

The Ethics of Data Mining on Social Media Platforms

Jeffrey Wang

University of North Texas

January 28, 2018

Every day, billions of people worldwide use social media platforms. The most popular conduit of our lives is undoubtedly Facebook, which recently reached one billion users (Zuckerberg, 2015). With the rapid rise of social media networks, traditional face-to-face conversations have been morphed into more convenient social media conversations at the expense of privacy. However, social media platforms like Facebook are privileged with the private data of its users and have chosen to analyze it and share it publicly with advertisers. I argue this breach of privacy is unethical because of the lack of consent by Facebook users.

Social media is a relatively newer paradigm of communication to which people are still adjusting. As such, the dynamics of social media communication significantly differ from traditional conversations. These dynamics can be described using Communication Privacy Management (CPM) theory, which defines privacy as “any information that makes people feel some level of vulnerability, thereby resulting in the desire to control the further dissemination of that information” (Child & Starcher, 2016). A severance of relationship (colloquially known as a “break-up”) should be counted as one’s privacy due to the delay of notification that Facebook has identified, which I believe indicates a reluctance to share information due to its vulnerable nature. As the communication conduit, Facebook has the responsibility of providing users the ability to control who their post reaches. On Facebook’s Privacy Basics page, the first paragraph states “You have control over who sees what you share on Facebook” (Facebook, Inc., 2018). I believe this statement clearly indicates that Facebook appears to support maintaining the privacy, or vulnerability, of its users’ content.

However, this privacy guaranteed by Facebook is only from other users and not from Facebook itself, as can be seen by its “People Insights” blog. What can explain this inconsistency?

Facebook operates as a free service for its consumer users, like most web companies do. For instance, the free language learning website Duolingo earns its revenue from licensing its translation services to other businesses, while collecting translation data from user contributions (the same users that learn languages using its platform). Typically speaking, free services earn revenue through unconventional channels; Facebook is not alone in doing so. Facebook primarily earns its revenue from selling advertising on its website. Since advertising is paid per click, Facebook is monetarily incentivized to match advertisements to relevant users. Therefore, as a company, Facebook ultimately sacrifices user privacy for advertising accuracy.

The dilemma between collecting money from end users with transparent intentions and collecting money through more indirect avenues has recently become a major issue in web journalism. The current difficulty in profiting from journalism has shifted interest from the traditional advertising and subscriptions model to cryptocurrency mining, where the end user agrees to mine cryptocurrency with their device while reading the news company's articles (Trustnodes, 2017). The general consensus seems to be cryptocurrency mining should not be used without the end user's permission, which is why prominent web-based cryptocurrency mining service Coinhive has introduced AuthedMine, a version of its service that only begins mining cryptocurrency with the consent of the user (Coinhive, 2018).

Similarly, I believe user consent is also necessary from users of Facebook before their data can be mined. In fact, just because its competitors mine data as well does not justify its reasoning. In my Political Science class, I learned about the Milgram experiment, which discovered that people would obey an authority figure, albeit reluctantly, even if the authority figure gave unethical commands (Milgram, 1974). I believe that Facebook is pressured by its

competitors (the “authority figure”) to conform and perform unethical deeds, which in this case is data mining of its users without their permission

Facebook’s Data Policy says it “collect[s] the content and other information you provide when you use [its] Services” and “analyze[s] the information [it has] to evaluate and improve products and services” (Facebook, Inc., 2016). The vague language gives Facebook broad powers it does not explicitly outline; one of which is to tell advertisers how to target users who are going through a break up, arguably when they are emotionally vulnerable. Even if users have legally agreed to Facebook’s Data Terms, in reality, very few users completely read the terms. In 2011, even lawyers admitted to CNN that they do not read the complete iTunes terms (Pidaparthi, 2011). Practically speaking, most users are unaware of this clause and therefore are not truly consenting to Facebook’s data collection practices.

Facebook, in effect, exploits the vulnerable secrets of its users to cater to the source of its revenue. Specifically, it shows advertisers how to exploit users at their most vulnerable state of mind—during and immediately following a breakup. The underlying issue is that Facebook appears double-faced: it claims to be the stalwart of privacy protection for the end user while liberally providing statistically-backed advice derived from its privacy-expecting users, so its advertisers will have more effective marketing campaigns and in effect, pays more money to Facebook. While I believe it would be ethical to data mine with the consent of the user, the user has legally only consented to a broad and vague set of data collection practices, and so is unaware of the exact actions done to their private data. Furthermore, Facebook’s potential to manipulate vulnerable users’ behavior in the favor of itself and its advertisers is certainly possible in this scenario. Facebook’s actions are therefore unethical because of its lack of transparency of its data mining practices and lack of proper consent from its users in doing such

actions. Our blind trust being violated by Facebook is, while naïve on our part, still unethical on the part of Facebook. And while Facebook is not alone in doing such practices, conforming to such “group-think” does not excuse its unethical behavior in any way.

Bibliography

- Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior*, 483-490.
- Coinhive. (2018, January 28). *AuthedMine*. Retrieved from Coinhive:
<https://coinhive.com/documentation/authedmine>
- Facebook, Inc. (2016, September 29). *Data Policy*. Retrieved January 28, 2018, from Facebook:
https://www.facebook.com/full_data_use_policy
- Facebook, Inc. (2018, January 28). *Facebook Privacy Basics*. Retrieved January 28, 2018, from Facebook: <https://www.facebook.com/about/basics>
- Milgram, S. (1974). *Obedience to authority: an experimental view*. New York: Harper & Row.
- Pidaparthi, U. (2011, May 6). *What you should know about iTunes' 56-page legal terms*. Retrieved January 28, 2018, from CNN:
<https://www.cnn.com/2011/TECH/web/05/06/itunes.terms/index.html>
- Trustnodes. (2017, October 12). *Can Crypto Mining Save Journalism?* Retrieved January 28, 2018, from Trustnodes: <https://www.trustnodes.com/2017/10/12/can-crypto-mining-save-journalism>
- Zuckerberg, M. (2015, August 27). *We just passed an important milestone*. Retrieved January 28, 2018, from Facebook: <https://www.facebook.com/zuck/posts/10102329188394581>