# PriMe: A Novel Privacy Measuring Framework for Online Social Networks

Ahmad Hassanpour
*Department of Information Security and Communication Technology*
*Norwegian University of Science and Technology (NTNU)*
Gjovik, Norway
Ahmad.Hassanpour@ntnu.no

Bian Yang
*Department of Information Security and Communication Technology*
*Norwegian University of Science and Technology (NTNU)*
Gjovik, Norway
Bian.Yang@ntnu.no

***Abstract*—Online Social Networks are responsible for disclosing a large amount of sensitive information. Users unintentionally reveal their sensitive information and are unaware of the privacy risks involved. But the users should be well informed about their privacy quotient and should know where they stand on the privacy measuring scale. In this paper, we proposed an adaptive privacy measuring framework called PriMe that can measure the privacy leakage score for each action of a user in an OSN and subsequently adjust the privacy settings based on the preferred privacy scopes and boundaries. Various types of data, actions, and personal characteristics of each user have been considered to ensure the calculated privacy leakage score is accurate.**

***Keywords— Online social network, privacy leakage, measuring privacy.***

## I. INTRODUCTION

The ubiquity of information communication technologies which is leading to present-day digital society has changed the basic principles of human interaction. Although privacy, as one of these principles, has been noted for several decades ago [1], it is attracted a lot of attention in recent years. Online social networks (OSNs) (e.g., Facebook, LinkedIn, MySpace), as a particular type of virtual community, attempt to provide helpful functionalities including maintaining/increasing social relationships [2], finding users with similar interests, improving our knowledge [3], and financial benefits, the published data in such environments can violate various aspects of users' privacy [4]. In fact, users are virtually interacting continuously, and disclose various levels of private information about themselves or others unconsciously [5]. Therefore, OSNs are one of the main bridges of revealing personal information by allowing users to upload their footprints (e.g., text, images, and videos) and interact with others in a variety of ways. Moreover, by raising the number of users of an OSN which lead to more dissemination of information, as well as sharing different varieties of information within many OSNs, users' privacy concerns may increase. Additionally, the recent approval of the GDPR (General Data Protection Regulation) compels OSN service providers to provide more data protection settings and offer further control to OSN users over their personal data. In the following, some challenging problems which users and OSN providers are facing due to preserving the privacy of users have been discussed.

First, privacy is a multi-dimensional concept especially when it is under investigation in the OSNs context. Inspiring by Burgoon et al. [6], Zhang et al. [7] proposed a four-dimensional privacy concept including *virtual territory privacy*, *factual privacy*, *interactional privacy*, and *psychological privacy*. **C1)** *virtual territory privacy:* differing from physical privacy which is defined as the freedom from surveillance and unwanted intrusions upon one's space by the physical presence, touch, sights, sounds, or odors of others, in the virtual social context, there are no physical boundaries that help define the private territory. However, people still feel ownership of the digital belongings that they are entitled to or that are created by them (for example, web-logs, personal spaces, profile pages, etc.). **C2)** *factual privacy:* refers to the ability to control identifiable personal information about oneself. **C3)** *interactional privacy:* individuals may feel compelled by or uncomfortable under some circumstances relating to social interaction. For example, conversation requests may be initiated obtrusively or at inappropriate times. **C4)** *psychological privacy*: people need the freedom to express their own views and the capability to hide themselves from norms that they do not agree with. Psychological privacy protects the individual from intrusions upon one's thoughts, feelings, and values.

Second, each user usually has a scope in his/her mind before publishing any data on OSNs, and privacy requires keeping the published information in its predesignate scope. The work [8] defined the scope as **S1)** *breadth* (the distribution of audience), **S2)** *depth* (the degree of allowed usage), and **S3)** *lifetime* (the long life of the published data). When a piece of information is moved beyond its predesignate scope in any of these dimensions (accidentally or maliciously), a privacy breach occurs. Therefore, a breach may occur when information is shared with a party for whom it was not intended (disclosure), when information is abused for a different purpose than was intended, or when information is accessed after its intended lifetime. Aside from the scope, users in OSNs are contending with privacy three boundaries [9] including **B1)** *disclosure* (users try to handle

IEEE/ACM ASONAM 2022, November 10-13, 2022
978-1-6654-5661-6/22/$31.00 © 

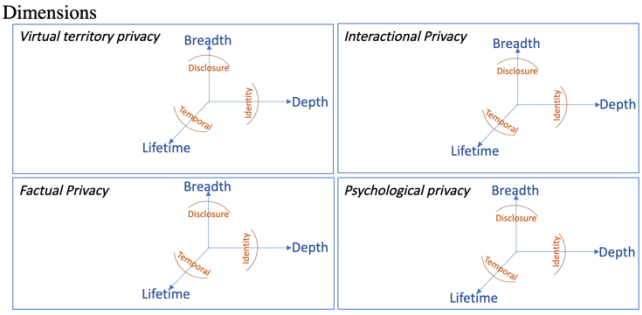


Fig1. The relation between privacy dimensions, scopes, and boundaries has been presented. Each dimension has its own scopes (i.e., breadth, depth, and lifetime), and each scope has its own boundaries (i.e., disclosure, identity, temporal).

the anxiety of disclosing their information in a public or private manner) **B2)** *identity* (the identity boundary is described as the ability to manage one's information with particular groups. For example, it shows users' behaviors in different situations: one at work and the other at a party) **B3)** *temporal* (it shows how the conduct of individuals may differ over time). Privacy has various dimensions, and users try to consider different scopes and have their own boundaries. Our notion of the relation between the dimensions, scopes, and boundaries has been presented in Fig.1 Each dimension has its corresponding scopes, and each user has a different boundary for each scope.

