Case 04

Facebook

1. Facebook’s policy states that they can use user information for no compensation. They also state that they use the users IP license until the user deletes their account.

“When you publish content or information using the Public setting, it means that you are

allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)”.

“We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use your feedback or suggestions without any obligation to compensate you for them (just as you have no obligation to offer them)”.

1. Cambridge Analytica is a UK based political data firm that collected private information from 50 million Facebook users.

1. Facebook was enabling the spread of misinformation by working with Cambridge Analytica because one of Cambridge's clients included Donald Trump's general-election campaign, which shows that Cambridge Analytica was collecting user data and targeted certain people with ads to benefit Donald Trump’s election.

1. It is impossible to protect your user information from applications like Facebook because Facebook may still be able to collect information on you that's posted by friends or family who continue using their accounts even after you've deleted yours. This means that your data could still be used even after a user has deleted their account. A second reason why it’s impossible to protect your user information is because there is no guarantee that all the data you previously entered will be deleted by the companies completely. Lastly, it is impossible to protect user information from applications like Facebook because some of the users personal data could be leaked to third party apps without the user knowing. So, there is no real way for a user to know where their personal data is being used.