Privacy in Microblogging Online Social Networks: Issues and Metrics

Samia Oukemeni
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya
CYBERCAT - Center for Cybersecurity Research of Catalonia
Barcelona, Spain
soukemeni@uoc.edu

Helena Rifà-Pous
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya
CYBERCAT - Center for Cybersecurity Research of Catalonia
Barcelona, Spain
hrifa@uoc.edu

Joan Manuel Marquès Puig
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya
Barcelona, Spain
jmarquesp@uoc.edu

***Resumen*—In the era of digital life, privacy is threatened by the rapid expansion of online social media, especially Microblogging Online Social Networks (MOSNs). Whether users are connected in real life or not, microblogging systems are a popular form of Online Social Networks (OSNs) that allow users to post short messages, share interests, and communicate with each other. Despite this popularity, they have a poor reputation in terms of protecting the privacy of users. The present paper examines different types of privacy threats and concerns in MOSNs. The threats can be either classic and common to other online platforms or specific to the environment of OSNs. In addition, this article describes various models that assess and quantify privacy in OSNs and finally proposes a new generic framework to evaluate the privacy in MOSNs. The proposed framework indicates the level of privacy protection provided by the system and helps to compare different MOSNs.**

***Index Terms*—Microblogging online social networks, privacy, security, issues, measurements, metrics, framework;**

I. Introduction

Privacy is recognized internationally as a fundamental human right. However, in this data-driven world, protecting privacy becomes one of the dominant issues as it is threaten by the terabytes of personal information revealed everyday. Privacy is an intuitive term that can be interpreted differently from abstract and wide to technical and specific. It is a common concept yet not easy to define. According to Oxford dictionary [1], privacy is defined as:

> ” A state in which one is not observed or disturbed by other people”.

The protection of privacy is usually associated with cryptography, authorization, and anonymization. Westin in 1968 defined privacy as ” the right to select what personal information about me is known to what people” [2]. Bünnig et al. [3] described privacy as protecting personal information from malicious and unauthorized entities. Privacy can also be defined as a set of policies that enforces the protection of private information [4]. Another definition of privacy is to hide some details from others [5]. All these different explanations and yet no single definition of privacy encompasses all aspects of the term.

Due to the exponential development of information technologies, protecting the privacy becomes extremely important, especially in the field of social media and microblogging services. A microblogging network is a popular form of Online Social Networks. It is a weblog where users are allowed to send snippets of a small number of characters (between 140 and 310 characters) [6]. The number of registered users for microblogging services is increasing each month. It reaches nearly 1 billion monthly active users between Twitter, Tumblr, etc. [7], [8]. MOSNs have become a source of news coverage and means of propagating all sorts of information [9], [10] as it happens in the coverage of the 2016 US presidential election [11].

As different as they can be, all microblogging systems offer to their users the ability to create customized profiles, follow and be followed, share interests and keep updated on the trending topics and news [12]. Users can include multimedia content in their posts, like pictures, links, or video links, and they can keep track of activities from other users, trends, companies, brands or celebrities [13].

However, such information attracts malicious users and attackers to gather, aggregate and exploit the data generated by users to commit cyber crimes against the users such identity theft, phishing, social scams, and social engineering. For example, the website Please Rob Me [14] raises the awareness of the danger of oversharing in social media, especially the information about the geographical location on Twitter. The website scans the feeds from Twitter and shows when the users tweet out locations other than their home. Furthermore, most of the known microblogging companies handle the users' data and generate their revenue by gathering and selling the data to third-party channels for advertisement or statistical purposes [15]. Despite the fact that MOSNs might provide privacy settings to fine-tune the visibility of profiles and posts, they often remain insufficient. Furthermore, privacy policies offered by the systems are too vague and expressed in a language that makes them difficult for users to understand how their information is handled and shared [18]. In fact, on the 17th of March 2018, a former Cambridge Analytica contractor admitted that the firm harvested more than 50 million Facebook profiles without permission to build an algorithm that targeted US voters with personalized political advertisements based on their psychological profile [16]. The data was collected through an app called ”thisisyourdigitallife”, built for academic purposes [17].