Finally, to perfectly utilize the provided functionalities of an OSN, users need to publish more information, thus, there is a tradeoff between optimal use of functionalities and user privacy. Moreover, another issue called the privacy paradox has been observed in users' online behavior [10][11]. Recent research has revealed discrepancies between user attitude and their actual behavior. More specifically, while users claim to be very concerned about their privacy, they nevertheless undertake very little to protect their personal data.

Considering all dimensions of privacy and users' scopes to preserve the privacy of users in OSNs is extremely challenging. As a solution, OSNs provide policies and privacy settings to control and adjust who can access users' profiles and posts [12], [13]. However, the privacy policies offered by the system are confusing and expressed in legal jargon that is difficult to understand. Furthermore, privacy settings are complex, time-consuming, and still insufficient to fully protect users' privacy [14]. Besides, OSN providers mostly store, process, analyze users' data, and sometimes sell them to third-parties for advertising and marketing purposes. Moreover, to prevent privacy breaches in OSNs, privacy has been investigated from various perspectives (i.e., social, legal, and technical ) among researchers.

One of the effective solutions for preserving the privacy of OSNs' users is measuring the privacy leakage for each piece of published data. By doing this, users will be noticed the portion of privacy that might be violated. Considering the intended scope of users and more technically, extracting risks from published data such as comments and posts to calculate the privacy score is a demanding task. Interestingly, publishing some information that is risk-free for many users can be detrimental to others such as a criticism against religion or government since in some countries such criticisms are acceptable, while in other countries, will lead to difficulties. Different authors have proposed various techniques and methods from the algorithmic approach to statistical ones to score and measure privacy. The main two approaches for measuring privacy are statistical or machine learning (ML)-based. For each approach, several models have been proposed to measure the privacy of users in OSNs. The most well-known methods related to these approaches have been discussed in the related work section.

In this paper, we proposed PriMe which is an adaptive privacy measuring framework that can measure the privacy leakage score (PLS) for each action of a user in an OSN and adjust the privacy setting of each user based on the preferred privacy scopes and boundaries. Various types of data, actions, and personal characteristics of each user have been considered to ensure the calculated PLS is accurate. Moreover, we discussed why the previous methods for calculating PLS are not precise and proposed a new method.

## II. Related Works

From the technical point of view, the statistical-based methods mostly rely on two intuitive properties (i) the *sensitivity* of the information being revealed and (ii) the *visibility* of the revealed information within the network. The proposed methods are working on Dichotomous or Polytomous variables or a combination of them. On the other hand, ML-based models mostly try to measure the privacy of unstructured data (text, photo, etc.). In the following, we briefly review the proposed methods for both approaches.

### A. Statistical-based Approaches

Notably, A dichotomous variable takes only one of two possible values when observed or measured. The value is most often a representation of a measured variable (e.g., age: under 65/65 and over) or an attribute (e.g., gender: male/female). A variable having more than two possible categories, either ordered or unordered called polytomous variable. For example, college matriculation could be described as a polychotomous variable: freshman, sophomore, junior, or senior. Table I summarizes several statistical-based methods for measuring privacy score the type of data (dichotomous, polytomous variables, or their combination), the proposed formulation, and a short description has been extracted for each paper. Most proposed methods, consider privacy score as a combination of the partial privacy scores of each one of his profile items (e.g., email, relationship status, mobile phone number). The contribution of each profile item in the total score depends on the sensitivity of the item and the visibility it gets due to the user's privacy settings.

one of the first attempts to design a privacy metric for online social networks was proposed by Maximilian et al. [15] in 2009. The authors have proposed a framework to calculate the privacy score based on the sensitivity $\beta_i$ and the visibility $v(i,j)$ of profile items $i \in \{1,\dots,n\}$ of user $j$ in a social network.

$$PR(i) = \sum_i PR(i,j) = \sum_i \beta_i \times v(i,j)$$

Several other papers, listed in Table I, proposed other methods for measuring PLSs based on the same components (i.e., sensitivity and visibility). In the following, we will review the definition of these components and how they have been used.

