A Survey On Privacy and Security for Online Social Network

TYAGARAJ S D[1],PAVITHRA B[2]

Post Graduate Student Department of M.C.A ,Dayananda Sagar College of Engineering, Bangalore,India

Assistant Professor, Department of M.C.A,Dayananda Sagar College of Engineering Bangalore ,India

----------***----------

Abstraction

With the rise of online social networks (OSN), the typical passive reader has become a content creator. Users can now communicate with people who share their interests by exchanging information, ideas, and self-expression in online virtual communities. However, OSN has transformed user social media into a marketplace. For OSN users, this should provide a privacy and security concern. OSN service providers gather sensitive and private data on its users, which could be abused by data miners, outsiders, or unauthorized users. This essay explains basic security and privacy concerns and offers suggestions for OSN users on how to safeguard themselves whenever they use social media.

OSN, security, traditional privacy risks, and contemporary threats

I. Introduction

Social media serve as a channel of communication for online interactions that build virtual communities via online social networks between the data owner (data generator) and viewers (end users). (OSN) [1]. The relationships between users, groups, and their social interactions are displayed in a social network's social graph. These kinds of individuals, groups, and organisations make up the network's nodes, while the links that connect them form its edges. A social network that allows users to connect with people who have similar interests, values, and/or connections in real life is known as an OSN. [2]. The modern online environment offers a wide variety of distinct social networking services. These are some of the typical characteristics of social networking. Sites[2,3]:

• All of the contemporary social networking services are web-based and run through the Internet. Through a centralized access management system, content is kept on cloud storage. Anywhere with an Internet connection and a web browser can access these contents.

• OSN users must construct a public profile in the predefined format of social networking sites. This profile information is primarily used during the social networking site's verification process.

• The majority of social networking platforms in use today make it easier for users to interact with one another socially by tying their profiles to those of other users who share information with them.

• The fact user-generated content used current OSNs for commercial purposes is intriguing element these sites.

Sharing material with as many users as possible is the core objective of OSNs. Users post their daily activities on OSNs like Facebook, Twitter, and LinkedIn. OSN users occasionally provide details about themselves and their life to friends and coworkers. However, some of the information exposed by the OSN in this released data is private and shouldn't be shared at all. Users typically share various aspects of their daily routine through status updates, photo and video sharing, or other means. Many OSN users currently use cellphones shoot photos and create films to share OSNs. These data may include embedded metadata and geographical information. OSN service providers gather variety of customer data in order to offer customised services, but it may also be exploited for financial gain. Users' data may also be disclosed to outside

parties, resulting in privacy leaks. Malicious individuals could be able to violate a person's privacy with this information [4].

Information retrieval and data privacy are two developing areas in computer science with various goals. Information retrieval strategies are available for data extraction. Furthermore, it offers set instruments for data analysis and decision-making based the data retrieved to an organization. Information is shielded from illegal access by data privacy. and unauthorized access that exposes, alters, assaults, or deletes the data internet storage or sharing. For instance, when developing solutions for information management and retrieval, researchers in information retrieval occasionally forget to address privacy issues. Data privacy experts frequently impose restrictions on information-retrieval procedures to protect sensitive data from attackers searching for personal information.

As social media has grown in popularity and online communication has become more common, More private information about people is online because to OSNs. Although a lot of the information shared through OSNs is not sensitive, some individuals nevertheless choose to disclose their personal details. As result, the disclosure of user privacy result from the availability publicly accessible sensitive data. When users' behaviours may linked publicly available data to mine it for sensitive information and extract it, the risk to their privacy increases.

Privacy can mean various things in various settings, depending on the shared materials' context. Nissenbaum[5].

outlined e importance of protecting data in the long run. help protect the contextual integrity of the shared data online. For analysis purposes, social media typically yields unwelcome information that is frequently useless. [6].