MOSNs have brought new challenges to privacy-oriented companies and academic community. Researchers have dis-

cussed new privacy-preserving controls and techniques and they have proposed different microblogging online social systems to protect and enhance the users' privacy like Diaspora [19] and Galaxy 2 [20]. As the definition of privacy is ambiguous and elusive, there is no standard means of how to build an efficient privacy-protecting system. Thus, the need for techniques to evaluate and measure the privacy of MOSNs. Some research analyzed the privacy settings provided in the systems to evaluate the privacy level [21]. Some other works proposed new models based on mathematical formulas to assess the privacy in the MOSNs. Our findings show that in spite of the number of proposed methods for measuring the privacy, there is no comprehensive framework that takes in all the aspects of privacy goals, nor a general proposal for measuring any MOSN and so, a global evaluation and comparison between different systems is not possible.
In this paper, we summarize privacy issues and challenges in MOSNs as described in section II. Section III provides an extensive catalog of privacy-specific measurement models in OSNs in general. This paper also contributes to the former subject by providing a comprehensive privacy measuring framework. An overview of the framework is described in section IV. Section V presents the conclusion of the present paper, including future work.

II. Privacy in Social Networks

Privacy has been a concern, even before the rise of new information technologies. But with the booming of online applications and services that require creating profiles with personal information, several data breaches targeting private information have intensified. The best-known example of data breach happened in 2014 when Sony Corp suffered the biggest data breach known in modern times, it was even labeled "the Hack of the Century". The cyber-invasion cost Sony Corp billions US dollars not only in terms of financial losses but also in terms of reputation. The attackers stole confidential internal documents such as movie scripts and highly classified and personal information of Sony employees (internal emails, salaries, and more than 47,000 social security numbers) [22]. These repeated incidents have highlighted the need to protect sensitive and private data, beyond deploying basic access control policies. As one of the answers to this need, the EU Parliament approved the General Data Protection Regulation (GDPR) on 14 April 2016. The new regulation was designed to harmonize data privacy laws across Europe and to protect the privacy of the users. It gives the users the right to access, download and erase their data. Also, the concept of privacy by design becomes a legal requirement in building new online platforms. GDPR is enforced by 25 May 2018 [23]

II-A. Understanding Privacy in the Context of MOSNs

MOSNs are now a trendy way for users to express themselves and connect with their entourage. Compared to regular OSNs, microblogging networks meet the need of a faster mode of communication to reach a larger group of people. By using shorter posts, the time to write and post an update is drastically shorten which allows a microblogger to post frequently several messages every day. Also, the popularity of MOSNs is due to the openness and the flexibility provided to the users. They can connect and communicate with their favorite celebrity, brand, politician, athlete or even other regular users without the obligation of a pre-existing social relationship.
To stay active in an MOSN, the users voluntarily share personal information about themselves without prior knowledge of who can access their private data or how it is handled by the service providers. A study of Twitter users sharing behavior shows that between 40 % to 50 % of tweets include personal information about the author, including personally identifiable information, contact data, health information and location data [24]. This fact of providing sensitive information willingly makes the protection of privacy more complex.
Furthermore, nearly all online companies like Twitter and Tumbler generate their profits by gathering, storing and processing users' data in order to sell them for advertisement or statistical purposes. These companies claim that before selling the data, they anonymize them, meaning that they remove any explicit information from the dataset that can directly identify the users (name, Social Security Numbers (SSNs)...) [25]. However, recent research [26] indicates that from the anonymized dataset of 1.5 million people, a person can be identified with 95 % accuracy in only four spatiotemporal points. Moreover, Montjoye et al. [27] studied an anonymized dataset of credit card transactions of 1.1 million people and were able to re-identify 90 % of individuals knowing again only four spatiotemporal points. In other words, it is simple and easy to identify a person based on non-identifying attributes (sex, birthdates..). Therefore, posting news and interest in social media can put the privacy of data in jeopardy when it is placed in the wrong hands.

II-B. Privacy Issues and Attacks in MOSNs

With the increasing popularity, microblogging systems and online social networks in general have become a hub for cybercriminal activities. Attackers and malicious users are drawn to these platforms and specifically to the critical data revealed, intentionally or unintentionally, by the users. With simple fake accounts, the adversary can engage the victims and spread malicious contents. Most of the attacks are driven by the purpose of harassment, identity theft and stealing information related to bank accounts or social security numbers. [28].

