Research of Facebook Data Breach

Paul Cumiskey

School of Cybersecurity, Old Dominion University

CYSE 300 26972

Dr. Md Morshed Alam

1/26/25

Research of Facebook Data Breach

One of the most valuable assets in the 21st century is data. Thanks to technological advancements massive amounts of data can be collected, stored, moved, and analyzed within seconds. While this is extremely beneficial for many professions and society as a whole there are many downsides such as our privacy. Many social media companies collect extremely personal data on people to improve their targeted advertisements. While this is almost always stated in the terms of service, many users don't fully understand the impact of signing away their data, what happens to them after they do, and whether it is safe. In the case of Facebook, it was not.

Facebook is the world's largest social media/networking site, encouraging users to interact with friends and family online. Facebook enables users to post status updates and send messages to other users. Facebook has a privacy setting that allows you to hide your profile. Unfortunately in April 2021, it was revealed that a massive data breach compromised the personal data of 500 million users from all over the globe. Personal data such as phone numbers, emails, relationship statuses, and locations were made publicly accessible. This incident was largely investigated by Ireland's Data Protection Commission to ensure that Facebook(Meta) complied with Europe's General Data Protection Regulation (GDPR) laws.

The biggest questions that needed to be answered after the data breach was revealed were what information was stolen and how the hackers got into Facebook's private data. It was found that the Hackers exploited a vulnerability in Facebook's contact importer feature. The contact importer feature allowed users to find friends by uploading contact lists. This feature is no longer available due to the exploit. The attackers used the technique of scraping to gain data from this feature. The attackers used automated tools to input millions of random phone numbers into the contact importer which allowed them to gain access to millions of different profiles. In a Forbes

article, this was described as ” Think of it as digital fishing with a massive net—the attackers cast their net wide, pulling in whatever user data they could find.”Daniel (2024) While this exploit was found and patched sometime in 2019 it was already too late and data was stolen. This would lead to large fines for Facebook and put its users at risk of identity theft and social engineering attacks.

Facebook faced many legal repercussions for its failure to protect its users' data. Ireland’s Data Protection Commission (DPC) imposed a fine of $275 million as well as enforced corrective measures(Cyber Security Hub, 2023b). The DPC announced that it had found Meta/Facebook violated several articles of the General Data Protection Regulation GDPR. Another legal repercussion was a German court ruling that Facebook users whose data was illegally obtained were eligible for compensation. The court stated that since Meta lost control over the users' online data the users had grounds for damages without having to prove specific financial losses.

Many actions could have been taken to prevent this massive data breach from occurring in the first place. First and foremost it is incredible that the contact importer feature was released with such a glaring security risk. While it is impossible to ensure that there are no exploits in any given piece of software this wasn’t a highly complex exploit that required hundreds of hours of coding to utilize. The team behind the contact importer feature most likely lacked any professional cybersecurity oversight; however, the breach did happen and simply saying to do better will likely lead to minimal results. Regular vulnerability assessments would prove extremely useful for preventing these types of data breaches. Performing them on new features or features in development would especially be helpful to help identify vulnerabilities. A method to reduce the risk of data breaches would be data minimization. Just because you input

someone's phone number into the contact importer feature does not mean you should have access to so much personal information. I believe Facebook as a whole should prioritize data minimization for private accounts. To specifically stop the exploit many solutions could be implemented such as a limit to how many phone numbers you can put in or requiring the account's user associated with the phone number to add you before you can view them.

In conclusion, Facebook was hit with a massive data breach in 2019, which was hidden from the public until 2021. This data breach affected hundreds of millions of people and put them at risk of identity theft. The attackers used a technique called scraping to pull information from a vulnerable feature on Facebook. Facebook was found guilty of violating multiple security guidelines because of this incident and fined millions of dollars. This security breach highlights the importance of cybersecurity. There is a tremendous amount of negligence when it comes to cybersecurity, especially for giant companies such as Facebook. The $270 million Facebook was fined, means very little to them. The privacy of their users also seems to have little value to Facebook.

References

Lyskoit, V., & Lyskoit, V. (2024, December 19). *Facebook data breaches: A detailed look at the most prominent data leaks*. NordVPN. https://nordvpn.com/blog/facebook-data-breach/?utm_source=chatgpt.com

Meta. (2021, April 6). The Facts on news reports about Facebook data. *Meta*. https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/?utm_source=chatgpt.com

Data breach: Examples, causes, and how to prevent the next breach | HackerOne. (n.d.). https://www.hackerone.com/knowledge-center/data-breach-examples-causes-and-how-prevent-next-breach?utm_source=chatgpt.com

Cyber Security Hub. (2023, August 29). *Meta fined US$275 million following enquiry into April 2021 data leak*. https://www.cshub.com/data/news/meta-fined-us275-million-following-enquiry-into-april-2021-data-leak?utm_source=chatgpt.com

Facebook: What is Facebook? (n.d.). GCFGlobal.org. https://edu.gcfglobal.org/en/facebook101/what-is-facebook/1/

Bowman, E. (2021, April 10). After data breach exposes 530 million, Facebook says it will not notify users. *NPR*. https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Facebook data breach: What & how it happened? | Twingate. (n.d.). https://www.twingate.com/blog/tips/Facebook-data-breach

Newman, L. H. (2021, April 6). What really caused Facebook's 500M-User data leak? *WIRED*. https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/

Daniel, L. (2024, November 19). Facebook Data breach Fallout—Millions may receive compensation. *Forbes*. https://www.forbes.com/sites/larsdaniel/2024/11/18/facebook-data-breach-fallout-millions-may-receive-compensation/