I. Literature Survey

Giving a brief outline of the privacy and security concerns brought up by the use of OSNs is the driving force behind this effort. This reality makes it vital for everyone to use technology in order to communicate easily and quickly. One form of communication that affects people in both bad and good ways is social media. OSNs speed up and make information sharing more convenient than face-to-face conversation. They enable globalization and give their users a platform for self-expression. OSNs, are moreover a new approach to create worldwide relationships. People can easily communicate with one another OSNs at any time and wherever in the world. In addition to these benefits, social media also has drawbacks, one of which is the concern over security and privacy. In addition to offering advice on how to preserve personal privacy while using OSNs, this paper discusses the problems that can impact OSN users.

III. Threats to OSNs' security & privacy

User experiences, views, and information so widely used that by 2023rs worldwide, or nearly 0.333 of entire world's population. (https://www.statista.com/topics/1164/social-networks/).The total number of user active across numerous well-known social media platforms is shown in Table 1. (https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/)

FaceBook	2750
YouTube	2790
Whatsapp	1999
Instagram	1211
weChat	688
teligram	495
Snap Chat	480
Reddit	350

Table 1: the number of active user in online social networks (OSNs)

Our ability to communicate in both our personal and professional life has changed result of social network tools. They significantly affect our social and professional lives, but they also present serious privacy and security risks. owing to the hundreds of thousands of frequent consumers they have, OSNs have attracted attackers' attention more than other target recent years. Due to extensive usage of social media, online users now face security and privacy risks. There are two categories of these dangers: conventional and modern. In addition to OSN users who do not use any OSN, other internet users are also at risk from "classic" online attacks. The second type of hazard is contemporary perils, which include OSN users' threats. because of the OSN infrastructure's potential to jeopardize user security and privacy [10]. Organizations are allegedly utilizing insufficient risk-evaluation scoring systems, according to a 2016 assessment by NopSec,a report on vulnerability state risk management (http://info.nopsec.com). Despite being one of the most popular channels for cybersecurity, the research claims that social media

is not taken into account when calculating risk evaluation scores.

a) Traditional Threats

Traditional threats have been a problem practically since the Internet's inception. malware [12], are examples of these threats. Even while researchers and industry previously mitigated these hazards by creating OSNs, They are spreading faster than ever before. Traditional threats are used to attack not only the target users but also their friends by obtaining the personal information provided by users via an OSN This is accomplished by altering the threat so that it correlates to the consumers' private qualities.

b). Viruses

Malicious software. It refers to intrusive software as a whole. It designed with the intention of entering into a person's computer and obtaining their sensitive information.The structure and user interactions of social networks make them less vulnerable to malware attacks than other online services.. The worst malware scenario entails assuming the identity of users and using their credentials send communications to their peers. The Koobface malware, for instance, disseminated over OSNs

c). Attacks by Phishers,

Phishing is the another deceptive attacking method which hacker assumes the identity of reliable third party and exploits that identity—either stolen or made up—to obtain the user's personal data. For instance, key U.K. and U.S. military officials were duped into becoming Facebook "friends" with person posing as U.S. Navy Admiral James Stavridis during an attack that the Chinese government claimed was the result intelligence [17]. The same way that phishers frequently exploited social media and adopted aliases [18–20]

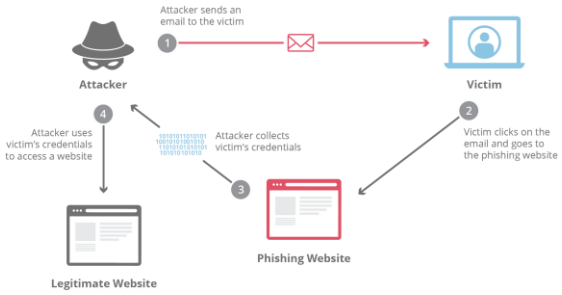

Fig:- Phishing Attacks

d) Attacks by spam

Unwanted text messages are known as spam. Spam might appear as a wall post or a spam instant message on OSNs. OSN spam is more harmful than spam in standard email since more people use it. Ads or hazardous links that could direct the recipient to phishing or malware sites are commonly included in spam communications. Spam frequently comes from fake profiles or spam software. I wish Fraudulent profiles are frequently created on someone's identity who is well-known [21].Spam bots and accounts that have been compromised frequently send spam messages [22]. But accounts that have been compromised are where the majority of spam comes from [23, 24]. Spam-filtering techniques are used to find any dangerous content before message is sent to target system.

e). Cross Site Scripting

XSS is weak web based software attack. It has a huge effect on online applications and is one of the most common and important security vulnerabilities [27]. An XSS attack gives the attacker the ability to run malicious code on the targeted user's web browser, compromise data, collect information from cookies, and save passwords and credit card numbers. Additionally, by integrating XSS with a social network architecture, On OSNs, a hacker can create an XSS worm that spreads like wildfire [28].

f) Contemporary Risks

Typically, these risks originate from OSNs. Modern attacks often focus on gathering personal data about users and their friends potential attackers, for instance, would be interested in learning about user's current employer. Users' Facebooker profiles readily be viewed by anyone if their privacy settings are violated. It only visible to their pals if they have a specific privacy setting, though. this case, the attacker make a Facebook profile and message the targeted users a friend request. When the friend request is accepted, the information is given to the attacker. Similar to this, collect users' personal information from peers, the attacker can utilise an inference attack. contents that are made available to the public.

g) Clickjacking,

Clickjacking, often referred to employment of a malicious technique to fool online visitors into clicking anything other than what they meant to is known asa redress attack on the user interface. A

perpetrator of clickjacking attacks can deceive Spam is posted on OSN members' timelines by them and unwittingly asking for "likes" on links. When conducting a clickjacking assault, attackers can additionally exploit the user PC's hardware, such as To capture their actions, use a microphone and camera [29].

h) Attacks on deanonymization

De-anonymization is data-mining approach that re-identifies a person in an anonymous dataset by comparing unidentified data with publicly available and well-known sources of information. OSNs offer reliable tools for contacts, content searching, and data sharing. Because OSNs automatically make the data they share publicly available, they are a prime target for deanonymization assaults [30].

Pseudonyms are employed in current internet services to provide data anonymity while yet making the data publicly accessible. Deanonymization techniques can be used to reidentify a person from such data, though. For instance, a recent study [31] asserts that social network data can be deanonymized with accuracy and sturdiness.

i) phoney profiles,

False profile attacks are frequent variety. assault most social networks. In this type of attack, attacker sets up account social network using fictitious information and sends messages verified individuals. It delivers spam users after getting friend requests from them. Fake profiles typically imitate humans and are automated or semiautomated. The bogus profile's objective is to gather private user information from the OSN, which is only visible to friends, and spread it as spam. Because it wastes their bandwidth, The OSN service providers are similarly concerned about the fake-profile attack [32]. It can also be used for a variety of other purposes, such advertisements. A significant IT industry exists that makes fake followers and retweets, and It is feasible due to bogus accounts [33], but viewers are given false information.

j) Attempted identity cloning

An attacker build a new phoney profile using information from stolen profile while utilising login credentials from another profile These assaults are identified by the acronym ICAs (identity clone attacks) [34]. The hacked credentials could be used on several networks or just one. Utilising the cloned user's trust, the attacker can steal data from peers or do various types online fraud [35].

k) Location Leakage

A type of risk that incorporates location leakage is data leakage. Mobile devices are being used by more and more people access social media. App typically used to link a mobile device to the internet. new privacy then danger is introduced when using mobile devices to browse the internet. location leaking. When using mobile devices to access the internet, users are more likely to reveal their position. information [40]. As a result, attackers may use the geolocation information that is disclosed on social networking sites to harm users.

l) Online harassment

Cyberstalking is when someone or a group is abused online or through social media. It might be employed for sex-related solicitation, harassment, threats, identity theft, or other offences [41]. Winkelman et al. [42] looked into the experiences and attitudes of women who had been harassed online. They did this by using an anonymous online survey. 293 women in total were questioned; the survey's participants were chosen from several OSN research sites. A sizable portion of participants, at 58.5%, were college or university students. Nearly 20persentage of women reported frequently receiving sexual messages or requests online. About 10% of them received pornographic communications from unidentified users, while more than 33% of them were subjected to cyberbullying.