Some privacy risks are more amplified in MOSNs compared to traditional service systems. These include:

- Malicious insiders that can connect with the victims and act as legitimate users.
- Unintentional disclosure of personal information from users like geographic location, interests, etc.
- The joint utilization of different online social networks that can bring in a new type of attacks based upon the fusion of multiple profiles of the same user across multiple OSNs.
- Third-party applications that use the API provided by the MOSNs and they can access the users' profiles. Also, these applications may have vulnerabilities that attackers can exploit to get to the users' accounts. For example, a vulnerability in Twitter Counter, a popular tool for analyzing Twitter followers, was exploited in 2017, which has led to taking control of hundreds of high-profile Twitter accounts like the European Parliament, UNICEF, and Amnesty International [29].

In addition to classic attacks on any online platform, like Denial-of-Service (DoS) Attack, SQL injection, Cross-Site Scripting XSS, social spamming, flooding, phishing and malware attacks [28], [30], [31], [32], there are other specific social media attacks. For example:

- Identity clone and theft attacks aim to create a fake profile in the system or clone and duplicate user's online presence to fool other users and commit fraud or espionage [33].
- Social profiling refers to the process of collecting information and constructing a user's profile. This occurs through aggregating information that is publicly and voluntarily published in MOSNs [34], [35].
- Social link prediction and disclosure occurs when an adversary predicts or discloses hidden links and masks relationship between two users, a relationship that the users would like to remain hidden from the public [36].
- Conversation and communication tracking is a type of profiling attack where the adversary tracks the communication feed of users and collects information about the users and their interests. This allows the adversary to create a more detailed user profile [37].
- Sybil attack or fake profiles attack [30], [38] is an attack where a single entity masquerades as multiple identities with the objective to make as many friends as possible with legitimate accounts. The influence of the adversary increase in the network and thereby engages in malevolent activities like spamming and identity fraud. This type of attacks is used also to increase the visibility of the content and manipulate the view counts and the network decisions.
- Clickjacking is used to trick users to redirect them to malicious sites by clicking on attractive buttons or links in a post [28], [39].
- De-anonymizing attacks are used to re-identify a particular user in an anonymized dataset [30].
- Crawling is the collection and aggregation of available information across the profiles of multiple users in the MOSN. In this attack, the adversary doesn't target one particular user. The information gathered can be used for users' activities analysis or in marketing advertising [37], [40].

III. Measuring and Evaluating Privacy in MOSNs

With the large number of threats and attacks on MOSNs, privacy oriented service providers and researchers have introduced new systems that offer microblogging functionalities and at the same time advocate for privacy protection. Some systems add a privacy layer while others are built using privacy by design methodologies.

With a multitude of privacy controls and techniques implemented in these new MOSNs, a necessity of services evaluating models appeared. These models are used to evaluate the effectiveness of these private networks. However, the challenge is how to measure and evaluate the privacy in MOSNs since defining privacy itself is a challenging issue. Privacy is subjective because it is related to what people consider sensitive, i.e. which information each person wants to keep secret. This can change based on the context and with the course of the time.

III-A. Metrics and Measurements

When we talk about privacy assessment and evaluation, we talk about metrics. A metric is defined as a system of measurement, i.e. the techniques and procedures, that evaluate and quantify an issue [41]. Metric and measurements are similar enough that the two terms are commonly used interchangeably. However, there is a difference between the two terms: measurements provide single-point-in-time views of specific factors while metrics provide standardized procedures and calculation methods to generate relevant numbers of the measured system.

III-B. Privacy Evaluation and Scoring in MOSNs

Privacy metrics can be used for decision making and in assessing, monitoring and predicting potential privacy threats in the system. Privacy evaluation empowers the academic community with a strong understanding of privacy and a better protection of information in the MOSNs.

