Social Media Privacy Using EDEE Security Model

Benjamin Yankson, Eric Cajigal Delgado, Amjad Al-Jabri, Natalie Gitin and Sydney Davidson
University at Albany, USA
Byankson@albany.edu

Abstract: Social Media platforms have become a significant part of our daily lives and a modern way to connect friends and family, document our lives, and share other great personal information about our lives. These activities leave us vulnerable to privacy and security breach due to lapse security controls necessary to protect users' sensitive data on these platforms. We conducted exploratory privacy and security analysis on paramount social media platforms such as Facebook and Snapchat and determined that current Social Media privacy and security posture insufficient and proposed Social Media platform Security through "Educate," "Determine," "Enable," and "Evaluate" (EDEE) Security model to address the evolving Social Media platform security as a growing concern in Cybersecurity for individual using the platform and companies hosting the platform.

Keywords: Security, Social Media, Privacy, Facebook, Snapchat, Model

1. Introduction

Social Media platforms allow us to interact with people around the globe with a click of a button and have become a crucial part of everybody's life. These platforms allow us to call, text, share videos and pictures, share experiences, and do much more at any time or any place for free. However, there is a price of once privacy at stake considering the information, we share on Social Media platforms without any assurances that platforms are putting in effort in protecting our intimate details against hackers or misuse (Center, 2020). Some of these large corporations, who own these platforms, have taken advantage of users' insatiable appetite to share intimate information about their lives on their platforms. Yet, they have made no serious attempt to secure user information. Also, there have been instances where these companies have been complicit in misusing users' data. For example, On March 16, 2018, Facebook admitted illegally transferring 50 million user profiles to Cambridge Analytica, the data analytics firm that harvested the data without user consent (Center, 2020). Most everyday users have always assumed that buying and selling data on the Internet was only done by hackers and cyber-criminal and not the legitimate organizations who runs these platform (Yankson et al., 2019). As a result, some platforms like Facebook and Snapchat have faced the United States courts many times concerning inadequate data protection or data exploitation resulting in a user privacy breach. Several of these lawsuits have resulted in settlement scenarios where these platforms have been forced to adopt new terms and conditions to improve their security posture. However, in many instances, there have been no meaningful actions to protect user data or privacy (Viala, 2018) (CBS, 2010).

As per Gemalto (Viala, 2018), a global leader in digital security, in their 2018 worldwide database breach index findings, the first half of 2018 experienced approximately 4.5 billion data records breach in 945 separate attacks. Out of these attacks, only 6 were Social Media platform attacks; yet, they accounted for more than 56% of the overall data record exposed (Viala, 2018). Including in the Gemalto breach index is the infamous Cam bridge Analytica-Facebook privacy breach. About 87 million Facebook user data was shared without users given the opportunity to give consent or deny consent. Table 1 presents some very well-known Social Media platform data breaches with the affected Social Media platform, the year of the breach, and the number of impacted users account as evidence of the criticality of addressing privacy and security concerns in social media user. Although while Social Media platform privacy and security breaches impacts may not seem serious to some people, based on the presumed type of information posted; the data available in the vast majority of Social Media user accounts can be leveraged by a malicious attacker to conduct social engineering attack possibly leading to identity theft. Further, access to such user information can be leveraged to access even users' other personal online or employer-related authentication credentials, resulting in data breaches such as users' email, employer payroll information, or customer databases.

Table 1: Well Known Social Media Platform Data Breaches

Social Media Platform	Breach Date	Impact (users)
Facebook	Sept 2019	419,000,000
500px	Feb 2019	14,800,000
Myspace	2016	360,000,000
Google+	Dec 2018	52,500,000
Instagram	Sept 2017	6,000,000
Facebook	Sept 2018	50,000,000

Based on the current security and privacy of Social Media platform breaches, as depicted in Table 1, some users can finally become aware that Social Media platforms or associated applications abuse their data. We hypothesize that the current security controls on most of these platforms are inadequate, and the gapping privacy and security holes on these platforms or related applications can lead to serious privacy and security risk. As a result, we present a theoretical research analysis of current Social Media privacy and security posture by evaluating some key platforms. Based on the results, we present the Social Media platform Security through Educate, Determine, Enable, and Evaluate (EDEE) Security model. EDEE improves the evolving Social Media platform security as a growing concern in Cybersecurity for individuals using these platforms and companies hosting them. This research work is divided into Section 2: analysis of the background and related work. Section 3: focuses on methodology and Facebooks' and Snapchat privacy and security analysis case study. Section 4: focuses on the EDEE security model. Section 5: Summarizes the work in the Conclusions.