M) User profiling

One frequent practice in practically all online services is user profiling, in which OSN Servers use a variety of machine-learning techniques to examine regular user behaviour in their domain. The use of user profiling offers some benefits for suggesting necessary objects to users. However, because user profiles include sensitive information, it could result in privacy breach. Therefore, user profiling is privacy concern, and in OSN setting, its protection is required. Online service providers profile users for profit, yet this practice could lead to privacy breaches [43].

IV. Findings and Conclusion

To gather information from OSN users, a questionnaire was created. Students pursuing bachelor's degrees posed questions. The study's objective was to ascertain whether consumers were

aware of or concerned about certain privacy-related options and how they affected them. The survey's participants were undergraduate students who had completed 16 years of study; They were selected by chance from a range of classifications. The survey's inquiries and responses unsatisfactory because many users even neglected to use privacy options that the service providers already provided.

Figure 1: presents an overview of the questionnaire's findings.

The participants were questioned on the following topics:

Do you have customizable privacy settings?

Almost all OSNs give their users some sort of access restriction. By employing the specialized access control mechanism offered by OSNs, users can limit access to their contents. On the other hand, 43% of Users didn't even make use of the OSNs' pre-existing privacy settings. Do you use a mobile device for social networking? If yes, does it have any passwords? Many consumers currently social networking on mobile devices. Apps that are frequently used for this. All of the apps that are installed on a mobile device are accessible to anyone with access to it. Therefore, any app that installed on user's mobile device needs to protected with password. According to this survey, 41% of Users let their mobile devices unprotected and did not even use passwords to keep them secure.

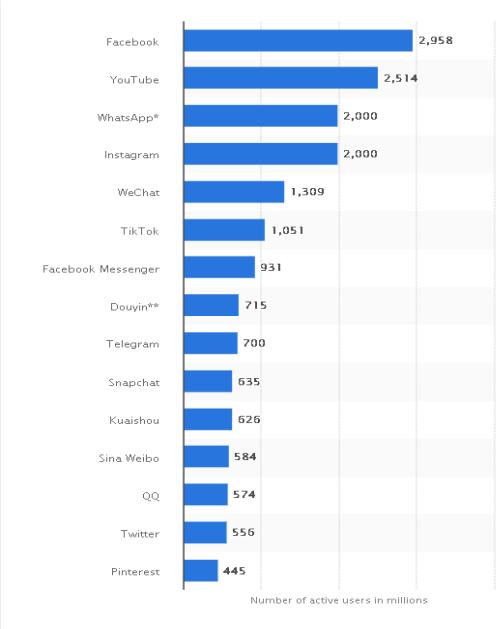

Fig 1: percent of users that are either unaware of or unconcerned with their privacy when utilizing OSN.

V. Suggestions

OSNs have lot of privacy and security concerns, but by taking preventative precautions, many privacy issues can resolved Due to users' carelessness, OSN privacy and security weaknesses are used by an attacker. Users of OSN should be aware that the information they share with their friend may end up the wrong hands, either in original form or in another context. comparable to this, shared content can be combined with other public datasets using reidentification techniques, which can lead to the reconstruction of a profile that further exposes private information [45]. Initially protecting yourself against

These privacy risks are made available by OSN-controlled privacy settings. However, due to the way they are created, these privacy settings' usefulness is insufficient. These privacy risks are accessible because to the OSNs' privacy settings. These privacy settings' limited usefulness results from the fact that they were developed as an deal with users to gather more data on them instead of maintaining their privacy.

We recommend following measures to protect users' privacy and stop unauthorised access to their content:

Privacy setting:

Sadly, 80 percent users don't check their OSNs or are aware of them. of their profile's privacy settings,regardless of whether default privacy settings or suitable privacy that meets the needed level have been provided [46]. Owners can alter settings to hide contents from unauthorised access even if OSNs offer specific level access control to data.

Nearly all OSNs limit privacy through their privacy settings [47] The default privacy and security settings are still being used by users of many social networks [48, 49].

