Criticism of terms and services and privacy policy of **Social Media** platforms

Developed By Fabiha Tasneem, Sanjida Kater, Sadia Huq

“You cannot hold us liable for the videos on YouTube. It's not our fault you got sick after following that cooking video's recipe.”

YouTube doesn’t take liability for showing inaccurate, offensive, indecent, or objectionable videos to its users. They don’t have any method to categorise the contents to avoid exposer of inappropriate contents to ineligible users. Thus, creates an unsafe environment for different group of its users.

“You must be 13 years or older”

YouTube doesn’t have any method to verify the real age of users. So, children can access inappropriate and offensive contents, and be mis-guided by watching videos.

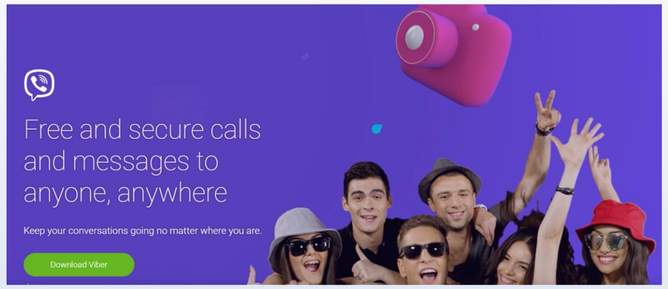
SnapChat

“The Content of Others”

Snapchat Is Not Responsible for Content of Others That Violates Terms. It cannot review the contents shared publicly or privately by the users or third parties as a result many drug dealing cases has arisen in recent years.

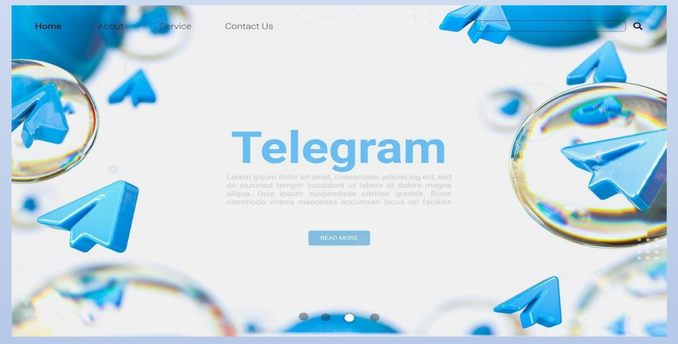
“How We Share Information”

Snap's collects data from basic data, geo-location, interactions, behaviours, cookies and share some public information with other snapchat users and with their affiliate’s companies. It is Unclear whether the company attempts to maintain the accuracy of data they collect.



“Content and Public Content”

Viber uses the public contents modifying or reproducing and distribute it for commercial or non-commercial purposes. The users don’t get any compensation for such use of their contents. Moreover, Viber uses a certain proportion of the public contents which can be misleading for other users and create violence among public.



“End-to-End Encrypted Data”

Telegram have E2E encryption for secret chats and is not applied by default. So, Telegram can read chat data since it handles the encryption/decryption of messages at the servers, privacy is not ensured here.

“Law Enforcement Authorities”

Telegram would share the Ip Address, phone number if there is a law enforcement issue. Data security is not provided as government can track people with this information.

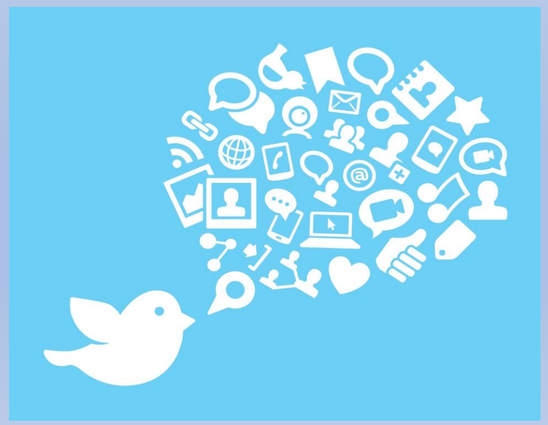
“Data policy of users”

Facebook claims to collect data for better user experience but there is no proper mentioning of where user’s information will be used. They limit their liability but it can be harmful to the society indirectly by creating violence. They allow third party apps to use user data about internet use and personal information (profile picture, public information etc.) which are stored in servers separated from Meta. This can be a threat to people’s personal security.
However, it is being discussed that how Facebook is related to some of the violence in recent times. It is thought to be the contents posted in Facebook create that violence among people which should be a matter of concern.

TikTok

“Your Account with Us”

TikTok has stated that once a user deletes his/her account, he/she can’t reactivate or retrieve any of the contents that he/she had shared before. But they haven’t clarified if they stored or deleted the user’s information and the contents which were shared by the users. This allows TikTok to store and use a deleted account’s information and contents for commercial and non-commercial purposes.



“What data do you collect about me? Information we collect when you use Twitter”

Twitter keeps track of how the users interact with each other. When a user uses direct message service, twitter collect the content of the messages and stores them. This infiltrates the privacy of users. Moreover, they don’t have end to end encryption to the messages the users send to each other to protect the privacy of the users.

Contact Us: +880 17123-45678 Gmail: group105@gmail.com

Source: facebook.com | snap.com | telegram.org | twitter.com | viber.com | tiktok.com | youtube.com