2. Background and Related Work

2.1 Social Media – Past to Present

Social Media platforms have only been around for a little more than two decades (Lamdan, 2015). Since its inception, we have witnessed conceptions, shutdowns, and those that have turned into obscurity, leading to a quiet and forgettable demise. In 1999, the portal was bought from the original developer by YouthStream, Media Networks, and it was shut down (Jones, 2020). As time went on and more people gained access to computers conjunctively with the creation of the Internet, there was bound to be a place for all these people to connect and socialize through an electronic medium leading to the rise of social media platforms. The Internet is now home to a few dozen Social Media platforms built solely to connect people online and made to foster a sense of community irrespective of geographical location restriction or language. Today, we have Facebook, Twitter, Instagram, Snapchat, YouTube, Tumblr, TikTok, Pinterest, LinkedIn, Discord, and GroupMe. All these platforms have a unique interface, and it's intended to provide us with an opportunity for purposeful communication in our personal and professional lives. Millions of people use these platforms daily, and it is up to the companies that build and maintain these platforms to ensure that they are secure and protect user privacy. It is important that Social Media companies see security as more important than anything considering the significant amount of user data in their respective care.

According to the PEW research group (PEW, 2020), as of Feb 2019, 72% of United States adults have at least one Social Media site account. Figure 1 presents a graph of Social Media usage growth from 2006 to 2018, demonstrating radical usage growth. It exhibits a very noticeable rapid increase in Social Media usage over the 12 years. There was a steep incline in 2008, and it continued that trend until it began to slowly flat line in 2018.

Figure 1: Trends of U.S Adults with a Social Media Account (PEW, 2020)

The reason why the usage of Social Media increased so much between 2008 and 2018 was that apps like Instagram and Snapchat were just being released in 2010 and 2012, respectively (McIntyre, 2014). These two apps and many others (Vine, Pinterest, etc.) were released within this period, which spiked the use of Social Media apps. Additionally, we can also attribute this growth to smartphone technological advancement and increased ease of access to these devices over time, thus making it easier for individuals to use these platforms more easily. Before this boom, Social Media platforms, particularly Facebook, were accessed by computers rather than smartphone devices.

2.2 Development of Security

According to the United States Department of Defense (DoD), Social Networking Sites (SNSs), such as Facebook and Snapchat, remain vulnerable to web application attacks, web browser vulnerabilities as well as social engineering attacks (Waldyogel, 2017). Amongst the web application attacks available today, the DoD specifically notes a susceptibility to "Buffer Overflow Attacks," "Cross-Site Scripting Attacks," and "Code Injection Attacks" (Waldyogel, 2017). Buffer Overflow attacks happen when an attacker injects malicious code into a program that runs beyond the allotted amount of memory. In turn, this causes the system to crash, thereby making it vulnerable to compromise. Code Injection Attacks occur when an attacker utilizes an ability "to inject malicious code into a system that" can then be executed by an application (Waldyogel, 2017). Finally, a Cross-Site Scripting Attack is a "type of code injection that occurs in the form of a browser-side script" (Waldyogel, 2017). This type of attack can result in sensitive data exfiltration and the possible destruction of the affected system. Common amongst all three types of attacks is the ability to exploit vulnerabilities on these platforms or vulnerabilities found on the targeted system to establish a compromised asset. These attacks can be utilized against flaws found in Operating Systems and software packages. DoD mentions that web browser vulnerabilities exploited while using a social media platform specifically pertained to publishing content in the form of plain text, HTML, or active content such as JavaScript or Adobe Flash (Waldyogel, 2017).