In online social networks, some attempts to evaluate and quantify the privacy are found in the literature. In 2009, Maximilien et al.[43] proposed a framework to calculate the privacy score based on the sensitivity and the visibility of attributes of a social network. They conducted a survey where the questions were designed to determine the privacy degree that users were willing to disclose each information in their profiles. The authors didn't offer any dataset to measure the effectiveness of their model. Liu and Terzi extended the approach in [44]. They developed a mathematical model to measure the privacy score of the users, based on the sensitivity and the visibility of attributes, using concepts from Item Response Theory (IRT) [45]. To evaluate the effectiveness of the score, the authors used both synthetic and real-world datasets. However, this model is not generalized to any kind of OSN since it assumes that the users are independent, the attributes are independent and it doesn't take into consideration the inferred data. Srivastava and Geethakumari extended Liu et al.'s model and included the hidden data in [46]. They also introduced privacy leakage that quantifies the privacy exposure for some user from a message. Both models [44] and [46] assumed that the sensitivity and visibility are the same across all users. Petkos et al. [47] enhanced the previous models and proposed a PScore framework. PScore considers the user's personal preferences in scoring the attributes, it includes the hidden and inferred information and it is structured based on different types of information. Pensa and Di Blasi introduced a new privacy assessment framework in [48]. This work was inspired from the model proposed by Liu and Terzi [44], it takes into consideration the circle (friends) of the users where the willingness ratio of a user to disclose information is proportional to the number of her or his friends. The framework measures the privacy leakage and set a model of privacy preferences for each user. If the score exceeds a given threshold, the framework notifies the user about the privacy risk. The privacy score is based on both the sensibility and the visibility of user profile attributes.

Some researchers took another approach to evaluate privacy beyond the sensitivity and visibility properties. Becker et al. [49] introduced PrivAware, a tool that quantifies the privacy risk from the amount of information inferred in social networks. PrivAware maps the privacy risk to a grading score and

sets recommended actions for users. Ngoc et al. [50] presented a privacy metric calculated based on the probability and entropy theory. This metric quantifies the information leaked in the users' posts. The authors built the metric based on the idea of how much an attacker can reveal of hidden sensitive information of a user from the sentences in the posts. Talukder et al. [51] proposed Privometer to measure the leakage of sensitive information based on the profiles of users and their social graphs. Privometer takes into consideration also the leakage of sensitive information from applications installed in the user's friend profiles. Privometer ranks the relationships of users based on the amount of information leakage and suggests self-sanitization recommendations to control the leakage. Akcora et al. [52] suggested measuring the risk score based on the feedback from users about others users and the sensitive information disclosure. The framework computes the risk level in terms of the friends' attitude and the similarities with the users. The authors used Facebook and real datasets to evaluate the effectiveness of the model. Vidyalakshmi et al. [53] developed a privacy scoring framework of friends to assist users in assessing their information sharing behavior and in taking a decision of who can see what information. The scores are based on the output of a friend and its position in the sorted list of friends and the total number of friends of the user.

Nepali and Wang [54] introduced a new model to monitor privacy exposure in real time. The model uses real data from social networks, instead of data from surveys. The privacy risk indicator (PIDX) is calculated based on the sensitivity and the visibility of attributes. The obtained value is used for privacy monitoring and risk control. SONET is based on 2 components, attribute to attribute (actor model) and user to user relationships (community model). SONET included hidden information that is not firsthand available, but it infers from direct data. The model is used to monitor the level of privacy in the system and to protect users from sensitive information disclosure. The authors extended the actor model of SONET in [55] and the community model in [56]. They included 3 metrics: known attribute list (direct, hidden and virtual), attributes sensitivity and attributes visibilities. The authors introduced the OSNPIDX tool in [56] as an implementation of SONET model. OSNPIDX defines an actor with 20 static-assigned privacy impact factor attributes.

The existing work in the field of privacy scoring models reveals that it is rather limited and is still relatively unexplored. Additionally, all the models evaluate privacy in OSNs from the user's perspective (the profile, the visibility and sensitivity of the items published, the information leakage from social graph...). There is no holistic view on evaluating the privacy in social networks and clearly, it still lacks a generic framework that evaluates the privacy and not specific to only one aspect or to one MOSN. *Table I* summarizes the reviewed privacy scoring approaches.