Personal Information: After being shared third party, there guarantee contents will remain secret. Therefore, sharing must be avoided by users. Private information not required on OSNs. Users may be aware of the importance of privacy, but due to OSN privacy regulations, there are usually misconceptions about the privacy of the content that users submit on such sites [50]. As an illustration, research found that 94% of users shared OSN content that was intended for private use [51].

Location Information: Numerous mobile applications collect user location information. OSNs have the ability to make use of location data and share it with outside parties, frequently financial advantage, undermines privacy. People don't use this kind of location data. collected by OSNs, however they typically include location tags in posts. If attackers are aware of your current location, they may misuse this location information. In order to safeguard themselves from these possible attackers, users are urged to avoid transmitting their location information over OSNs.

Applications from third parties:

Numerous privacy and security issues are brought up by applications from third parties. due to the hosting of their code separately from OSN and user controls. Naturally, this makes it more difficult for users and the OSN to control and monitor the operations of the programme and to take proactive measures to thwart detrimental incursion. Because the data have been relocated outside of the OSN, Users are not in charge of how their content is utilised or shared [57]. They need to uninstall third-party applications to safeguard their data from being exploited.

VI.. Conclusions

In addition to privacy and security issues, social media has also been linked to other difficulties that should be acknowledged. One such problem is the possibility of online harrassment and cyberbullying, which can have negative psychological and emotional impacts on people. Social media platforms' guarantee of anonymity might occasionally encourage bad behaviour and endanger users' wellbeing.

Furthermore, it is impossible to ignore social media's addictive qualities and effects on mental health. Anxiety, despair, and loneliness have all been related to excessive use of these sites. Users must be mindful of their online behaviours and engage in digital wellbeing to maintain a balance between their online and offline connections.

In conclusion, social media platforms have significantly improved connectivity and communication. They do, however, present issues with security, privacy, cyberbullying, and mental health. By being knowledgeable and using appropriate digital practices

REFERENCES

1. Boyd, D.M.; Ellison, N.B. Social network sites: Definition, history, and scholarship. J. Comput.-Mediat. Commun. 2007, 13, 210–230. [CrossRef]

2. Obar, J.A.; Wildman, S. Social media definition and the governance challenge: An introduction to the special issue. Telecommun. Policy 2015, 39, 745–750. [CrossRef]

3. Kaplan, A.M.; Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. Bus. Horiz. 2010, 53, 59–68. [CrossRef]

4. Shozi, N.A.; Mtsweni, J. Big data privacy in social media sites. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, Southern Africa, 30 May–2 June 2017; pp. 1–6.

5. Nissenbaum, H. Privacy as Contextual Integrity. Wash. L. Rev. 2004, 79, 101–139.

6. Davison, H.K.; Maraist, C.C.; Hamilton, R.; Bing, M.N. To Screen or Not to Screen? Using the Internet for Selection Decisions. Empl. Responsib. Rights J. 2012, 24, 1–21. [CrossRef]

7. Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. J. Comput.-Mediat. Commun. 2014, 19, 248–273. [CrossRef]

8. Marwick, A.E.; Boyd, D. Networked privacy: How teenagers negotiate context in social media. New Media Soci. 2014, 16, 1051–1067. [CrossRef]

9. Ashtari, S. I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy. J. Inf. Priv. Secur. 2013, 9, 80–82. [CrossRef]

10. Fire, M.; Goldschmidt, R.; Elovici, Y. Online social networks: Threats and solutions. IEEE Commun. Surv. Tutor. 2014, 16, 2019–2036. [CrossRef] 11. Heymann, P.; Koutrika, G.; Garcia-Molina, H. Fighting spam on social web sites: A survey of approaches and future challenges. IEEE Internet Comput. 2007, 11, 36–45. [CrossRef]

12. Everett, C. Social media: Opportunity or risk? Comput. Fraud Secur. 2010, 2010, 8–10. [CrossRef]

13. Alarm, S.; El-Khatib, K. Phishing Susceptibility Detection through Social Media Analytics. In Proceedings of the 9th International Conference on Security of Information and Networks, Newark, NJ, USA, 20–22 July 2016; pp. 61–64.

