At the end of 2024, Meta's subsidiary, Instagram, is one of the most used social media networks around the globe, with over 1.5 billion subscribers. The transparency of the content in the platform's privacy policy is variable-it's a mix of transparent and opaque parts; some are quite explicit, while others are totally vague. This variablity of transparency in the content brings out confusion among people, raising their concern for privacy.

This allows data sharing across all apps associated with Instagram, such as Facebook and WhatsApp, increasing surveillance and the exploitation of identity. In this way, any control that users may seemingly have over their digital identities is annihilated. Instagram's privacy policy is full of terms such as "may collect," "may share," and "may use" that are not clearly defined, which leaves the user in limbo regarding what data is being collected, how it is processed, and who is actually gaining access to that data.

The idea of the "personalised" experience is, therefore, their most marketed benefit to consumers through the use of Instagram-from curating who populates each feed based on interest to running "interest-targeted advertisements." Here, Instagram did explain that through the use of cookies, data use and collection flow well on both its own network and third-party websites and partners as part of their ability to provide. The problem starts once customers have no exact idea of this effect.

The other shocking part is that, though Instagram allows deleting an account, it reserves the data even after deletion-a clear cause of concern regarding loss of control and vague retention periods. Because of Instagram's ad targeting that's advanced, many suspicions have been pointed against it for probably listening to user conversations.

In reality, the underlying algorithms of Instagram depend on behavioral tracking, third-party data integrations, and probability modeling to estimate user behavior in patterns and correlations. Even if Instagram is not actually listening, those predictive capabilities may be just invasive.

It gathers a lot of sensitive information, which is highly exposed to breaches that could lead to the leak of personal information, private content, and behavioral insights. Even tech giants like Meta are not safe; for example, the 2019 Facebook breach released data from over 500 million of its users.