IV. Privacy Measurement Framework for Microblogging Online Social Networks

As explained in the above (see section III), all the reviewed frameworks and scores focus on one aspect to assess and evaluate the privacy in OSNs, either they compute privacy scores based on the sensitivity and visibility of some attributes in the systems or they measure the information leakage from social graphs. Some of these frameworks are system-specific tools that can be used to evaluate only one specific OSN. They don't include other aspects of privacy protection goals like how the system protects the confidentiality of the data and users, or how the storage type can affect the privacy of the data. Also, all the frameworks focus on the impact of the visibility of data to other users but not to the system provider. In response to the limitations of these privacy evaluation frameworks, we propose an enhancing generic privacy scoring framework to quantify, assess and evaluate privacy in MOSNs. The framework is generic and universal, and allows comparing the privacy protection between different systems. Our proposed framework is designed with these considerations in mind:

Figura 1. PDSA life cycle

- It must be generic and applicable to different MOSNs and also it can be fine-tuned to meet the needs of specific situations and be modified to fit the needs of specific system.
- It must take into consideration all the MOSNs stakeholders namely: the users (profile, relationships, groups...), the data generated by the users, the system itself and third-party components.
- It must include security metric as well because of the existing synergy between security and privacy and also, because security is necessary to achieve privacy.
- It must take into consideration all types of data as proposed in [57].

The proposed framework follows a four-steps methodology inspired by the Plan-Do-Study-Act cycle (PDSA) [58] (See *Fig.1*):

- **Step 1** sets the boundaries, it determines the objectives and the scope of of the framework.
- **Step 2** follows the Goal-Question-Metric (GQM) paradigm [59] to design the engine of the framework. The engine monitors and gathers data from different sources, including user feedback, risk assessment reports, research surveys, event loggers..., and answers the questions defined in each goal. We define 4 metrics that provide quantitative information to answer the following goals:
  - Metric 1: How the system protects itself from the privacy and security point of view.
  - Metric 2: How the privacy and the security of data are handled in the system.
  - Metric 3: How the system protects the users and the data.
  - Metric 4: How various assumptions and functions in the system might affect the privacy and the security.

Tabla I
OVERVIEW OF THE REVIEWED PRIVACY SCORING APPROACHES

Privacy score	Description	Features
Privacy Scores: [43], [44], [46], [47], [48]	A score generated based on the sensitivity and visibility of the items posted by an OSN user. Some scoring frameworks take into consideration the hidden and inferred information and the circle (friends) of the users.	Profile items, sensitivity per item, visibility per item. For some articles, leakage per item is also included.
PrivAware: [49]	The score is calculated based on the total of visible attributes divided by the total of attributes in a profile.	The amount of information inferred in social networks
Privometer: [51]	A score generated based on the sensitivity of the profiles of users and their social graphs.	Sensitive attribute inference from the information available in immediate friends' profiles.
Privacy Index: [54], [55], [56]	A score calculated based on the sensitivity and the visibility of public attributes.	Sensitivity score per item, visibility level per item.
Privacy score from social graphs: [52], [53]	A score calculated based on the risk level in terms of the friends attitude and the similarities with the users.	How much an attacker can reveal of relationships

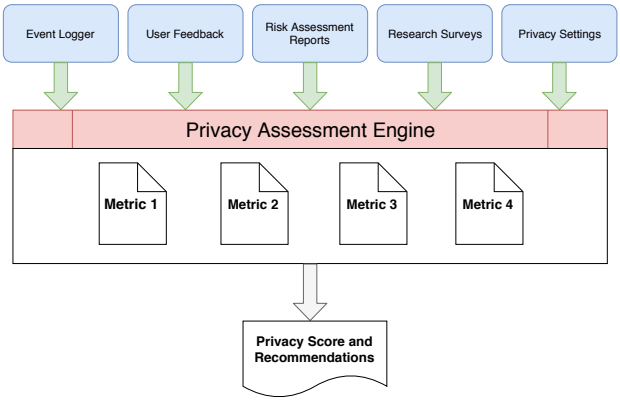

Figura 2. Privacy scoring process flow

The proposed framework, then, computes an overall privacy score based on the assessment of the impact of information security objectives (confidentiality, integrity, and availability) in addition to the privacy objectives as defined by the National Institute of Standards and Technology (NIST): predictability, manageability and disassociability [60]. Based on the obtained score, the framework offers suggestions and recommendations for effectively controlling the privacy and security of the system. The process of building the engine is summarized in *Fig.2*.

- **Step 3** determines whether the results of the proposed framework are accurate, clear, understandable and fully explained in case of uncertainty.
- **Step 4** is based on the results of step 3, it derives what can be changed and improved in the framework.

It is envisioned that, due to its generality, the framework will enable the analysis of privacy in MOSNs in more details. At the same time, it will empower the ability to measure the performance, the efficiency, and the effectiveness of the controls and settings provided in terms of privacy and security and to gauge how well the system under investigation is meeting the privacy and security objectives, thereby reducing the number of threats and attacks on MOSNs.