The results of a malicious payload can come in the form of downloaded malware, an HTTP request to a malicious site, or even a Denial-of-Service (Waldyogel, 2017). The DoD attributes social engineering methods, specifically "Phishing" attacks, as one of the more elusive attack vectors. A Phishing attack is a type of attack in which a falsified email is sent to the target to gain information from them, such as login credentials. This can also result in the user downloading a malicious file that appears to be legitimate. These types of attacks typically "do not flow their network email servers" and, thereby, "can escape implemented email content filters" (Waldyogel, 2017). These platforms have been hacked on multiple occasions, and the portals have evolved as a response. For example, when you log in to Facebook after some time or from an unknown location, the website makes you go through a test to make sure you are who you say you are.

3. Methodology

For this study, we select to conduct an exploratory privacy and security analysis on paramount social media platforms such as Facebook and Snapchat; to determine if current Social Media privacy and security posture is insufficient based on select cases, existing literature, and perceived privacy. Contrary to the existing null hypothesis that users privacy is protected on Social media, we hypothesize that:

H_1: The current security controls on most of these platforms are inadequate. The gapping privacy and security holes on these platforms or related applications can lead to serious privacy and security risk.

3.1 Facebook Case Study Analysis - Perceived Privacy

In 2003, a Harvard sophomore hacked into the University's student database to create a social media webpage called "FaceMash" (Huggman, 2015), which was later shutdown. In 2004, the creator of FaceMash used his knowledge and experience to make a Social Media site for Harvard students called "Facebook." The use of Facebook spread out of the boundaries of Harvard to more mainstream use. As of December 2019, Facebook hit the highest record of users. During the third quarter of 2012, Facebook active users surpassed one billion, making it the first social network to pass that mark, with approximately roughly 2.91 billion monthly active users as of the fourth quarter of 2021 (Statista, 2021). Facebook has become the most popular Social Media platform of its time. Although Facebook user growth is significant, based on Table 2, we can fairly indicate that the organization can do more to improve on security and privacy practices in order to protect users' privacy. Table 2 presents a decade of major incidents resulting in a data breach that impacted Facebook user privacy.

Table 2: A decade of data breaches impacted Facebook user privacy (Heiligenstein, 2021)

Date	Incident	Privacy Impact
April 2021	Facebook users' data was leaked on an online forum	Over 530 million user data was posted in an online hacking forum.
June 2020	Facebook accidentally made available users' information to third-party developers	Users' personal information was made available without consent.
March 2020	Hacker group captures data from Facebook Accounts	42 million more users were impacted
December 2019	Hacker group captures data from Facebook Accounts	Approximately 267 million accounts account impacted
September 2019	Data for Facebook users found on an exposed server	419 million Facebook Users impacted
April 2019	Facebook uploads users' Email contacts without permission	1.5 million users impacted
April 2019	Facebook user records found on public Server	Approximately 540 million Facebook user records captured by app developers stored in an Amazon cloud public server
March 2019	Facebook passwords stored in plaintext files exposed to employees, some dating back to 2012.	600 million Facebook user passwords had been stored in plaintext files
December 2018	New York Times discovers Facebook is sharing user data without permission to sell users' information to over 150 companies.	All Users
September 2018	Attackers access data of up to 90 million Facebook Users	50 to 90 million users impacted
May 2018	Facebook bug makes 14 million Users' private posts Public	14 million users' private posts were shared publicly even though they were initially posted with viewing limitations
March 2018	Cambridge Analytica exploited a loophole in Facebook's API that allows compiling profile data not just from users who downloaded the app but also from their friend networks	50+ million users impacted
June 2013	Bug exposes personal data of 6 million Users	approximately 6 million users sensitive personal data impacted

As per the April 2021 incident depicted in Table 2, over 533 million Facebook users' personal information, including phone numbers, was made available online (Heiligenstein, 2021). Similarly, in December 2019, approximately 267 million Facebook user accounts data, including names, phone numbers, and Facebook ID, was found unprotected on the dark web. Following the 2019 discovery, in March 2020, a second discovery was made on a server containing about 42 million more users, bringing the total up to 309 million. (Heiligenstein, 2021). In July 2019, the FTC fined Facebook $5 billion for privacy violations and mandated privacy requirements to align Facebook user privacy requirements. Based on these occurrences, as illustrated in Table 2, Facebook's user data privacy, security, and privacy rights whiles using the application show inadequacy.

