

Data Collection is the biggest issue through the lens of Social Science. Data collection is the process of gathering information about an individual, such as their behavior, through scrolling, liking, posting, or searching. Not just one platform but multiple are collecting information about users behavior, interests, and even their location. The article, IEEE Digital Privacy, mentions how crucial these privacy risks are because users do not completely understand how much data is being collected or how it's being used.

The Federal Trade Commission also talks about major social media and streaming companies participating in large-scale surveillance, meaning they are constantly tracking users across different apps and services. According to the article, Journal of Computer-Mediated Communication, psychology talks about why users are continuing to use social media even when concerned about their privacy. They describe it as a privacy paradox, meaning users are aware of this issue and care about their privacy, but continue to use it because it's more convenient for them. Sociology also allows us to see that oversharing on social media has become a normal and repeated habit in society.

Technical and Social solutions are the most effective strategies to implement to lower these risks. On the technical side, organizations can enhance their privacy by using stronger encryption, limiting the amount of data collected from users, and making privacy settings easier to navigate and understand. The Federal Trade Commission also recommends stronger policies to ensure companies are not collecting more data than needed. Even though these solutions could make the organization safer. Many users still choose convenience over privacy, even when they are aware of these risks. Additionally, Social media companies rely on data from users to advertise or make a profit, which causes less control over reducing data collection of users.

In reflection, looking at cybersecurity from a social science perspective can allow us to better understand how human behavior can play a major role in creating risks. Throughout this case study, it is clear that privacy issues on social media are not just caused by the companies but also by the choices people make, such as what they share and how they interact online. When looking at psychology and sociology factors, we can understand why people use these platforms to share information, even if it means oversharing information, knowing the risks behind it. It also shows us that people are influenced by convenience more than security.

In conclusion, this case study shows us how using social science in cybersecurity helps us understand real-world problems like the exposure of users privacy on social media platforms. By looking at and understanding these issues, we can create solutions to help us reduce risks for individuals and society altogether.

Works Cited

“Privacy Risks and Social Media.” *IEEE Digital Privacy*,
digitalprivacy.ieee.org/publications/topics/privacy-risks-and-social-media/.
Accessed 21 Apr. 2026.

(DAD, Matthew Chesnes, and Stephanie T. Nguyen. “FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens.” *Federal Trade Commission*, 25 Sept. 2024,
www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance.

Taking Stock of Social Media Privacy: Meta-Analytic Evidence on How Control, Trust, and Concerns Are Associated with Social Media Use, Disclosure, and Protection | *Journal of Computer-Mediated Communication* | Oxford Academic,
academic.oup.com/jcmc/article/31/1/zmaf025/8456523?login=false. Accessed 21 Apr. 2026.