TABLE I. SUMMARIZE OF VARIOUS PRIVACY SCORING SOLUTIONS BASED ON STATISTICAL-BASED APPROACHES

| Author and year | Approach/Data Type | Data Source | Proposed formulation | Description |
|---|---|---|---|---|
| Renner (2010) [16] | Dichotomous | Facebook | Risk = Negative consequence × Likelihood | defining privacy risk by considering two privacy metrics including negative consequence information leakage and the likelihood of information leakage. |
| Maximilien et al. (2009) [15] | Dichotomous | - | $PR(k,l) = \beta_k \times v(k,l)$ $\beta_k = \frac{(M-\lvert R_k \rvert)}{M}$ | $PR(k,l)$ shows privacy score. $\beta_k$ shows the sensitivity of $k$-th attribute, $v(k,l)$ shows the visibility of attribute $k$ of user $l$, $\lvert R_k \rvert$ is the number of individuals that make their attributes publicly available, $M$ is number of users. |
| Maximilien et al. (2009) [17] | Dichotomous | - | $PR(k,l) = \beta_k \times v(k,l)$ $\beta_k = \frac{(M-\lvert R_k \rvert)}{M}$ | $PR(k,l)$ shows privacy score. $\beta_k$ shows the sensitivity of $k$-th attribute, $v(k,l)$ shows the visibility of attribute $k$ of user $l$, $\lvert R_k \rvert$ is the number of individuals that make their attributes publicly available, $M$ is number of users. |
| Srivastava and Geethakumari (2013) [18] | Dichotomous/Unstructured | private dataset | $PQ(j) = \sum_k \beta_k \times v(k,l)$ $v(k,l) = \frac{\lvert R_k \rvert}{M} \times \frac{\lvert R_l \rvert}{M}$ $\beta_k = \frac{(M - \lvert R_k \rvert)}{M}$ | $PQ(j)$ is final privacy score. $\beta_k$ shows the sensitivity of $k$-th attribute. $v(k,l)$ shows the visibility of attribute $k$ of user $l$, $\lvert R_k \rvert$ is the number of individuals that make their attributes publicly available, $M$ is number of users. |
| Domingo-Ferrer (2010) [19] | Dichotomous/Structured | Simulation-based experiments | $PRF = \frac{\sum_{j'=1,j'\neq j}^{N} \sum_{i=1}^{n} \sum_{k=1}^{l} \beta_{ik} V(i,j',k) I(j,j',k)}{1 + \sum_{i=1}^{n} \sum_{k=1}^{l} \beta_{ik} V(i,j',k)}$ | Where $j$ and $j'$ are the two users in the social networks, $k$ indicates the number of links between users and n indicates the number of attributes for a user. I(j, j′, k) = 1 1 If $j'$ and $j$ are $k$ links away from each other, otherwise 0. |
| Nepali and Wang (2013) [20][21] | - | - | $PIDX = \frac{\sum_{k=1}^{m} p'_k s'_k}{\sum_{k=1}^{n} s_k} \times 100$ | $p'_k$ shows the visibility of each attribute, and $s'_k$ shows the corresponding weight.$n$ indicates the number of attributes, and $m$ shows a subset of them which belongs to $k$-th user. |
| Talukder et al. (2010) [22] | Dichotomous/Structured | - | $S_\gamma^i = \sum_{k=0}^{q} \omega^{(k)} \psi_i^{(k)} \tilde{\psi}^{(k)}$ | $\omega^{(k)}$ is the relative sensitivity vector for attributes, Privometer records the success and failure of the inferred attributes as a vector, called attribute matching vector, $\tilde{\psi}$. We also represent $\psi_i^{(k)}$ as matching vector that records the matches between two attributes. |
| Petkos et al. 2015 [23] | Dichotomous | - | $PQ(j) = \sum_k \beta_k \times v(k,l)$ | $PQ(j)$ is final privacy score. $\beta_k$ shows the sensitivity of $k$-th attribute. $v(k,l)$ shows the visibility of attribute $k$ of user $l$. |
| Liu and Terzi (2010) [24] | Polytomous/Structured | Synthetic and private dataset | $P_{ij} = \frac{1}{1 + e^{-\alpha_i(\theta_j - \beta_i)}}$ | $\beta_i$ shows the sensitivity of attribute $i$. $\alpha_i$ quantifies the discrimination power.3 |
| Becker and Chen (2009) [25] | Polytomous | Facebook | Privacy measured based on inference detection | Try to infer attributes of each user. |
| Aghasian et al. (2017) [26] | Polytomous/Structured | Facebook, ResearchGate, LinkedIn, and Google+ | Privacy = $\frac{\sum_{i=1}^{m} \beta_i \times F_{vis}(xi)}{m}$ | $\beta_i$ shows the sensitivity of attribute $i$. $F_{vis}(xi)$ indicates the visibility score for each attribute calculated by fuzzy rules. |
| Pensa and Di Blasi (2017) [27] | Polytomous/Structured | Facebook | Privacy measured based on sensitivity and visibility | measure the privacy risk of the users and help the users customize semi-automatically their privacy settings |

*Sensitivity*: Specifying the sensitivity of data is a challenging task since sensitive data can be a number of things. One of the easiest ways to evaluate is to think of personal data you would not want to be openly shared with just anyone. There are, of course, federal laws and regulations that set specific guidelines on what types of sensitive data must be protected, like financial information (e.g., Credit card numbers, bank account information, and social security numbers), government information (e.g., any document that is classified as secret or top-secret, restricted, or can be considered a breach of confidentiality), business information (e.g., accounting data, trade secrets, financial statements or accounts, and any sensitive information in business plans), personal information (e.g., addresses, medical history, driver's license numbers, or phone numbers). However, GDPR makes a clear distinction between sensitive and non-sensitive personal data. Article 9 of GDPR establishes special categories that require extra attention. Sensitive data, or special category data, according to GDPR is any data that reveals a subject's information including racial or ethnic origin, political beliefs, religious beliefs, genetic or biometric data, mental health or sexual health, sexual orientation, and trade union membership. Besides having various types of sensitive data, the level of sensitivity of each data type can be different for each user. For example, politicians publish their political opinions on OSNs without having any concerns.