V. CONCLUSION

In this paper, we discussed two important and trending topics in microblogging online social networks: privacy challenges and issues and privacy measurements and evaluation. While users enjoy sharing interests and connecting with friends via online social media, a large amount of personal information becomes accessible to everyone. In addition, advanced data retrieval and analytic techniques have made it easier for attackers to collect and aggregate unlimited data and to target different types of attacks. This paper discussed also some privacy metrics to measure and quantify the privacy in social networks with the goal of evaluating the privacy choices in a system. Our study shows that all the proposed metrics are system-specific and there is a lack of a generic model. To answer this lack, we presented a high-level overview of a comprehensive framework to assess and evaluate the privacy of social media and compare different OSNs. As future work, we plan to implement and extend the proposed framework on different types of microblogging social networks.

ACKNOWLEDGMENTS

This work has been partially supported by the Spanish Ministry of Economy and Competitiveness (TRA2013-48180-C3-P, TRA2015-71883-REDT, TIN2014-57364-C2-2-R and TIN2015-70054-REDC), FEDER, and the Erasmus+ Program (2016-1-ES01-KA108‐02346).

REFERENCIAS

[1] "Privacy — Definition of privacy in English by Oxford Dictionaries", in *Oxford Dictionaries — English*, [Online]. Available: https://en.oxforddictionaries.com/definition/privacy.

[2] A.F. Westin: "Privacy And Freedom", in *25 Wash. & Lee L.*, Rev. 166, 1968.

[3] C. Bunnig, and C.H. Cap: .Ad Hoc Privacy Management in Ubiquitous Computing Environments", in *Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services*, 2009.

[4] Q. Ni, E. Bertino, J. Labo, C. Brodie, C.M. Karat, J. Karat, and A. Trombeta: "Privacy-Aware Role-Based Access Control", in *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, n.3, pp.24-31, 2010.

[5] S. Taheri, S. Hartung and D. Hogrefe: .Achieving Receiver Location Privacy in Mobile Ad Hoc Networks,in *2010 IEEE Second International Conference on Social Computing, Minneapolis, MN*, pp. 800-807, 2010.

[6] A. Java and X. Song and T. Finin, and B. Tseng: "Why We Twitter: Understanding Microblogging Usage And Communities", in *Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis - WebKDD/SNA-KDD 07*, pp. 56–65, 2007.

[7] Statista: "Twitter MAU worldwide 2017 — Statistic", in *Statista*, [Online]. Available: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

[8] Statista: "Tumblr: total number of blogs 2018 — Statistic", in *Statista*, [Online]. Available: https://www.statista.com/statistics/256235/total-cumulative-number-of-tumblr-blogs/.

[9] M. Broersma and T. Graham: "Twitter As News Source", in *Journalism Practice* , vol. 7, pp. 446-464, 2013.

[10] C. Chamberlain: "How Has Twitter Changed News Coverage?", in *News Bureau — Illinois, 22-Oct-2015*, [Online]. Available: https://news.illinois.edu/view/6367/267046.

[11] M. Das Sarma: “Tweeting 2016: How Social Media is Shaping the Presidential Election”, in *Inquiries Journal*, 2016. [Online]. Available: http://www.inquiriesjournal.com/a?id=1454.

[12] H. Kwak and C. Lee and H. Park, and S. Moon: “What Is Twitter, a Social Network or a News Media?”, in *Proceedings of the 19th international conference on World wide web - WWW 10*, pp. 591–600, 2010.

[13] T. Aichner and J. Frank: ”Measuring the Degree of Corporate Social Media Use”, in *International Journal of Market Research 57*, n. 2, pp. 257-276, 2015.

[14] “Raising Awareness About Over-Sharing”, in *Please Rob Me*. [Online]. Available: http://pleaserobme.com/.

[15] P. Gadkari: “How Does Twitter Make Money?”, in *BBC News*, 2013. [Online]. Available: http://www.bbc.com/news/business-24397472.w

[16] P. Greenfield: “The Cambridge Analytica Files: The Story so Far,” in *The Guardian*, 2018. [Online]. Available: https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far.