Adding to privacy issues presented in Table 2, In June of 2020, Facebook accidentally shared user data with a third-party company known as "Cambridge Analytica." Before the Cambridge Analytica incident was unearthed, Facebook users were unaware that Cambridge Analytica was taking their information. A lot of the time, when another application asks for the user's permission to access Facebook, the user may just hit "accept" without reading any of the fine print. It can be very dangerous because sensitive information could be taken, such as bank account information, where the user lives, and this data could hurt them financially or physically. In addition, Facebook users, in most cases, are unaware of relinquishing their intellectual property of the content they post or private information shared. In addition to the Cambridge Analytica data breach, another incident targeted Facebook and affected over 90 million users housed on the social media platform giant (Center, 2020) (Jones, 2020). The attack vector that led to the result of the breach ended up allowing the hackers to obtain access tokens for Facebook users. The access tokens are the digital keys that keep users logged in to Facebook without asking them to re-enter their password every time they use the website. The attack was a combination of 3 bugs or software flaws, which created this vulnerability. These bugs were the "View As" feature, the code that lets people with the user a happy birthday, and the video uploader, which would create an access token even though it should not have been able to by design. To address this issue, Facebook reset all the access tokens without knowing the hackers' intentions. Nathaniel Gleicher, Facebook's head of Cybersecurity Policy, stated that it is unclear who was behind the attack and commented: "sophisticated adversaries" (Kerner, 2018).

One thing that stands out in that snippet from the Facebook Terms and Conditions is the line "consistent with your privacy and application settings (Sayin et al. 2019). This implies that there are ways to turn this off, so to say, but the user would have to know how to do this. As explained by John Quain, Minute Technology consultant, during a CBS news segment from 2010, asserted that there are ways to adjust their Facebook privacy settings to make their profile more secure (CBS, 2010). Facebook should have made the user profile secure by default, and the opportunity was given to users who decided to relax the privacy and security setting. The current Facebook privacy and security setting is Insecure by default. It is very complicated for users to change these settings to make it easier for Facebook to share user information with other websites. For example, Facebook can collect data on users' "Like" buttons, which Facebook can later sell to third-party companies for targeted advising and profile profiling. The privacy feature and consent structure of Facebook by default, the user gets no say if they want their data released to other websites and companies. Facebook makes that decision for them. Unless they know how to shut it off, it will stay on permanently (FTC, 2019).

Interacting with people on Facebook has its accessibility rules. What may be visible for some people may not be visible for others, depending on the privacy settings of all the users involved in a post. In comment and owner interaction, a person's comment may be visible beyond what they were expecting to reach. For instance, when a person changes their privacy for a post to the public instead of friends only, anyone who has commented on the post will have their interactions shown publicly without any notification explaining the change sent to them. Many people disagree with that as it shows their intended reach for their interaction was changed to beyond what they intended. Another issue is raised when a person's interaction is not visible because of the past owner's change of tag in their post. When person "A" creates a post and tags person "B," with the privacy setting set to "Friends Only," everyone in A's and B's friends list will be able to interact with the post. When "A" removes "B's" tag, everyone who commented on the post from B's list and who is not on A's friends' list will not be able to comment or like in that post. They will also not be able to access their comments or likes in that post and not even see it in their activity log. This raises an issue for those people who lost accessibility to the post as they cannot see their interactions while others can see them (Sayin et al., 2019).

3.2 Snapchat Case Study Analysis - Perceived Privacy

Since its inception, Snapchat has been used and recognized as one of the leading popular social media platforms available. However, its unique features have raised debate about the privacy rights of an individual and drawn distinctive criticism stemming from the company's leadership and internal procedures. Similar to other Social Media applications, Snapchat has been the victim of security exploits. As a result, the company has had to publicly disclose the nature of these incidents and the corrective tactics utilized in remediating them. Although social media platform such as Snapchat has faced their fair share of data security and user privacy concerns, it remains very popular amongst Social Media platforms.

In 2013, Snapchat's software fell victim to exploitation, in which 4.6 million users' details were leaked (Krebs, 2014). In the months predating this breach, researchers at Gibson Security, an Australian firm, had notified Snapchat that their software was found to be vulnerable to an exploit in which an attacker could "trawl" for name and number combinations (Krebs, 2014). This vulnerability allows an attacker to take advantage of the "Friend Finder" function on the application. As a result, a user can look up a person's phone number to find the associated user. In addition, rate-limiting was not an enabled function found on the application, thereby allowing a user to search thousands of records at a time. However, Snapchat did not take any meaningful action citing it as theoretical and not practical. As a result, Gibson Security publicly discloses the vulnerability, which within a week led to the publication of the "SnapchatDB.info" database online and forced Snapchat to disable the feature for their Friend Finder function on their application as well as implement appropriate rate-limiting (Krebs, 2014).

