

Concern	Escalation 1	Escalation 2	Escalation 3
<i>Censorship</i>	The software application does not intervene when messages containing nothing else than hate speech gets sent to its users by other users.	The software application removes links that direct to rival companies. An example would be Facebook removing a link that directs to Twitter since both are social networking sites.	The software application company blocks any content that supports a political standpoint outside of its own. It does this without warning or notification.
<i>Discrimination</i>	The software application implements updates that make its services run slower on older devices, forcing you to buy a new device.	The software application has no support to accommodate persons with visual impairment, persons who are hard of hearing, or those who have color vision deficiency.	The software application creates a profile around you and then blocks certain functionalities depending on characteristics such as religion, gender, or age.
<i>Inappropriate content</i>	The software application does not show a warning whenever inappropriate content is displayed.	The software application favors profiles that post inappropriate content by showing them more frequently in the software application than users who post appropriate content.	The software application adds inappropriate content to user profiles that did not post this. It does this without notifying anyone.
<i>Manipulative design</i>	The software application does not offer an online method to delete an account online. Instead, a number can be called available only 3 hours per day.	The software application uses fake notifications made to look like that of other software applications. If you try to remove this notification, the software application starts.	The software application does not close. Every time you press quit or try to close it through other means, an intrusive message shows up. The only way to close the software application is to reboot the device the application is being used on.
<i>Misinformation</i>	The software application has no measures in place to notify you of misinformation that is spread on the application.	The software application deliberately shows political lies in favor of a party that supports the application company.	The software application company spreads misinformation and forces this onto you. It does this by showing content within the software application that can not be blocked, such as pop-up messages. It cites false sources to make those lies seem true.
<i>Privacy</i>	The software application accurately tracks your location without informing you.	The software application tracks everything that you do on the device you use it on. Examples are other software applications that you use on your phone, what you are searching for using other software applications etc.	The software application tracks not only your location but also that of friends and family. It tries to build a profile around them and then keeps data on people they went to in a similar fashion.
<i>Scam</i>	The software application has no measures in place to protect you from being scammed by other users.	You pay for additional software application functionality. After payment, that functionality is not provided.	The software application uses your credit card information to transfer fees to the company of a substantial amount. It does this without informing you.
<i>Transparency</i>	The software application recommends content to you based on what it thinks you like. It does not disclose how it got this information.	The company behind the software application actively lies to you about what your data is being used for. An example would be telling you your data is not being sold while it is.	The software application has been breached by hackers and user data has been compromised. It does not disclose this data breach to you.