TABLE II. SUMMARIZE OF VARIOUS PRIVACY SCORING SOLUTIONS BASED ON MACHINE LEARNING-BASED APPROACHES

| Author and year | Approach/Data Type | Data Source | Machine learning Algorithm | Description |
|---|---|---|---|---|
| Li et al., (2020) [28] | Structured | Collect data from Sina Weibo | Deep neural network | Calculating privacy score by extracting profile information and graph structure information of users' friends. |
| Aghasian et al., (2020) [29] | Structured and unstructured (text) | Collect data from Facebook and Twitter | Fuzzy-based model | measure and warn users regarding the textual data privacy risks they have shared in online social platforms. |
| Aghasian et al., (2017) [30] | Structured | Collect data from Facebook, ResearchGate, LinkedIn, and Google+. | Statistical and fuzzy systems | specify the potential information loss for a user by using obtained privacy disclosure score |
| Yu et al., (2018) [31] | Unstructured (image) | public image sets, PicAlert and Mirflickr | Deep neural network | recommending fine-grained privacy settings for social image sharing by considering content sensitiveness of the images and trustworthiness of the users |
| Orekondy et al., (2017) [32] | Unstructured (image) | Visual Privacy (VISPR) dataset | Deep neural network | predict user specific privacy score from images in order to enforce the users' privacy preferences |
| Orekondy et al., (2018) [33] | Unstructured (image) | Visual Privacy (VISPR) dataset | Deep neural network | obfuscating the image regions related to the private information which leads to privacy while retaining utility of the images |
| Battaglia et al., (2020) [34] | Unstructured (text) | Collect data from social media | k-NN, decision tree (DT), Multi-layer Perceptron (MLP), SVM, Random Forest (RF), and Gradient Boosted trees (GBT) | Assign a score to any text sample according to its degree of sensitivity |

Shortly, sensitive data is information most people would not want to share with others who don't have approval, and sensitivity shows the risk associated with the attributes of the user. when the sensitivity of an attribute increases, the risk posed by information disclosure of the individuals also increases. If $|R_k|$ shows the number of individuals that make their attributes publicly available, $M$ is number of users, [15] calculates the sensitivity of $k$-th item by $\beta_k = \frac{(M-|R_k|)}{M}$.

*Visibility:* The probability of leakage of private information of a user also depends on the position of the user in network topology. If the user himself is directly or indirectly connected to a large set of nodes in the network, then the chances of information leakage through his neighbors increase. For example, if a user considers his birth date as a piece of private information and shares only with his friends, it is highly likely that any one of his friends may share such information further with his friends, thereby causing an information leakage. The probability of this leakage will primarily depend on the number of users in his vicinity in one or more hops. Therefore, the probability of leakage increases with the visibility of the user himself (i.e., the number of users who would be interested in the information of the user) as well as the visibility of his/her friends.

Assuming independence between items and users, we can compute $P_{i,j}$ to be the product of the probability of a 1 in the $i$-th row of $R$ (i.e.,$\frac{|R_i|}{N}$) and the probability of a 1 in the $j$-th column of $R$ (i.e., $\frac{|R_j|}{n}$ ). That is, if $|R_j|$ is the number of items for which $j$ sets $R(i,j)$=1, we have $v(i,j)$= ($\frac{|R_i|}{N}$)*( $\frac{|R_j|}{n}$) . this notion does not measure the visibility for a specific item very accurately. Consider two users $i$ and $k$ in an OSN with 10 users, and a specific item $j$. Assume user $i$ revealed 3 items out 10 items that existed in the OSN, and user $k$ revealed 6 items, both revealed item $j$. Also assume the probability of revealing item $j$ is 0.7 (i.e., $\frac{|R_j|}{n}$=*0.7* ). Therefore, the visibility score for user $j$ and item $j$ is $v(i,j)$= 0.3*0.7=0.21 and for the user $k$ is $v(i,j)$=0.6*0.7=0.42. The problem here is that the more a user discloses its information, the more visibility score will be charged for each disclosed item. Moreover, here, the visibility of an item is calculated without considering the users' network. Therefore, if user $i$ and $k$ have the same network (friends), their visibility scores for the same item ($j$) is not equal because one of them revealed more information.

*Discussion on statistical-based approaches*: The proposed statistical-based methods are using traditional privacy metrics to obtain quantitative statistics on all the aspects that affect users' privacy disclosure, including but not limited to attribute information, network environment information, trust between users, and publishing information content. However, these approaches face two problems. First, these approaches are inefficient. Most of these approaches first extract features, then measure them separately, and finally integrate them into a numerical value. In addition, the calculation method also faces various doubts because privacy is a virtual concept without a unifying principle, and any calculation is considered to be subjective and unconvincing. Second, this method relies too strongly on artificial feature extraction. In previous research on privacy metrics, feature extraction is a difficulty. Which features can be used for privacy measurement? Which features are more important to measure privacy leakage more accurately? What associations exist between these features? These problems urgently need to be solved. Meanwhile, when considering the network environment of users, there may be tens of millions of links around a user. Previous methods obtained only one user's privacy score after analyzing the whole network, which is undoubtedly inefficient and inaccurate [35].

### B. Machine Learning-based Approaches

Apart from statistical-based approaches, ML-based models have been recently used to measure privacy leakage in unstructured data (text, photo, etc.). Some works like [38] can be used to warn the users when part of their biometric data is not hidden, however, ML-based methods can be used to infer the hidden patterns which can assist to disclose the privacy of

users. To do this, these approaches try to extract informative private features from

TABLE III. THE PROPOSED PRIVACY LEAKAGE METRICS FOR EACH DATA TYPE

| Data type | Proposed Metrics |
|---|---|
| user network | Number of friends, Measuring trust for each friend |
| structured / unstructured data | If the data include sensitive information, types of sensitive information (e.g., biometric, religion, political view), transparency of provided data, uniqueness. |
| action | if the action include sensitive information (e.g., post a content, like a post), lifetime of action. |

unstructured data. Table II presents some methods which used ML methods like deep learning to measure privacy leakage.

## III. PROPOSED PRIVACY ADAPTIVE METER FRAMEWORK

Fig. 2 shows our proposed adapted privacy meter framework called PriMe including five main modules called *User Data*, *Personal Attribute Analyzer*, *Privacy Leakage Metrics*, *Privacy Meter*, and *Adaptive Privacy Awareness*. By considering various data types, actions, and privacy preferences, this framework allows to design and implement an adaptive privacy meter such that different dimensions, scopes, and boundaries of privacy will be measured and adapted for each user separately. Moreover, the framework is highly flexible due to our modular design, thus, some proposed modules can be changed depending on the OSN's requirements.

Moreover, we proposed a different way of measuring PLS comprising three main parameters called sensitivity, linkability, and visibility, leading to a more accurate PLS.

### A. Users Data

OSNs' Users generate and provide various types of data including their actions (e.g., like, reshare, add/remove/block to their friendship list), unstructured data (e.g., images, texts, videos), structured data (e.g., birth date, marital status, hometown), and user network (e.g., name of current friends, blocked friends). Undoubtedly, each of this information discloses the privacy of the user to a different degree. For instance, sharing a personal video clip that includes our biometric information (e.g., our face image) reveals more sensitive data compared to liking our friends' post that includes his face image. Therefore, to have a comprehensive privacy meter framework, all provided data types by users should be considered during the calculation.

### B. Privacy Leakage Metrics

For each type of data, some metrics are calculated to assist the *privacy meter* module in measuring the PLS more accurately. These metrics extract some characteristics from the raw data or analyzed data. Table III shows some of our proposed metrics for different data types.

### C. Content Analyzer

Measuring the sensitivity of published unstructured data is a highly challenging task. For instance, a political view can be revealed by a short text, an image, or posting a protesting clip by the user. To detect the revealed political view in each of these modalities, different types of AI algorithms are required (e.g., usually natural language processing algorithms are being used for analyzing texts, and computer vision algorithms for analyzing images and videos). Thus, the *content analyzer* should include several AI models which can detect various types of sensitive content in different unstructured data.

### D. Personal Attribute Analyzer

*Personal attribute analyzer* has the responsibility of extracting static (e.g., big five traits) and dynamic (e.g., emotions) personal attributes from the shared data. These features assist us to measure privacy leakage more accurately. For example, if a user posts, likes, or shares more compared to other users, the value of the extravert attribute can increase for that user, and consequently, he is leaking his privacy. Moreover, measuring these attributes help us to develop an adaptive privacy measuring framework.

### E. Privacy Meter

*Privacy meter* is the main module of this framework which has the responsibility of calculating PLS based on the received raw data, *personal attribute analyzer*, *content analyzer*, and the calculated metrics by *privacy leakage metrics* module. It should continuously measure the PLS for each taking or withdrawing action. The main four submodules of *privacy meter* are the *sensitivity calculator*, *visibility calculator*, *linkage calculator*, and *privacy leakage score calculator*. Therefore, the privacy leakage score will be a function of three inputs $PR = F$ (*sensitivity*, *linkage*, *visibility*). The function $F$ should be implemented in the *privacy leakage score calculator*, and each of the three parameters has its own block, explained in the following subsections.

