Article 1 Review

In the article “Tell Me More, Tell Me More: Repeated Personal Data Requests Increase Disclosure,” Fleming et al. (2023) attempt to answer the question of what factors contribute to the privacy paradox. Fleming et al. created a primary and secondary hypothesis to attempt to answer their research question. The primary hypothesis is that multiple requests would increase the likelihood of a person sharing personal information without affecting their data privacy concerns. The secondary hypothesis predicts that certain individual aspects, such as compliance, agreeableness, trust, social desirability, and need for cognition, influence the disclosure of personal information.

Fleming et al. (2023) designed a two-part study to test their hypotheses. The first section was conducted in an in-person laboratory setting that attempted to create a realistic scenario by providing the participants with modest compensation for their data and telling them that the data would be published publicly online for two weeks. This first section used the survey research method because it employed a series of questionnaires to gather data on personality traits, level of privacy concern, privacy behavior, and the amount and types of information participants are willing to disclose. For the second part of the study, Fleming et al. (2023) modified the procedures from part one to validate its results and make up for any potential shortcomings in the study’s initial design. Unlike the first study, which asked participants to answer questions, the second study presented questions hypothetically. Instead of answering the questions posed, participants in the second study were asked to indicate the highest-ranked question that they would not be willing to answer if asked in exchange for moderate compensation. Additionally, the first study only surveyed subjects about their levels of privacy concerns before being asked questions. The second section included the privacy concern survey both before and after disclosing personal information. Furthermore, Fleming et al. conducted the second section online to make it more closely emulate a real-life scenario of online privacy behavior. Since the second part utilized most of the same questionnaires and was conducted in a more realistic environment, it is a multimodal research method using both survey and field research methods.

Fleming et al. (2023) created several indices to classify, quantify, and analyze the survey data. To measure the amount and sensitivity of data participants were willing to disclose, they made the personal information disclosure index (PIDI). The PIDI uses a list of questions ranked from most to least sensitive, with question number one being the least sensitive. For part one of the study, the PIDI questionnaire had 67 questions, and part two had 70. The highest numbered question a participant was willing to answer would be assigned as their PIDI value to quantify the amount and sensitivity of the information they provided. Additionally, Fleming et al. used a concern for information privacy (CFIP) scale and privacy behavior scale. These two scales were formatted similarly and asked participants to rate how much they agreed or disagreed with certain privacy and online behavior-related questions. The CFIP and privacy behavior scales allowed participants' concerns for privacy and cyber hygiene to be measured and compared before and after the study by assigning a quantifiable value. Furthermore, Fleming et al. used a social desirability scale and personality inventory to account for individual differences that may influence the study's results. By assigning quantifiable numeric values to each of these constructs, Fleming et al. could compare the data and observe how information disclosure and privacy concerns changed after repeated requests and how individual differences may have influenced the results.

Fleming et al. (2023) used several social scientific principles when conducting their study. For instance, the researchers rejected their secondary hypothesis when the study's data indicated that social desirability and agreeableness traits did not meaningfully influence the amount of information disclosed. As a result, they demonstrated empiricism by letting real-world observations guide their conclusions rather than letting bias lead them to discount information that did not align with their initial expectations. This paper also relates to determinism because it investigates how past experiences can affect future behavior. In this case, the study suggests that past prompts for personal information make it more likely that a person will give out more information when asked again. Finally, Fleming et al. exhibit ethical neutrality by protecting the participants' privacy. Even though participants agreed to their information being made public as part of the study, the researchers respected the participants by not releasing the information, as doing so was not necessary for the study's integrity.

The topic discussed by Flemming et al. also relates to several concepts in the social sciences covered in this class's materials. Human factors is a field that accounts for human abilities, behaviors, and other tendencies when creating products or devices (Michigan Technological University, 2024). The privacy paradox and Flemming et al.'s (2023) finding that repeated requests for information increase the likelihood of disclosure are examples of human behavior that could be accounted for when designing effective cybersecurity solutions or scams. Additionally, their study found that individual differences, such as high openness to experience, may make some more susceptible to repeated requests than others. This is an example of victim precipitation because the recipient of such requests may be at greater risk of being targeted because of their tendencies. The article also relates to the theoretical and empirical planes of research, as Bhattacherjee (2012) discussed in the textbook. For instance, Flemming et al. created variables in the empirical plane, such as the PIDI, CFIP, and personality behavior scale, to represent and measure constructs in the theoretical plane. These theoretical constructs were information disclosure, personal concern for privacy, and the amount of online privacy behavior participants engaged in, respectively. Finally, internal and external validity could be applied to analyze Flemming et al.'s research. Given that their study was relatively small, focused on college students, and the participants' genders were heavily skewed in one direction, it is possible that the current state of the findings is low in external validity and thus may not be generalizable.

Using repeated requests to gather more personal information could be concerning for marginalized groups in two key ways. During the 2016 presidential election, there is evidence suggesting that the Trump campaign attempted to use social media to deter black voters from going to the polls disproportionately (Sabbagh, 2020). By collecting vast and varied personal information, future political campaigns could categorize voters based on factors such as race and gender and create detailed profiles about those individuals' personalities and behavioral tendencies. Consequently, minority voters could be more effectively targeted, leading to an unfair disadvantage in losing their ability to achieve equal representation in government. Another way that marginalized groups could be disproportionately affected by repeated information requests is from a lack of cybersecurity education. Recent data shows that school districts primarily serving people of color receive less funding per student on average (The Education Trust, 2022). As a result, many students in these districts receive a lower-quality education and experience poorer outcomes. This likely also means that many living in these school districts have less access to up-to-date technology and cybersecurity education (Inspiroz, 2023). With limited exposure to cybersecurity education, many in these school districts may be more susceptible to providing personal information to those who ask for it because they are unaware of the potential ramifications of disclosing such information. Therefore, more comprehensive personal data may be collected on marginalized groups, thus making them more vulnerable to the nefarious activities for which personal information is used.

One of the primary contributions of Fleming et al.'s (2023) study is that it helps provide a foundation for explaining the existence of the privacy paradox. Their research demonstrates that many people will provide greater amounts of information over time without a decrease in their reported concern for personal privacy. This provides a starting point for future research on the privacy paradox. Now that there has been a mechanism of action demonstrated to cause a disparity between privacy concerns and privacy behavior, researchers can now focus on discovering what causes people to disclose information after repeated requests without losing concern for privacy. Additionally, because many participants disclosed more personal information after only the second request, Fleming et al.'s paper also establishes that increased disclosure after repeated requests is a distinct phenomenon rather than an extension of privacy fatigue.

References

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. Anol Bhattacherjee.

Fleming, P., Edwards, S. G., Bayliss, A. P., & Seger, C. R. (2023). *Tell me more, tell me more: Repeated personal data requests increase disclosure. Journal of Cybersecurity*, 9(1). https://doi.org/10.1093/cybsec/tyad005

The Education Trust. (2022, December 8). *School districts that serve students of color receive significantly less funding.* https://edtrust.org/press-release/school-districts-that-serve-students-of-color-receive-significantly-less-funding/

Inspiroz. (2023, April 10). *Why cybersecurity education should be a top priority for education leaders*. LinkedIn. https://www.linkedin.com/pulse/why-cybersecurity-education-should-top-priority-leaders-inspiroz/

Michigan Technological University. (2024). Ihttps://www.mtu.edu/cls/undergraduate/human-factors/what/

Sabbagh, D. (2020, September 28). *Trump 2016 campaign "targeted 3.5m black Americans to deter them from voting."* The Guardian. https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting