Case Study

Project by- Ashmita Pandey (2433150)

10.01.2025

Mozilla RCC

Consent, Confusion, or Corruption: Ethical Dilemmas and the Impact of Language in Privacy Policies

In a world where every swipe or scroll leaves digital footprints, digital surveillance to data privacy emerges as significant. To maintain a balance between data protection and user interest, it has become crucial for digital platforms to set strict privacy policies. Legality communicated through privacy policies and data agreements is what governs privacy and surveillance. The language used within these documents stand crucial to how users comprehend and agree to data collection, ways to data handling and distribution. For instance, Snapchat offers simple and transparent explanation that directs towards the data collection and handling while also avoiding technical and legal jargon. The privacy policy of Snapchat includes examples about how they use the data and how the user can control his/her information. The policy defines terms like “Services”, “Terms” and “Snapchatters” within the document, to ensure vivid and easy understanding of their meanings in context. The information in the document is segregated into sections about user control, data collection, information sharing and the duration for retaining the information within the system. The statement, “we may collect your personal information from, transfer it to, and store and process it in the United States or other countries outside of where you live. Whenever we share information outside of where you live, we ensure safeguards are in place to protect the data as required by law where you live.”, [i] within the policy is reassuring and demonstrates accountability regarding third-party data sharing practices. While the statement regarding the content integration by the Snapchat integrated partners which bluntly mentions, “integrations in Lenses, Camera editing tools, to provide Scan results, and third-party developer integrations. Through these integrations, you may be providing information to the integrated partner as well as to Snap. We are not responsible for how those partners collect or use your information.”[ii], explicitly avoiding to take responsibility

of the privacy offered by the integrated partners thereby distancing Snapchat from liability. Snapchat has faced criticism for its privacy practices for sharing the data with third party applications without taking accountability of the consequences that could be faced. However, the framing of the policy is clear and holds transparency to a large extent. On the flip side, many policies have been criticized for holding ambiguity, for instance, Google's privacy policy mislead users into thinking that the location tracking would stop on turning of the Location History. The legal action refers to a widely reported 2018 revelation turning off one location-tracking setting in its apps was insufficient to fully disable the feature. However, through other services, Google continued collecting the location data.[iii] The lack of transparency which emerged as deceptive practices and resulted in misleading interpretation, culminated in legal allegations of violating consumer protection laws.

The language of a privacy policy plays significant in reflecting the organization's promise towards users' expectations of privacy and security. Transparency and clarity of data collection, handling and how much control over the data the user has must be explicit in the language used while framing the privacy policy. Although, simplified language makes policies readable at ease, they sometimes lack detail while other times become lengthy enough for the user to quit halfway. For instance, Uber has an eleven pages long privacy policy which leads to only plenty of the users going through it. Though, it is observable to notice that Indian companies (like Flipkart and Paytm) have significantly shorter privacy policies than multinational companies. With this, it is also necessary to make privacy policies available in various Indian languages as less than a quarter of the population that speaks English, considers it to be the first language and less than half the population of the country has Hindi as first language. Despite the fact, most companies do not have non-English privacy policies. However, impact of language used in the making of the policy does not solely impact the privacy breach or violation of laws. A

striking example that reveals the other responsible factors rather than exhibiting language impressions of privacy policies as the only determiner of privacy misconduct is the Facebook-Cambridge Analytica scandal, where corruption and detrimental practices played a pivotal role along with misleading terms of the policy.