*Sensitivity Calculator:* previous methods calculated the sensitivity based on the behaviors of users of a specific OSN which means the more users reveal a piece of information, the less sensitive score is considered for it. But article 9 of GDPR defined the categories of sensitive information, explained in section II (A). Therefore, if the content analyzer detects the seven categories of sensitive data (racial or ethnic origin, political beliefs, religious beliefs, etc.), a high sensitivity score will be assigned for that piece of information. Other information will be categorized into semi-sensitive and non-sensitive data. The semi-sensitive data refers to those data that some users may have concerns about revealing them like home address, phone number, working organization, or even some actions such as liking a post. Semi-sensitive and non-sensitive can be adaptively categorized for each user separately which will be done in the *adaptive privacy awareness* module, described in the next section.

The sensitivity calculator receives the required information from the *content analyzer*, *privacy leakage metrics*, or even *user data* modules. Therefore, based on the received information, the type of sensitivity (sensitive, semi-sensitive, non-sensitive) will be measured and converted to a score.

*Visibility Calculator:* the proposed methods by previous works for calculating the visibility of a specific item are

dependent on the visibility of other items shared by the user. Obviously, the more users can see a specific item, the more

$$PR = F(sensitivity, linkage, visibility) = sensitivity * linkage * visibility$$

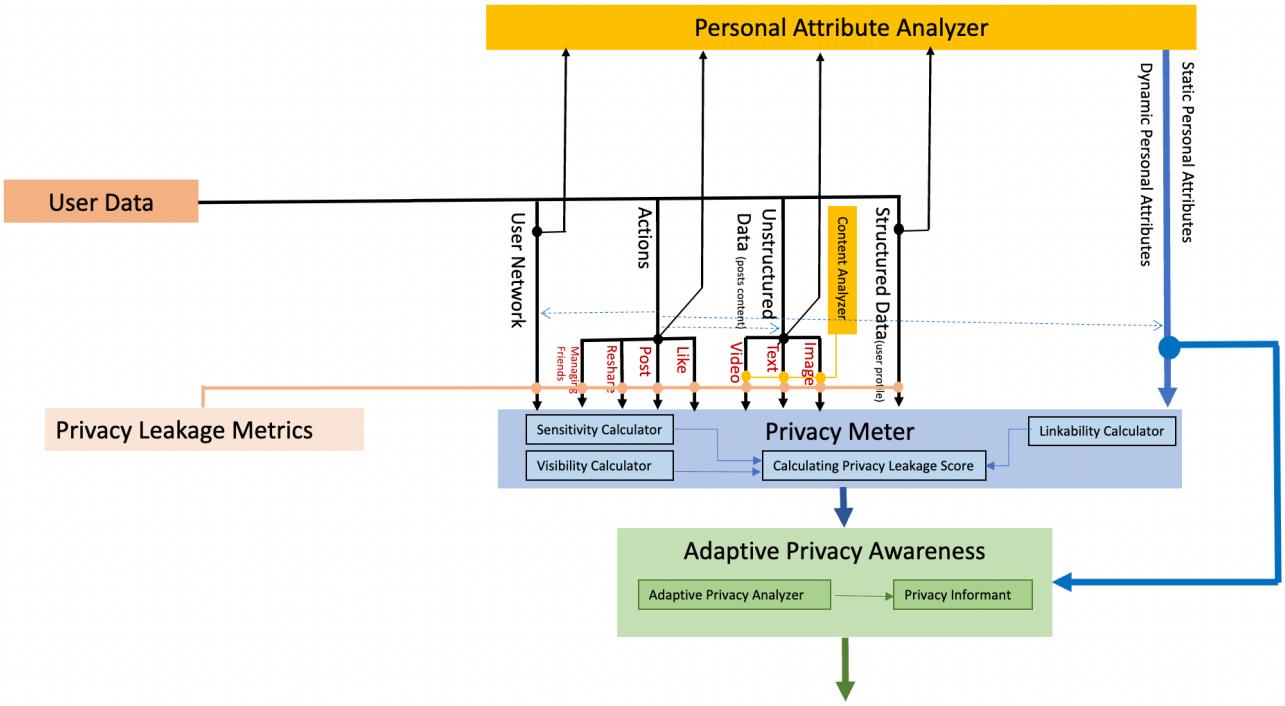


Fig. 2: Overview of proposed privacy measuring (PriMe) framework including five modules called *user data*, *privacy leakage metrics*, *personal attribute analyzer*, *privacy meter*, and *adaptive privacy awareness*.

visibility score should be considered for it. For those users who do not have a small number of friends, the visibility of a published item should not be high even if he/she is published many other personal items/data. Moreover, a trustworthiness score should be considered for each user who existed in the network. Undoubtedly, the visibility score will decrease if the users in the network receive a high trustworthiness score since the revealed data will not share with other users in the network.

The visibility of an OSN should be considered as another factor for measuring the visibility of each published item. Some OSNs are open to search engines, thus, all users on the Internet can search for the content of the published information in a specific OSN. Besides, in some OSNs like LinkedIn some actions (e.g., like, share) lead to users who are not in our connections being able to see our published posts, resulting in more visibility of data.