One of the issues prevalent amongst social media usage, especially Snapchat, is the user's perception of privacy when using the service. This platform differentiates from others in that the "users control the visibility of the contents they share with others by defining how long these contents may be available" (Rauzzino and Correa, 2017). With this in mind, we must focus on the usage paired with this social media platform amongst the population. Specifically, this social media application has notably been known to be used for sending funny pictures and selfies, but, most sensitive of all, the platform has been used for sexting and sending sexual and pseudo-sexual material. A 2017 study (Rauzzino and Correa, 2017) aimed to identify the differences amongst both sexes and all socioeconomic status about the individually placed importance of their private lives. Since the platform is especially popular amongst millennials, the study utilized 268 users between 18 and 25, with sixty percent of the sample being female (Rauzzino and Correa, 2017). The study results stated that perceived privacy

was an important concern overall by the sampled individuals, with two exceptions. It was found that the female population placed more importance on users knowing the use of their personal information and on wishing they could be notified "every time a company looks into their personal use of Snapchat" (Rauzzino and Correa, 2017). Figure 2 below illustrates participants' responses to the statement "I know about the use that is given to my info in my profile" (labeled D) (Rauzzino and Correa, 2017). This statement particularly highlights the truthfully skeptical mindset witnessed when asked if we know how Snapchat is using our data as well as other social media platforms.

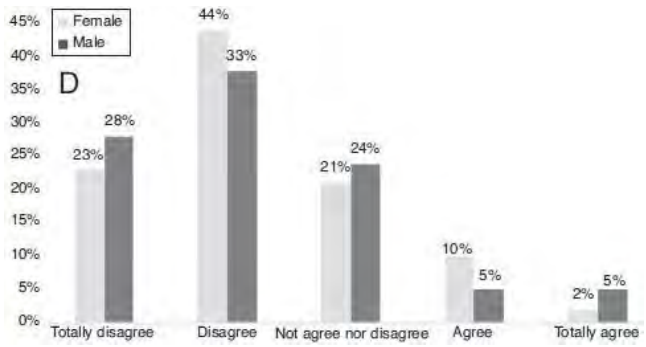

Figure 2: Participants Response to "I know about the use that is given to my info in my profile"(Rauzzino and Correa, 2017)

With this in mind, it is important for individuals who use the platform to be aware of their settings and manage them according to their privacy preferences. This issue is a combination of technical and social education. It does not seem to be disappearing any time soon, especially with the rise of Social Media usage in recent years stemming from the technological developments that have come about in the past decade.

3.3 Discussion

Several steps have been taken regarding online privacy and its concerns. Laws, regulations, and social education have been key components in achieving better practices concerning online privacy. Yet, based on the two case studies above, it is obvious that their privacy gaps range from poor security control implementation, education, and poor privacy legal control enforcement. Although some Social Media companies do a good job providing user-required privacy policies, there currently lack a shorter and clearer version of the most significant details of the policy so that consumers can know what to expect beforehand and determine whether to continue reading the entire policy or not (CBS, 2010). Based on the analysis of the two cases, the current security controls on most of these platforms are inadequate, and the gapping privacy and security holes on these platforms and related applications can lead to serious user data privacy violations.

4. EDEE Security Model

To address the issue with Social Media platform security, we present key elements needed in making best-case decisions to help users and organizations maintain important individual privacy while using social platforms. We present the Social Media EDEE model, as depicted in Figure 3.

