

Privacy laws cannot make Facebook and Google accountable

Pranesh Prakash

2019-01-03

Hindustan Times

Abstract

To safeguard users' privacy, we need to be able to move away from platforms like Facebook without losing access to their networks.

The past year was Facebook's annus horribilis. We have much to thank intrepid journalists, who have painstakingly documented Facebook's wrongdoings. However, while 2018 was the year of amazing investigations on Facebook, there have been grave letdowns in reporting and analysis.

Let's take the example of Cambridge Analytica (CA). Many seem to believe that Facebook had unwittingly shared users' data with CA without users' consent, and that CA used this data to successfully manipulate elections. The Observer's headline called this a "data breach". However, around 320,000 people were paid to willingly give an app called "thisisyourdigitallife" consent to access their Facebook data (name, birth date, pages they had liked, friends lists, etc.), including their private messages, and the data of their friends (name, gender, current city, tagged photos, and pages they had liked) if those friends had allowed their data to be used by their friends' apps in their privacy settings. (Friends-of-users data was used by apps like Yahoo, Skype, and Daily Horoscope, and hundreds of thousands more, and this feature was removed by Facebook in 2015.) The terms of service, which the app's users consented to, possibly without reading, even gave the app maker, a company called GSR, the right to sell this data, which was a violation of Facebook's terms of service. GSR went on to license information derived from this data to a number of companies, including SCL Elections, which was CA's parent company. While Facebook was rightly fined for not doing enough to make people realise that their friends could share their data with apps, it was your friends (or you) who did the sharing, not "Facebook"; nor was "Facebook data" breached, unlike what the headlines suggested.

In 2015, when Facebook found out that their terms of service had been violated, they requested GSR and all its clients to delete all data collected. Whether they complied fully is still being investigated. Interestingly, Christopher Wylie — whom the Observer painted as a conscientious, gay, vegan, liberal Canadian whistleblower — was the one who contacted GSR, helped draft the

terms of service for the “thisisyourdigitallife” app, and unethically obtained the data for CA, thus breaching users’ trust as well as the law. He even licensed GSR’s data after he left CA and formed his own firm — Eunoia Technologies — which pitched, unsuccessfully, to the Donald Trump campaign. Clearly the “whistleblower” lacked an ethical compass.

On election manipulation, let’s look at the facts. CA first came to light in 2015, when it was providing its services to Ted Cruz and Ben Carson — two failed candidates whom Trump beat hands down in the 2016 Republican presidential primaries. In Nigeria, it was hired to work against Muhammadu Buhari, who went on to be elected president. While CA seems to be an odious company by all accounts, it clearly doesn’t have a magical way to manipulate votes.

More recently, The New York Times proclaimed that Facebook had given “Netflix and Spotify the ability to read Facebook users’ private messages”. What the Times, and others who reported on the story, failed to convey to their readers was that users had to specifically grant Netflix and Spotify the permissions to read (and send) private messages, and that this was necessary to be able to share music and movie recommendations over Facebook privately with your friends. When presented in this context, this seems innocuous, and far more so than the privacy-invasiveness of companies like TrueCaller.

Alongside Facebook, companies that one may not have heard of — like Epsilon, Equifax and Experian — are far more intrusive and actually sell your data, unlike Facebook. India doesn’t have a proper privacy and data protection law to safeguard citizens against such leeches. Companies like Facebook and Google are dangerous due to the power they wield over society. But privacy laws won’t suffice to make them accountable. No set of privacy defaults will fit the needs of over two billion users — “advanced” users can engage in privacy self-determination in a way that most average users can’t, since they will consent to anything. To safeguard users’ privacy, we need to be able to move away from platforms like Facebook without losing access to their networks — similar to the way you can e-mail people using Yahoo Mail even if you use Gmail. And to enable that we need to focus on competition and platform openness, rather than privacy alone, which is leading to more closed platforms.

Pranesh Prakash is policy director at Centre for Internet and Society