*Linkage Calculator*: The linkability between two posts or a post and action can disclose more privacy and thus increase the PLS. For instance, user's political view can be revealed after liking several posts of a specific party. Therefore, the linkability between the provided information and actions should be considered during calculating the PLS (the dashed blue lines in Fig. 2). Generally, for each portion of data *d*, the dependency and linkage with other portions that existed in the whole internet should be calculated, $d \perp\!\!\!\perp \mathbf{I}$, where $\mathbf{I}$ demonstrates the set of all data on the internet and $\perp\!\!\!\perp$ shows the linkability.

*Privacy Leakage Score Calculator*: After calculating the three main parameters, the PLS can be measured by simply multiplying the three parameters:

Since the PLS should be measured continuously, thus, continual ML-based methods that preserved the privacy of users should be utilized [36][37].

### F. Adaptive Privacy Awareness

Discrepancies between users' attitude and their actual behavior, and having different tastes and priorities for revealing information force a privacy framework to be adaptive. For instance, revealing biometric information is not important for some people while they do not like their political views to be disclosed. Therefore, to have an adaptive privacy informant, some personal characteristics of each user are required.

*Adaptive Privacy Analyzer:* After calculating the PLS by *privacy meter* for each action of a user, each reaction of the user will be monitored by this module. This assists to find a relation between the user's personality and his privacy preferences. By doing this, the preferred scopes and boundaries of a user can be fulfilled and measured continuously.

*Privacy Informant:* this module can inform the user about any privacy leakage after each action or adjust the privacy settings automatically.

### G. Discussion

The characteristics of the proposed framework (i.e., considering all data types, analyzing the personal attributes of each user, measuring the PLS, and more importantly an adaptive privacy setting) lead to cover all aspects of privacy including dimensions, scopes, and boundaries. Regarding dimensions (i.e., **C1-C4**), using PriMe users can specify their own virtual territory, the identifiable information and

psychological attributes of each user will be detected, and privacy settings will be adjusted such that it complies with the *interactional privacy.* In regard to the scopes (i.e., **S1**-**S3**), users can utilize the provided metrics (by *privacy leakage metrics*) for their published data (i.e., network, actions, and data), and decide about breadth, depth, and the lifetime of data. The adaptivity of the proposed framework allows for fulfilling all boundaries and thus, each user can choose its own identity, temporal, and disclosure.

Calculating the sensitivity, linkability, and visibility for each piece of data is not a trivial task, mostly because of two reasons. First, when the data is unstructured, extracting sensitive features should be done by some ML algorithms e.g., deep learning models, which need a large amount of training data. Moreover, the selected ML algorithm should be trained on each sensitive category separately, which might be different for each user. Second, calculating linkability between a large number of actions on an OSN such that the detected linkability leads to an increase or decrease of PLS is a difficult task.

## IV. Conclusion

In this paper, we proposed an adaptive privacy framework that can measure a score for each action of a user including posting, liking, adding someone to the network, etc. The proposed framework includes five main modules including *User Data*, *Personal Attribute Analyzer*, *Privacy Leakage Metrics*, *Privacy Meter*, and *Correlation Analyzer*. Moreover, we proposed a more accurate method for measuring PLS which comprises three parameters called sensitivity, linkage, and visibility. In future works, we will further elaborate on the PriMe's modules and provide practical solutions for calculating PLS with more details.

## Acknowledgment

This work was supported by the Project Privacy Matters (PRIMA) under Grant H2020-MSCA-ITN-2019-860315.