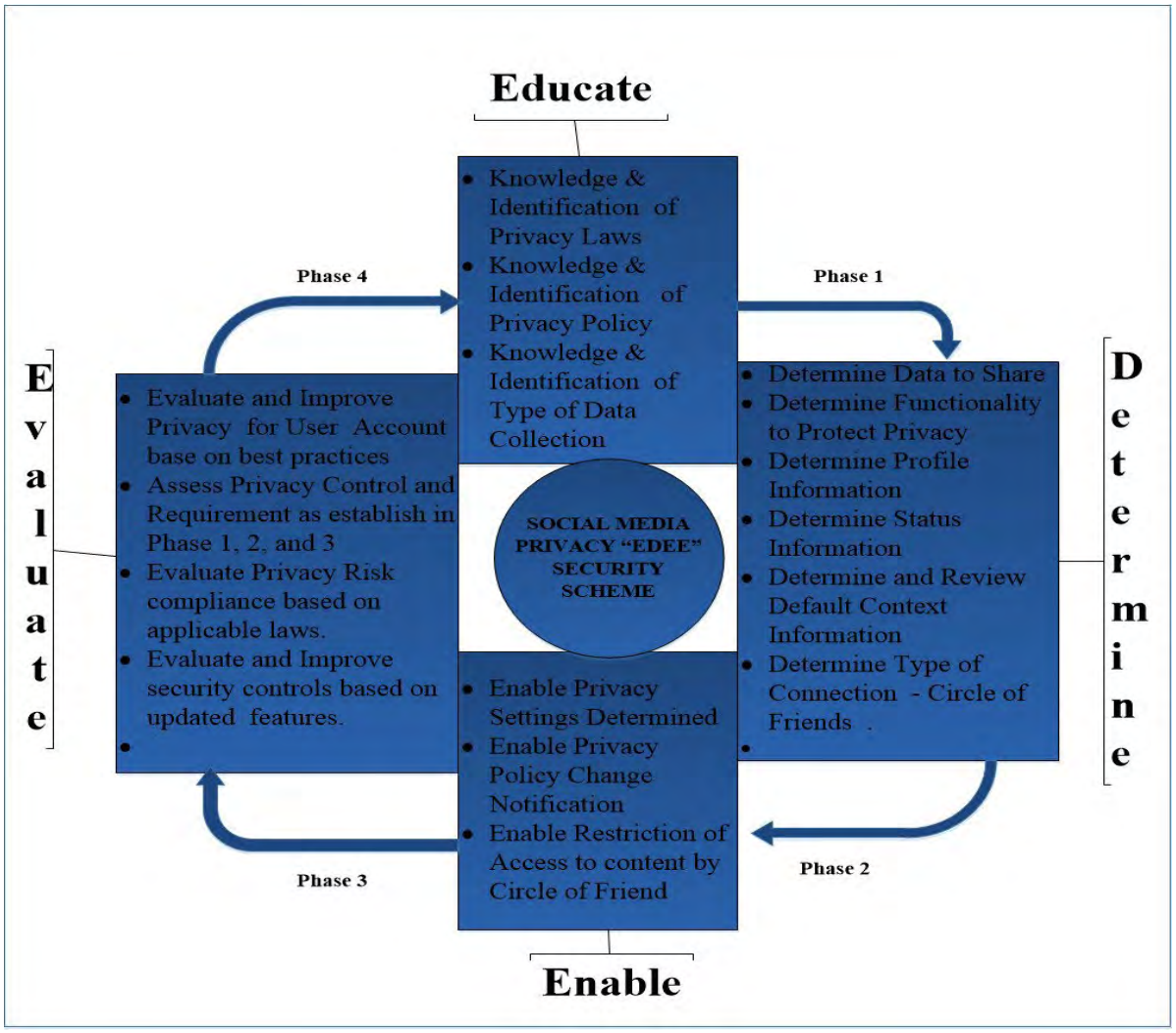

Figure 3: Social Media Privacy Through "EDEE" Security Model

As per the EDEE model, "; in Phase 1, the "Educate" Phase, the user gains knowledge about all applicable user privacy laws within the jurisdiction the platform is being used from; and the privacy policy of the platform you are using to determine what type of information the law protect and what the social media platform can collect on you. For example, suppose the user uses the platform from any European Union countries. In that case, the users will explore the data privacy rights protected under GDPR and the privacy policy of the specific platform they are using. In addition, at this phase, the users also understand the privacy implications of social media data breaches, resulting in reputation or financial loss.