14. Nithya, V.; Pandian, S.L.; Malarvizhi, C. A survey on detection and prevention of cross-site scripting attack. Int. J. Secur. Appl. 2015, 9, 139–152. [CrossRef]

15. Baltazar, J.; Costoya, J.; Flores, R. The Real Face of Koobface: The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research. 2009. Available online: https://www.trendmicro.de/cloud-content/us/pdfs/ security-intelligence/white-papers/wp_the-real-face-of-koobface.pdf (accessed on 27-06-2023).

16. Alghamdi, B.; Watson, J.; Xu, Y. Toward detecting malicious links in online social networks through user behavior. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence Workshops, Omaha, NE, USA, 13–16 October 2016; pp. 5–8.

17. Protalinski, E. Chinese Spies Used Fake Facebook Profile to Friend Nato Officials. Available online: https: //www.zdnet.com/article/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials/ (accessed on 27-06-2023).

18. Dvorak, J.C. LinkedIn Account Hacked. Available online: https://www.pcmag.com/article2/0,2817, 2375983,00.asp

19. Miller, S. Sen. Grassley's Twitter Account Hacked by SOPA Protesters. Available online: https://abcnews. go.com/blogs/politics/2012/01/sen-grassleys-twitter-account-hacked-by-sopa-protesters/ (accessed on 1 November 2018).

20. Vishwanath, A. Getting phished on social media. Decis. Support Syst. 2017, 103, 70–81. [CrossRef]

21. Fire, M.; Katz, G.; Elovici, Y. Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. Human J. 2012, 1, 26–39

22. Egele, M.; Stringhini, G.; Kruegel, C.; Vigna, G. Towards detecting compromised accounts on social networks. IEEE Trans. Dependable Secure Comput. 2017, 14, 447–460. [CrossRef]

23. Grier, C.; Thomas, K.; Paxson, V.; Zhang, M. @spam: The underground on 140 characters or less. In Proceedings of the 17th ACM conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; pp. 27–37

24. Gao, H.; Hu, J.; Wilson, C.; Li, Z.; Chen, Y.; Zhao, B.Y. Detecting and characterizing social spam campaigns. In Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, Melbourne, Australia, 1–3 November 2010; pp. 35–47.

25. Thomas, K.; Grier, C.; Ma, J.; Paxson, V.; Song, D. Design and evaluation of a real-time URL spam filtering service. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 22–25 May 2011; pp. 447–462.

26. Gao, H.; Chen, Y.; Lee, K.; Palsetia, D.; Choudhary, A.N. Towards Online Spam Filtering in Social Networks. In Proceedings of the 19th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, 5–8 February 2012; pp. 1–16.

27. Gupta, S.; Gupta, B.B. Cross-Site Scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. Int. J. Syst. Assur. Eng. Manag. 2017, 8, 512–530. [CrossRef]

28. Faghani, M.R.; Nguyen, U.T. A study of XSS worm propagation and detection mechanisms in online social networks. IEEE Trans. Inf. Forensics Secur. 2013, 8, 1815–1826. [CrossRef]

29. Lundeen, R.; Ou, J.; Rhodes, T. New Ways Im Going to Hack Your Web APP. Black Hat Abu Dhabi. Available online: https://www.blackhat.com/html/bh-ad-11/bh-ad-11-archives.html#Lundeen (accessed on 1 November 2018).

30. Ding, X.; Zhang, L.; Wan, Z.; Gu, M. A brief survey on de-anonymization attacks in online social networks. In Proceedings of the IEEE International Conference on Computational Aspects of Social Networks (CASoN 2010), Taiyuan, China, 26–28 September 2010; pp. 611–615.

31. Gulyás, G.G.; Simon, B.; Imre, S. An Efficient and Robust Social Network De-anonymization Attack. In Proceedings of the Workshop on Privacy in the Electronic Society, Vienna, Austria, 24 October 2016; pp. 1–11.

32. Wani, M.A.; Jabin, S.; Ahmad, N. A sneak into the Devil's Colony-Fake Profiles in Online Social Networks. Available online: https://arxiv.org/ftp/arxiv/papers/1705/1705.09929.pdf (accessed on 29 October 2018).

