

Facebook Privacy Policy on Restrictions to Sharing Residential Information

Response from IT for Change to the
Facebook Oversight Board's
Roundtable (held on October 7)

October 2021

Personal data, using the [GDPR definition](#), would include a person's residential address. The issue of Facebook Community Standards placing restrictions on users sharing residential information and consequent removal of any such content has to be assessed within the confines of not only rights of privacy and freedom of speech, with focus on the right to be forgotten, but also of the safety and security of users. In that context, the following perspectives, including implications for India, are relevant.

Safety and Privacy of Users

An obvious and significant risk with allowing sharing of residential information online is the possibility of [doxing](#). While blanket removal of residential information can violate an individual's freedom to include such information on social media, it has to be weighed against the possible harm of allowing this information to remain on the platform. [India has no specific laws against doxing](#), and so, in the Indian context, such removal may be a solution against illegal release of such sensitive information like house address - often used to threaten and intimidate women.

However, the narrow framing of the issue by Facebook naturally limits the discussion to only one of the possible mechanisms by which a Facebook user's private information - location - information in particular - is leaked on the platform. While doxing by another user is one way by which a user's location information is leaked without their consent, Facebook has [admitted](#) the platform itself captures information that could be used to guess their location using means that are not transparent to the user, and makes use of that information for enabling location targeted [advertising](#). It has been demonstrated that advertisers can craft such fine-grained audience criteria they can [infer user locations](#) to a fair degree of certainty. A user has no way of knowing what role Facebook's inference of their current or recent location played in the presentation of an ad with which they may interact (unless they happen to have explicitly granted Facebook access to that information via their profile, their GPS location or other explicit action). This in some ways is as bad, if not worse, than doxing, because the user does not even know that their location information is compromised, especially to an unknown actor in the form of an advertiser, all without a recourse.

It is also necessary to ask if collection of location data by a platform like Facebook is essential at all. Access to a platform should not be made conditional to part with one's data being collected for profit. The UN Special Rapporteur on Privacy, in its [first mandate report in 2016](#), questioned

whether platforms could track individuals 'to ensure just compensation'. If needed at all, users should be given a choice to opt-in to such data being collected by privately-owned platforms, with the default being no data collection without express consent. While [individualistic methods](#) are provided to enable deleting data collected on Facebook, it puts the onus on users, rather than the platform itself, to regulate how data already collected is stored.

Global Takedowns and Right to be Forgotten

With regard to situations where private information that is made public should be removed by Facebook, this has to be seen in light of the principles of global takedowns and the right to be forgotten - rights that have been recognized in India as well through judicial orders. In 2019, the Delhi High Court in India allowed potentially defamatory content to be removed from platforms globally (this case is [pending](#) in appeal). The same court has [recognized](#) the right to be forgotten as part of right to privacy as part of fundamental rights guaranteed to all people, which will make it necessary for Facebook to remove such content.

In the Indian context, the court order on global takedowns is also significant because of Facebook's statement in the verdict declaring that any content published on its platform which violates its Community Standards will be removed globally. Such a stand shows that Facebook's role in such content moderation is concretized in the Indian context.

In essence, merely because private information is publicly available will not preclude removal by judicial orders and will require appropriate Community Standards to abide by the local laws of the region.