In Phase 2, the "Determine" phase, the user determines what information to share and what functionality to use to protect privacy based on phase 1. This includes the user's decision on profile information, including personally identifiable or demographic information. In determining profile information, the user's role is to provide as minimum information as possible. Other information to consider here also includes the type of status update the user will post to identify an activity or event that an attacker can leverage to conduct a social engineering attack. This means users post very minimal information about present activities about themselves or the people they know. Also, in this determining phase for users to review, non-interactive information such as context data includes location information gathered and what to share with the social media platform. Last but not least is determining the content to share with and whom to share those content with. In this particular area, the idea is to have a sharing concept where users minimize privacy exposure by restricting sharing content to trusted friends within the user cycle.

In Phase 3, the "Enable" Phase, the user determines privacy settings on the social platform and enables privacy settings that disable public information sharing. The goal here is to understand the information shared by the Social Media platform publicly by default and the other information that a user shares yet can be turned off.

This includes and is not limited to a case where the platform can share information, and the user determines if the settings exist to enable who can access the content. The user can enable privacy policy change notifications. Any time privacy policy changes, the user can be aware of what has changed and how that impacts current user information or future content. The other consideration included determining approved contact such as friends and individual you follow and determining who see certain content. Further, the user enables options to disable the third application that, by default, gain access to user information.

In Phase 4, the Evaluate phase, the user actively assesses that the privacy controls enabled are functional through evaluations Phase 1, Phase 2, and Phase 3. These phases are cyclic as the user using this scheme will continue to Phase 1(Educate), Phase 2(Determine), Phase 3(Enable), and Phase 4(Evaluate). The EDEE Security Scheme allows users to observe respective privacy rights and treat them as property rights after the customer initiates the social media platform or application. Being mindful of online presence is helpful as sharing too much unnecessary information on social media can be shown to anyone and collect information. Therefore, users should only release information they feel comfortable sharing with others and not share unnecessary birth dates and locations.

5. Conclusions

Social Media platforms have been a very important part of many people's lives, considering the amount of PII and interactive. Other related information shared, the issue of privacy and security of such information should be addressed by the organization running these companies and while at the same time individuals made away of the privacy implications associated with the use of Social Media platform and effort that can be invested to protect the information they share. We demonstrated theoretically that based on the available information, some of these Social Media platforms continue to have vulnerabilities that can leave users subject to attack. Such information proves that the current security controls on most of these platforms are inadequate, and the gapping privacy and security holes on these platforms or related applications can lead to serious privacy and security risk. Our EDEE security model demonstrated that users need to be more educated about how the information they share could target them by advertisers if not to hack them. Users also need to be more aware of setting their privacy settings to achieve a perfect balance between using Social Media without sacrificing much personal information. Finally, in this work, we have demonstrated Social Media platform Security EDEE Security model can address the evolving Social Media platform user privacy concerns.

References

CBS. (2010) "Facebook Privacy" [Video File]. Retrieved from https://www.youtube.com/watch?v=smF1ZV7vikw&feature=emb_title

Center E. (2020) "EPIC - In re Facebook - Cambridge Analytica." Epic.org, Available:https://epic.org/privacy/facebook/cambridge-analytica/.

Critchley, T. (2018) "The threat on the end of the phone: the danger of contact centre agents." Computer Fraud Security, 2018(2), 13–15.https://doi.org/10.1016/ S1361-3723(18)30015-0

FTC imposes restrictions on imposes $5 billion Penalty and Sweeping New Privacy Restrictions on Facebook. (2019, July 24). Retrieved from https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5- billion-penalty-sweeping-new-privacy-restrictions

Heiligenstein M. X (2021) "Facebook Data Breaches: Full Timeline through 2022", Firewalltimes.com, 2022. [Online]. Available: https://firewalltimes.com/facebook-data-breach-timeline/ [Accessed: 30- Jan- 2022].

Huffman, B. (2015) "Developments in social media: First Amendment, Privacy, and misappropriation." Business Lawyer, 71(1), 305–319

Isaak, J., Hanna, M. J. (2018) "User Data Privacy: Facebook, Cambridge An- Analytica, and Privacy Protection." The Policy Corner, 56–59. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8436400

Jones D. (2020) "COMPANY NEWS; YOUTHSTREAM TO ACQUIRE SIXDEGREES FOR $125 MILLION", Nytimes.com, 2020. [Online]. Available:https://www.nytimes.com/1999/12/16/business/company-news-youthstream- to-acquire-sixdegrees-for-125-million.html. [Accessed: 20- Apr- 2020].

