

To: Professor Klena

From: Wayne Ricks Jr, Cyber law 406, 01228362

Subject: Freedom of Expression and Privacy in the Digital World

Date: March 19, 2025

1.) **Freedom of Expression.** One platform that I use to communicate and share information with friends and acquaintances is Instagram. I primarily use this platform due to its simplicity towards sharing information, as well as the overall aesthetic. It's simplicity comes from having access to all directives of the platform from the homepage, whether that be messaging others, searching for a trend, or just casual scrolling. The platform's Terms of Use Agreement tells each user that their data used to create their profile will be used to assist in the personalization of advertisements tailored to each specific user. The platform is moderated by team of individuals that look for any accounts that are involved in illicit activities. These activities can include the posting and distribution of controlled substances, spreading of false information, fraudulent schemes, and the harassment of other users. Any accounts accused of not following the Terms of Use Agreement may face consequences ranging from the removal of illicit content to the most extreme, permanently disabling one's account. Based off my experience with the platform, I've had an incident where a user tried to involve me in a fraudulent bank scheme. After reporting the account with my reason being that they are involved with fraudulent activities, the moderators of the platform permanently removed the account. I believe that the policy for the platform is followed based off what they explained to users in the agreement. I say this because before the release of the updated agreement, I recall many

accounts that have posted content that was illegal, but even after actions like reporting such activities, the accounts seemed to not adhere to the terms.

2.) Online Retailers. One retailer I have shared my personal information with is my online banking account. In order to have this set up properly, I needed to provide personal information such as full legal name, date of birth, current home address, social security number, as well as an active phone number. After reading over Langley's Privacy Policy, they state that some personal information, such as social security, account balances, and credit reports, will be subjected to being shared as long as it pertains to the institution's everyday business. All members are allowed to limit the amount of their personal information being shared, but not fully prevent it from being shared. It also states that when a member decides to no longer bank with the institution, they will continue to share the information that was previously listed. In regards to how they protect this information, Langley has a security/fraud department that will notify a member if there has been any suspicious activity associated with an account. I can recall a time where my credit card number was leaked and there were unauthorized purchases appearing on my bank statement. After calling the department, they were able to trace the card number to where it was last used and how much was bought using the card. In the end, I was able to obtain a new card, while the compromised one was deactivated to prevent further usage. I feel like their policy adequately protects my personal information, although I am not too certain about the fact that they still share your information even after your membership has been terminated. I begin to wonder what would happen if a person decides to leave the institution, but then a cyber attack is unleashed, exposing and jeopardizing the information of countless members.

3.) **Personal Concerns.** What concerns me the most about my online presence is the thought of my information being in the hands of another person without my consent or knowledge. Now, when it comes to my information, I specifically mean personal information that I would give to a federal institution or governing association like my social home address. The information that I input for social media will not be anything more than my date of birth or an alias, as I'm certain that the protections aren't as guaranteed like with federally-backed institutions. According to the CyberPedia article, which goes into depth about privacy leaks and data breaches, it argues that having your personal information exposed is nearly inevitable, but it's not always on the user if that information gets out. Some of these exposures come from a lack of security awareness or poor cybersecurity practices within an institution that could lead to the compromise of such information. It is also worth noting the difference between a data leak and a data breach, where a leak is deemed an accidental exposure, while a breach is a premeditated act of exposure. My concerns stem from me thinking about all the online retailers that I've used to make purchases and whether the information that I input is still circulating or worse, being sold off to the highest buyer to create some unknown profile on me. Some people may think that one's being overly precautionary about their information, but can you really blame them; with how prevalent identity theft and compromised data has become today? Though it is thought to be inevitable at some point, we all can do our part in protecting our information from falling into the wrong hands by implementing good practices such as doing the right amount of research before blindly trusting anything that will involve the input of personal information.

References

Bitdefender. “Check If Your Private Info Is Exposed Online.” *Cyberpedia*, 2025,
www.bitdefender.com/en-us/cyberpedia/what-are-private-data-leaks?irclickid=zP63nDSqJxyKUhm24JzYlw5RUks3U%3A1W01Uj0Q0&irgwc=1&MPid=2003851&cid=aff%7Cc%7CIR%7CBing%20Rebates%20by%20Microsoft