened up to outside developers — allowing all sorts of third-party apps to painlessly add a social component.

Unfortunately, the company also made a critical misjudgment: It assumed that if users were willing to share personal information with their friends, they were also willing to let their friends re-share that information.

That's how Cambridge Analytica, now in the spotlight for its role as a digital consultant to Donald Trump's presidential campaign, wound up "scraping" reams of data from the profiles of some 50 million Facebook users, leveraging the consent of just 270,000 who'd installed a personality quiz app.

CA wasn't the only political shop to come up with that trick, of course. In previous elections, Barack Obama's digital team had been hailed for its new media savvy for employing similar tactics. As Obama for America data-mining guru Carol Davidsen explained: "We ingested the entire US social graph. We would ask permission to basically scrape your profile and also scrape your friends, basically anything that was available to scrape. We scraped it all."

But Cambridge Analytica went about its "scraping" in a far dodgier way: The Obama team had at least vacuumed up data via an app that was explicitly billed as helping a political campaign. Cambridge got its from a scholar, Aleksandr Kogan, who had pledged to use it only for academic research.

Worse, recent reports indicate that when Facebook discovered its user information had been passed along, Cambridge retained it even after assuring the company it had been deleted — an assurance Facebook appears to have blithely accepted.

By 2014, the social-media platform had altered its policy and shut off apps' access to most types of information about users who hadn't themselves installed that app. As it turned out, however, Facebook was closing the barn door after the horses had bolted — which is why it's facing backlash now over a policy it changed years ago.

The furor, however, has inspired a number of other overdue changes: Facebook will be making an effort to notify users whose data was obtained, conducting audits of developers who hold large amounts of user data and revoking third-party apps' access to the data of users who haven't logged in to those apps for several months.

The backlash has also, predictably, spurred an array of fresh calls to regulate platforms like Facebook. Some of these — like a federal breach notification requirement — have merit.

Whether personal data is leaked through hacking or developers simply breaking confidentiality promises, users need to be able to hold companies accountable for acting as responsible stewards of information.

They can't do that if the firms are able to simply sweep incidents like this under the rug, as Facebook seemed content to do until press reports forced the issue. It would be a mistake, though, to think regulatory micromanagement is likely to safeguard user privacy.

Too often, privacy rules take the form of more stringent notice and consent requirements — a longer series of boxes to check each time data is shared. Like antibiotics, these invariably become less effective the more they're used: Force users to click through too many privacy notices and, like most websites' terms of service, they become one more nuisance users sleepwalk through.

Either way, Facebook's own efforts to improve users' control over their privacy are healthy developments. But the incident — and the heat Facebook is taking as a result — should serve as a sobering reminder to Silicon Valley that the damage from bad privacy design choices can be hard to undo. Data, like trust, is hard to recover once it slips away.

Julian Sanchez is a senior fellow at the libertarian Cato Institute.