33. Perlroth, N. Fake Twitter Followers Become Multimillion-Dollar Business. The New York Times, 9 April 2013. Available online: https://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimilliondollar-business/?_php=true&_type=blogs&ref=technology&_r=0 (accessed on 1 November 2018).

34. Kharaji, M.Y.; Rizi, F.S.; Khayyambashi, M.R. A New Approach for Finding Cloned Profiles in Online Social Networks. arXiv, 2014, arXiv:1406.7377.

35. Lewis, J. How spies used Facebook to Steal NATO Chief's Details. The Telegraph, 10 March 2012.

36. Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B. Preventing private information inference attacks on social networks. IEEE Trans. Knowl. Data Eng. 2013, 25, 1849–1862. [CrossRef]

37. Viswanath, B.; Bashir, M.A.; Crovella, M.; Guha, S.; Gummadi, K.P.; Krishnamurthy, B.; Mislove, A. Towards Detecting Anomalous User Behavior in Online Social Networks. In Proceedings of the USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 223–238.

38. Torabi, S.; Beznosov, K. Privacy Aspects of Health Related Information Sharing in Online

Social Networks. In Proceedings of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, Washington, DC, USA, 12 August 2013; p. 3.

39. Scism, L.; Maremont, M. Insurers Test Data Profiles to Identify Risky Clients. The Wall Street Journal, 19 November 2010.

40. Humphreys, L. Mobile social networks and social practice: A case study of Dodgeball. J. Comput.-Mediat. Commun. 2007, 13, 341–360. [CrossRef]

41. D'Ovidio, R.; Doyle, J. A study on cyberstalking: Understanding investigative hurdles. FBI Law Enforc. Bull. 2003, 72, 10–17.

42. Burke Winkelman, S.; Oomen-Early, J.; Walker, A.D.; Chu, L.; Yick-Flanagan, A. Exploring Cyber Harassment among Women Who Use Social Media. Univers. J. Public Health 2015, 3, 194–201. [CrossRef]

43. Ali, S.; Rauf, A.; Islam, N.; Farman, H.; Khan, S. User Profiling: A Privacy Issue in Online Public Network. Sindh Univ. Res. J. (Sci. Seri.) 2017, 49, 125–128.

44. Fuchs, C.; Trottier, D. Towards a theoretical model of social media surveillance in contemporary society. Commun. Eur. J. Commun. Res. 2015, 40, 113–135. [CrossRef]

45. Gross, R.; Acquisti, A. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7–10 November 2005; pp. 71–80

46. Zhang, W.; Al Amin, H. Privacy and security concern of online social networks from user perspective. In Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP2015), ESEO, Angers, Loire Valley, France, 9–11 February 2015; pp. 246–253.

47. Carminati, B.; Ferrari, E.; Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B. Semantic web-based social network access control. Comput. Secur. 2011, 30, 108–115. [CrossRef]

48. Strater, K.; Richter, H. Examining privacy and disclosure in a social networking community. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 18–20 July 2007; pp. 157–158

49. Miltgen, C.L.; Peyrat-Guillard, D. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. Eur. J. Inf. Syst. 2014, 23, 103–125. [CrossRef]

50. Fletcher, D. How Facebook Is Redefining Privacy. Available online: http://content.time.com/time/magazine/article/0,9171,1990798,00.html (accessed on 10 November 2018).

51. Madejski, M.; Johnson, M.; Bellovin, S.M. A study of privacy settings errors in an online social network. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, Lugano, Switzerland, 19–23 March 2012; pp. 340–345.

52. Penni, J. The future of online social networks (OSN): A measurement analysis using social media tools and application. Telemat. Inform. 2017, 34, 498–517. [CrossRef]

53. Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. Design and analysis of a social botnet. Comput. Netw. 2013, 57, 556–578. [CrossRef]

54. Makridakis, A.; Athanasopoulos, E.; Antonatos, S.; Antoniades, D.; Ioannidis, S.; Markatos, E.P. Understanding the behavior of malicious applications in social networks. IEEE Netw. 2010, 24, 14–19. [CrossRef]