[17] E. Graham-Harrison and C. Cadwalladr: “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach,” in *The Guardian*, 2018. [Online]. Available: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[18] “Gpen Privacy Sweep 2017 Finds Ambiguity in Privacy Policies”, in *Office of Information and Data Protection Commissioner*, 2017. [Online]. Available: http://www.idp.al/2017/10/25/gpen-privacy-sweep-2017-finds-ambiguity-in-privacy-policies/?lang=en

[19] “Welcome to JoinDiaspora*”, in *diaspora* social network*. [Online]. Available: http://www.joindiaspora.com/.

[20] “Galaxy2”, in *Omeka RSS*. [Online]. Available: https://socialmediaalternatives.org/archive/collections/show/10.

[21] A. Srivastava and G. Geethakumari: “A Framework to Customize Privacy Settings of Online Social Network Users”, in *2013 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, pp. 187–192, 2013.

[22] P. Elkind: “Sony Pictures: Inside the Hack of the Century”, in *Fortune.com*, pp. 65–88, 2015.

[23] “Home Page of EU GDPR,” in *EU GDPR Portal*, 2018. [Online]. Available: https://www.eugdpr.org/eugdpr.org.html.

[24] C. Honeycutt and S.C. Herring: ”Beyond Microblogging: Conversation and Collaboration via Twitter”, in *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICSS-42)*, pp. 1–10, 2009.

[25] B.C. Fung and K. Wang and and P.S. Yu: “Anonymizing Classification Data for Privacy Preservation”, in *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, n. 5, pp. 711–725, 2007.

[26] Y.A.D. Montjoye and C.A. Hidalgo and M. Verleysen, and V.D. Blondel: “Unique in the Crowd: The Privacy Bounds of Human Mobility”, in *Scientific Reports*, vol. 3, n. 1, 2013.

[27] Y.A.D. Montjoye and L. Radaelli and V.K. Singh and A. Pentland: “Unique in The Shopping Mall: On The Reidentifiability of Credit Card Metadata”, in *Science*, vol. 347, n. 6221, pp. 536–539, 2015.

[28] G. Nalinipriya and M. Asswini: “A Survey On Vulnerable Attacks in Online Social Networks”, in *International Confernce on Innovation Information in Computing Technologies*, pp. 1–6, 2015.

[29] J. Russell: “Prominent Twitter Accounts Compromised After Third-Party App Twitter Counter Hacked”, in *TechCrunch*, 2017. [Online]. Available: https://techcrunch.com/2017/03/15/twitter-counter-hacked/.

[30] L. Bilge and T. Strufe and D. Balzarotti, and E. Kirda: “All Your Contacts Are Belong to Us: Automated Identity Theft Attacks On Social Networks”, in *Proceedings of the 18th international conference on World wide web - WWW 09*, pp. 551–560, 2009.

[31] G. Yan and G. Chen and S. Eidenbenz and N. Li: “Malware Propagation in Online Social Networks”, in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS 11*, pp. 196–206, 2011.

[32] I. Kayes and A. Iamnitchi: “Privacy and Security in Online Social Networks: A Survey”, in *Online Social Networks and Media*, vol. 3-4, pp. 1–21, 2017

[33] O. Goga and G. Venkatadri and K. Gummadi: “Exposing Impersonation Attacks in Online Social Networks”, in *ACM CONFERENCE ON ONLINE SOCIAL NETWORKS (COSN’14)*, 2014.

[34] D. Chandrasekaran and D. Costello and P. Stubbs: ”Social Media Profiling”, in *US Patent App. 13/465,335, issued November 7, 2013*, 2013.

[35] Electronic Privacy Information Center: “EPIC - Privacy and Consumer Profiling”, in *Electronic Privacy Information Center*. [Online]. Available: https://www.epic.org/privacy/profiling/.

[36] E. Zheleva and E. Terzi and L. Getoor: ”Privacy in Social Networks”, in *S.l.: Morgan & Claypool*, 2012.

[37] L.A. Cutillo and M. Manulis and T. Strufe: “Security and Privacy in Online Social Networks”, in *Handbook of Social Network Technologies and Applications*, pp. 497–522, 2010.

[38] C. Zhang and J. Sun and X. Zhu and Y. Fang: ”Privacy And Security for Online Social Networks: Challenges and Opportunities”, in *IEEE Network*, vol. 24, n. 4, pp. 13-18, 2010.

