Camryn Patillo

CYSE406: Professor Klena

Old Dominion University

March 23, 2025

Freedom of Expression and Privacy in the Digital World

Over the many years of having access to social media, I've used several online media platforms for content, communication, and information. Some examples of social media platforms I currently use today are Instagram, X (formerly known as Twitter), YouTube, and TikTok. What is great about these platforms is that personal information is collected and shared when the user shares with the interface on their profiles. The users can manage these profiles to either keep their profiles private or public or make specific posts and comments visible to a select number of people for a specific time. From a user's point of view, these social media platforms are trustworthy if individuals can manage their personal information. However, it is not as simple when considering all the information needed to operate a social media platform. These concerns are usually explicitly discussed in the Terms and Conditions/User Agreement for these platforms. Social media developers use machine learning and automation to recognize the interaction patterns of both individual users and larger groups. It helps increase user engagement within the platform by providing users the ability to personalize their algorithms. It also benefits third-party contributors such as content creators and businesses through recommend connections. This method of data analysis makes for a successful social media interface. However, the amount of data being collected to provide such performance should be of more concern. For example,

TikTok's Privacy Policy emphasizes the corporation's benefit from their users' data for marketing purposes. These corporations include Facebook, Instagram, Twitter, and Google. Some of the information collected and shared includes profile information, user-generated content, messages, item purchases & card information, and phone information, which includes other contact information stored on your device. While it is also stated that the information listed assists the platform for content moderation, it is also information that gets shared with third-party companies. While social media moderation is important to keep the platform age-appropriate, the amount of personal information shared with other platforms and corporations is troubling.

As a student and staff member of Old Dominion University, I have a lot of important and sensitive information shared and stored by the university. This would include details regarding my personal contact information, home address, financial information, tuition payments, and more. Because the information the university collects from me is extremely confidential, the measures taken to protect that information are optimal. ODU is FERPA compliant, which means my student information is protected. This would mean that access to my personal information is extremely limited and protected from unauthorized access. ODU uses methods like encryption and two-factor authentication to prevent any form of unauthorized access to my accounts and personal information.

While online surveillance and data collection are used to ensure safety and content moderation, it can also be used for malicious purposes. If users rely on themselves to protect their privacy, it may affect the performance of online media usage. On the other hand, social media platforms collect user data and do not provide enough measures to ensure their users that their data is safeguarded. This dilemma is a huge concern for me because if we provide complete control of user data to one, it can dissatisfy the expectations of the other, and it leaves room for a

lack of control over data being collected. Cooperation between both social media platforms and their users is needed to provide quality safeguard practices and service,s which is easier said than done. According to the article “American Attitudes About Privacy, Security, and Surveillance,” approximately 93% of reported adults in America have felt they should be more in control of who can access and share their information. Despite the overwhelming number of individuals who wish to be more in control of their privacy, the majority of those reported have stated that they do not feel like they can manage their personal information. This could also be the case beyond the scope of just digital surveillance. Government security cameras and surveillance are used to ensure public safety. But like digital surveillance and data mining, these surveillances may be used for other purposes. Security cameras at retail or grocery stores can be used to track customer interest to see which products attract the most customer attention. Security cameras can be a great tool to analyze what can make them make more money by tracking customer behavior. However, if this is the case that companies and the government use surveillance for other benefits, it is not explicitly disclosed to the public and the individuals they are surveilling, which can be a huge breach of privacy.

References

Madden, M., & Rainie, L. (2015, May 20). *Americans’ Attitudes About Privacy, Security, and Surveillance*. Pew Research Center. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/#:~:text=The%20surveys%20find%20that%20Americans,anonymous%20for%20certain%20online%20activities.

Tiktok. (2024, August 19). *Privacy Policy* - United States. https://www.tiktok.com/legal/page/us/privacy-policy/en