Kerner, S.M. (2018) "Facebook Data Breach Extended to Third-Party Applications." EWeek, 1-2. Retrieved from http://search.ebscohost.com.libproxy.albany.edu/login.aspx?direct=true&db=a9h&AN=132117848&site=ehost-liv

Krebs, B (2014) " Target and Snapchat suffer major data breaches". . Computer Fraud Security, 2014(1), 1,3–1,3. https://doi.org/10.1016/S1361-3723(14)70001-6

Kryder, C. (2012) "Social Media and Privacy Issues: A Matter of Common Sense." AMWA Journal: American Medical Writers Association Journal, 27(1), 36. retrieved from http://search.ebscohost.com.libproxy.albany.edu/login.aspx?direct=true&db=a9h&AN=85712790&site=ehost-live

Lamdan, S. S. (2015) "Social Media Privacy: A Rallying Cry to Librarians." Library Quarterly, 85(3), 261–277. https://doi.org/10.1086/681610

McIntyre, K. (2014) “The Evolution of Social Media from 1969 to 2013: A Change in Competition and a Trend Toward Complementary, Niche Sites”. The Journal of Social Media in Society, 3(2). Retrieved from https://thejsms.org/tsmri/index. php/TSMRI/article/view/89/43

Nadeau, M. (2019) “General Data Protection Regulations (GDPR): What you need to know to stay compliant.” Retrieved from https://www.csoonline.com/article/3202771/general-data-protection- regulation-gdpr-requirements-deadlines-and-facts.html

Ortiz-Ospina, E. (2019) “The Rise of Social Media.” Retrieved from https:// ourworldindata.org/rise-of-social-media

Perrin, A. (2015) “ Social Media Usage: 2005-2015”. Washington, D.C.: Pew Internet American Life Project. Retrieved October 12, 2015, from http://www.pewinternet. org/2015/10/08/social-networking-usage-2005-2015/

PEW (2020)"Demographics of Social Media Users and Adoption in the United States," Pew Research Center: Internet, Science Tech, 2020. [Online]. Available:https://www. pewresearch.org/internet/fact-sheet/social-media/. [Accessed: 21- Apr- 2020

Rauzzino, A., Correa, J. (2017) “Millennials' sex differences on Snapchat perceived privacy.” Suma Psicológica, 24(2), 129–134.https://doi.org/10.1016/j.sumpsi.2017. 08.002

Roberts, M. (2019) “The Cyber Threat and Globalization: The Impact on U.S. National and International Security.” By Jack A. Jarmon and Pano Yannakogeorgos. Lanham, MD: Rowman Littlefield, 2018. Journal of Strategic Security, 11(4), 85–88.https://doi.org/10.5038/1944-0472.11.4.1716

SAYİN, B., ŞAHİN, S., KOGIAS, D. G., PATRIKAKIS, C. Z. (2019) “Privacy issues in post dissemination on Facebook.” Turkish Journal of Electrical Engineering Computer Sciences, 27(5), 3417–3432.https://doi.org/10.3906/elk-1811-25

Viala V. (2018) "Data Breaches Compromised 4.5 Billion Records in First Half of 2018*", Gemalto.com, 2020. [Online]. Available:https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx.

Waldvogel, D. (2017) “Social Media and the DOD: benefits, risks, and mitigation. (COMMENTARY)(Report)”. Air Space Power Journal, 31(2), 119–125.

Whiting, R. (2018) “Don’t Be Evil, Move Fast, Think Different: How Your Social Media Phone Applications Work against Your Privacy.” Thomas Jefferson Law Review, 41(1), 127–162. Retrieved from http://search.ebscohost.com.libproxy.albany.edu/login.aspx?direct=true&db=a9h&AN=134978314&site=ehost-live

Yankson, B., Iqbal, F., Aleem, S., Shah, B., Hung, P. C. K., and de Albuquerque, (2019) "A Privacy-Preserving Context Ontology (PPCO) for Smart Connected Toys," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 2019, pp. 1-6.

Yankson, B., Iqbal, F., and Hung, (2021) "Systematic privacy impact assessment scheme for smart connected toys data privacy compliance” Int. Journal of Big Data Intelligence 8(1), , pp. 47-66.