## References

[1] R. Gavison, "Privacy and the Limits of Law," The Yale law journal, 89(3), pp.421-471, 1980.
[2] X. Zhao, J. Yuan, G. Li, X. Chen, and Z. Li, "Relationship strength estimation for online social networks with the study on Facebook," Neurocomputing, 95, pp.89-97, 2012.
[3] M. Pavlovic, N. Vugdelija, and R. Kojic, "The use of social networks for elearning improvement," Hellenic Journal of Music, Education and Culture, 6(1), 2015.
[4] N. Kökciyan, and P. Yolum, "Priguard: A semantic approach to detect privacy violations in online social networks," IEEE Transactions on Knowledge and Data Engineering, 28(10), pp.2724-2737, 2016.
[5] J. Chen, J. He, L. Cai, and J. Pan, "Disclose more and risk less: Privacy preserving online social network data sharing," IEEE Transactions on Dependable and Secure Computing, 17(6), pp.1173-1187, 2018.
[6] J. K. Burgoon, "Privacy and Communication," In Communication Yearbook 6, M. Burgoon (ed.), Beverly Hills, CA: Sage, 1982.
[7] N. Zhang, C. Wang, and Y. Xu, "Privacy in online social networks," 2011.
[8] M. Beye, A.J. Jeckmans, Z. Erkin, P. Hartel, R.L. Lagendijk, and Q. Tang, "Privacy in online social networks," In Computational Social Networks, pp. 87-113,. Springer, 2012.
[9] L. Palen, and P. Dourish, "Unpacking privacy for a networked world," In Proceedings of the SIGCHI conference on Human factors in computing systems, 2003, pp. 129-136.
[10] S. Barth, and M.D. De Jong, "The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review," Telematics and informatics, 34(7), pp.1038-1058, 2017.
[11] D.J. Solove, "The myth of the privacy paradox," Geo. Wash. L. Rev., 89, p.1, 2021.
[12] Y. Liu, K.P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, 2011, pp. 61-70.
[13] S.j. De, and A. Imine, "Choosing the Right Privacy Settings," In Privacy Risk Analysis of Online Social Networks, pp. 59-67, 2021.
[14] F.D. Stutzman, R. Gross, and A. Acquisti, "Silent listeners: The evolution of privacy and disclosure on Facebook," Journal of privacy and confidentiality 4, no. 2, 2013.
[15] E.M. Maximilien, T. Grandison, T. Sun, T., D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the facebook platform," In Proceedings of Web (Vol. 2), 2009.
[16] C. Renner, "Privacy in Online Social Networks," Thesis, 2010.
[17] E. M. Maximilien, T. Grandison, K. Liu, T. Sun, D. Richardson, and S. Guo, "Enabling privacy as a fundamental construct for social networks," In 2009 International Conference on Computational Science and Engineering, vol. 4, pp. 1015-1020. IEEE, 2009.
[18] A. Srivastava, G. Geethakumari, "Measuring privacy leaks in online social networks," In advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on, p. 2095–2100, 2013.
[19] J. Domingo-Ferrer, "Rational privacy disclosure in social networks," In International Conference on Modeling Decisions for Artificial Intelligence, 2010. p. 255–265.
[20] 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, 2013, pp. 162-166.
[21] Y. Wang, R.K. Nepali, and J. Nikolai, "Social network privacy measurement and simulation," In 2014 International Conference on Computing, Networking and Communications (ICNC), 2014, pp. 802-806.
[22] N. Talukder, M. Ouzzani, A.K. Elmagarmid, H. Elmeleegy, and M. Yakout, "Privometer: Privacy protection in social networks," In: Data Engineering Workshops (ICDEW), 2010 IEEE 26th International Conference on, 2010, p. 266–269.
[23] G. Petkos, S. Papadopoulos, and Y. Kompatsiaris, "PScore: A Framework for Enhancing Privacy Awareness in Online Social Networks," In: Availability, Reliability and Security (ARES), 10th International Conference on, 2015, p. 592–600.
[24] K. Liu, and E. Terzi, "A framework for computing the privacy scores of users in online social networks," ACM Transactions on Knowledge Discovery from Data (TKDD), 5(1), pp.1-30, 2010.
[25] J.L. Becker, "Measuring privacy risk in online social networks," University of California, 2009.
[26] E. Aghasian, S. Garg, L Gao, S. Yu, and J. Montgomery, "Scoring users' privacy disclosure across multiple online social networks," IEEE access, 5, pp.13118-13130, 2017.
[27] R.G. Pensa, and G. Di Blasi, "A privacy self-assessment framework for online social networks," Expert Systems with Applications, 86, pp.18-31, 2017.
[28] X. Li, Y. Xin, C. Zhao, Y. Yang, and Y. Chen, "Graph convolutional networks for privacy metrics in online social networks," Applied Sciences, 10(4), p.1327, 2020.
[29] E. Aghasian, S. Garg, and J. Montgomery, "An automated model to score the privacy of unstructured information—Social media case," Computers & Security, 92, p.101778, 2020.
[30] E. Aghasian, G. Saurabh and J. Montgomery, "A privacy-enhanced friending approach for users on multiple online social networks," Computers 7, no. 3, 2018.
[31] J. Yu, Z. Kuang, B. Zhang, W. Zhang, D. Lin, and J. Fan, "Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing," IEEE transactions on information forensics and security, 13(5), pp.1317-1332, 2018.
[32] T. Orekondy, B. Schiele, and M. Fritz, "Towards a visual privacy advisor: Understanding and predicting privacy risks in images," In Proceedings of the IEEE international conference on computer vision, 2017, pp. 3686-3695.
[33] T. Orekondy, M. Fritz, and B. Schiele, "Connecting pixels to privacy and utility: Automatic redaction of private information in images," In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 8466-8475.
[34] E. Battaglia, L. Bioglio, and R.G. Pensa, "Classification-based Content Sensitivity Analysis," In 28th Symposium on Advanced Database Systems 2020, Vol. 2646, pp. 326-333.

[35] R. Jain, N. Jain, and A. Nayyar, “Security and privacy in social networks: data and structural anonymity,” In Handbook of Computer Networks and Cyber Security, pp. 265-293, 2020.
[36] S. Farquhar, and Y. Gal, “Differentially private continual learning,” arXiv preprint arXiv:1902.06497, 2019.
[37] A. Hassanpour, M. Moradikia, B. Yang, A. Abdelhadi, C. Busch, and J. Fierrez, “Differential Privacy Preservation in Robust Continual Learning,” IEEE Access, 10, pp.24273-24287, 2022.
[38] A. Hassanpour et al., “E2F-GAN: Eyes-to-face inpainting via edge-aware coarse-to-fine GANs,” IEEE Access, vol. 10, pp. 32406–32417, 2022.