Facebook - Cambridge Analytica data scandal

"This Is Your Digital Life", an app developed by Aleksandr Kogan, an American Scientist was responsible for data privacy breach which affected such a large audience that it evoked people to initiate a #Deletefacebook movement. The hashtag was tweeted almost 400,000 times on Twitter within a 30-day period after news of the data breach.[iv]

A British consulting firm, Cambridge Analytica collected personal data from thousands of Facebook profiles without consent. The purpose of data collection was political advertising during the election period. The data was collected through the app- This Is Your Digital Life- where users needed to complete a quiz, the pre requisite to what was logging in to their Facebook account. Through this, users' personal data like date of birth, post interactions, location and Facebook likes significantly was shard with the firm. The individual quiz data compiled with the user's Facebook data into a psychometric model created a sort of personality profile. This psychometric model was then combined with voter records and was sent to the Cambridge Analytica to favour their political and promotional needs. The operation was carried out without the user consent. The process did not stop here but Cambridge Analytica along with Aleksandr Kogan accessed even the profile data of the user's (who volunteered for the quiz) friends which was again an act of violating user privacy. Facebook policy allowed third-party apps to access not only user data but also access the data of users' friends, without any explicit

consent. Statements like “we share information with trusted partners to improve user experiences” within privacy policies mask the true intent and extent of data sharing. This eventually results in a breach of user expectations. Lack of transparency about data collection and sharing, omission of details of the third-party applications and lack of disclosure about the degree to which user data is accessed by third-party platforms, altogether demonstrate how deceptive the privacy policies could be.

However, resolving data breaches does not limit the approach to altering policy language and requires attention towards a multifaceted approach by recognising multiple dimensions of the violation of privacy laws. Companies or third-party entities may knowingly enter into unethical practices and exploit user privacy for other specific intentions like financial and political gains. In the Cambridge Analytica case, the violation of user privacy was driven by a clear political agenda to manipulated and wire political campaigns. Political benefits were hierarchized over user privacy. The insufficiency of surveillance of engagements with third-party platforms, outdated systems, and poor encryption can enable unauthorised access. So, does the concern lie in the language used within the documents of policies about privacy offered, solely? Lack of cybersecurity measures leave platforms open to hackers, as seen in, Equifax Data Breach (2017), lack of accountability and oversight does not strictly restrict other party applications on limiting their extent of data collection and usage as seen the Google Location Tracking Case (2002) and significantly the users’ ignorant behaviour to read and comprehend the privacy policies grants permissions too freely. The framing of privacy policies is often critiqued for not offering transparency, simple language and essential details. Nevertheless, this raises an expository question. Does the focus rely exclusively on the language preference of the policy documents entirely, or are broader systemic changes necessary? Prioritization of profit over ethical actions and exploitation through cyberattacks due to vulnerabilities created along with

inadequate enforcement of data protection law needs to be scrutinized. Veering off from surveillance roles to improper monetization formalities highlights the lack of attentiveness towards ethical boundaries and data usage in corporate practices. The concern which stands ahead is whether improving the language of privacy policies independently restore user trust or the greater need lies in holding accountability for unethical practices when policies are intentionally vague or complex?

References

[i] Snapchat- *"We may collect your personal information from, transfer it to, and store and process it in the United States or other countries outside of where you live. Whenever we share information outside of where you live, we ensure safeguards are in place to protect the data as required by law where you live." Snap*, Snap Inc., https://values.snap.com/privacy/privacy-policy. Accessed 5 Jan. 2025.

[ii] Snapchat- *"Integrations in Lenses, Camera editing tools, to provide Scan results, and third-party developer integrations. Through these integrations, you may be providing information to the integrated partner as well as to Snap. We are not responsible for how those partners collect or use your information." Snap Inc.*, https://values.snap.com/privacy/privacy-policy. Accessed 5 Jan. 2025.

[iii] BBC- *"The legal action refers to a widely reported 2018 revelation turning off one location-tracking setting in its apps was insufficient to fully disable the feature. However, through other services, Google continued collecting the location data." BBC*, 24 Jan. 2022, https://bbc.com/news/technology-60126012. Accessed 7 Jan. 2025.

[iv] Wikipedia- *"The hashtag was tweeted almost 400,000 times on Twitter within a 30-day period after news of the data breach." Wikipedia*, Wikimedia Foundation, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal. Accessed 7 Jan. 2025.