[39] U.U. Rehman and W.A. Khan and N.A. Saqib, and M. Kaleem: “On Detection and Prevention of Clickjacking Attack for OSNs” ,in *2013 11th International Conference on Frontiers of Information Technology*, pp. 160–165, 2013.

[40] C. Canali and M. Colajanni and R. Lancellotti: ”Data Acquisition in Social Networks: Issues And Proposals”, in *Proceedings of the International Workshop on Services and Open Sources (SOS’11)*, 2011.

[41] E. Chew and M. Swanson and K. Stine and N. Bartol and A. Brown and W. Robinson: “Performance Measurement Guide for Information Security”, in *National Institute of Standards and Technology (NIST)*, 2008. [Online].

[42] S.C. Payne: “SANS Institute – A Guide to Security Metrics - Research,” 2006.

[43] E.M. Maximilien and T. Grandison and T. Sun and D. Richardson and S. Guo, and K. Liu: ”Privacy-As-A-Service: Models, Algorithms, And Results On The Facebook Platform”, In *Proceedings of Web*, vol. 2, 2009.

[44] K. Liu and E. Terzi: “A Framework for Computing the Privacy Scores of Users in Online Social Networks”, in *2009 Ninth IEEE International Conference on Data Mining*, pp. 1–30, 2009.

[45] F.B. Baker and S.H Kim: İtem Response Theory: Parameter Estimation Techniques”, in *CRC Press*, 2004.

[46] A. Srivastava and G. Geethakumari: “Measuring Privacy Leaks In Online Social Networks”, in *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 2095–2100, 2013.

[47] G. Petkos and S. Papadopoulos and and Y. Kompatsiaris: “PScore: A Framework for Enhancing Privacy Awareness in Online Social Networks”, in *2015 10th International Conference on Availability, Reliability and Security*, pp. 592–600, 2015.

[48] R.G. Pensa and G.D. Blasi: “A Privacy Self-Assessment Framework for Online Social Networks”, in *Expert Systems with Applications*, vol. 86, pp. 18–31, 2017.

[49] J. Becker and H. Chen: ”Measuring Privacy Risk in Online Social Networks”, in *University of California, Davis*, 2009.

[50] T.H. Ngoc and I. Echizen and K. Komei and H. Yoshiura: “New Approach to Quantification of Privacy on Social Network Sites”, in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 556–564, 2010.

[51] N. Talukder and M. Ouzzani and A.K. Elmagarmid and H. Elmeleegy and M. Yakout: “Privometer: Privacy Protection in Social Networks”, in *2010 IEEE 26th International Conference on Data Engineering Workshops (ICDEW 2010)*, pp. 266–269, 2010.

[52] C. Akcora and B. Carminati and and E. Ferrari: “Privacy in Social Networks: How Risky Is Your Social Graph?”, in *2012 IEEE 28th International Conference on Data Engineering*, pp. 9–19, 2012.

[53] B.S. Vidyalakshmi and R.K. Wong and C.H. Chi: ”Privacy Scoring of Social Network Users as a Service”, in *2015 IEEE International Conference on Services Computing, New York, NY*, pp. 218-225. 2015.

[54] R.K. Nepali and Y. Wang: ”SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking”, in *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, Philadelphia, PA*, pp. 162-166, 2013.

[55] Y. Wang and R.K. Nepali: “Privacy Measurement for Social Network Actor Model”, in *2013 International Conference on Social Computing*, pp. 659–664, 2013.

[56] Y. Wang and R.K. Nepali and J. Nikolai: “Social Network Privacy Measurement and Simulation”, in *2014 International Conference on Computing, Networking and Communications (ICNC)*, pp. 802–806, 2014.

[57] B. Schneier: “A Taxonomy of Social Networking Data”, in *IEEE Security & Privacy*, vol. 8, n. 4, pp. 88-88, 2010.

[58] Wikipedia: ”PDCA”, in *https://en.wikipedia.org/wiki/PDCA*, 2018

[59] V.R. Basili: ”Software Modeling and Measurement: The Goal/Question/Metric Paradigm”, in *University of Maryland at College Park*, 1992.

[60] M. Garcia and N. Lefkovitz and S. Lightman: ”Privacy Risk Management for Federal Information Systems”, in *NIST Internal Report (NISTIR) 8062*, 2017.