A Conceptual Model of Privacy Exposure on Digital Social Networks

Román Pablo Zenobi[1] y María Luciana Roldán[12][0000-0002-4786-5592]

[1] Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina
rozenobi@hotmail.com
[2] Instituto de Desarrollo y Diseño (CONICET/UTN), Santa Fe, Argentina
lroldan@santafe-conicet.gov.ar

Abstract. A Digital Social Network is a group of people connected to each other through a software platform that allows each person to define their profile and communicate with others. The profile that a person defines in this Digital Social Network is called "digital biographical profile". The vulnerability concerning their privacy may be unknown to the users because they are not aware of the risks, they expose themselves to, due to the assumption of being supported by a platform "with established privacy protection conditions". Exposure on a digital biographical profile carries a great responsibility for people, as they must be the guardians of their privacy. The objective of this paper is to propose a conceptual model of digital biographic profiles, factors increasing exposure, and associated mitigation forms, to serve as a basis for the implementation of computerized user awareness tools. The proposed model can be used as a strategy to protect individuals from exposure on digital social networks, which allows for mitigating attacks that compromise their privacy and that of their environment.

Keywords: Privacy, Digital Social Networks, Exposure, Vulnerability.

1 Introduction

Each individual has a psychological profile that is determined by their personality, which distinguishes them from all others. In computer science, a Digital Social Network (DSN) refers to a group of people who are connected to each other by means of a software platform that acts as a mediator and provides support for each individual to define his or her profile and to be able to communicate with other human beings. The profile that a person defines in the DSN is called "digital biographical profile" or simply "digital profile".

As the author Andy Stalman [1] points out, "social networks are an amplifier of what people already are as a society, in the sense that the way we act in our physical or earthly life should be the same as the way we develop ourselves, also digitally”. That is, they are the same people, but amplifying their lives in digital social networks. Therefore, people should be aware that digital social networks also imply the amplification of their level of exposure, thus increasing the vulnerability of suffering attacks on their privacy and that of their environment. The author stresses that we are witnessing the birth of a new man, whose challenge is to learn to live between two worlds: online and offline.

Received May 2024; Accepted June 2024; Published July 2024
https://doi.org/10.24215/15146774e054

ISSN 1514-6774

In the digital world, where social networks are one of the most widely used platforms for peer-to-peer interaction, people expose themselves. The way in which their personal characteristics, biographical profile, privacy, and life issues are shown to others is called "exposure", making them accessible so that other subjects can get to know them from an DSN platform. When a person is exposed on a DSN, it is possible for "someone" to find a way to take advantage of the information that the person has shared. A malicious person could follow a series of steps and reveal the degree of exposure that the user has in his digital social networks and carry out an attack on his privacy.

The aforementioned problems about privacy in digital social networks constitute the motivation for this work. Many people do not know how to properly configure privacy in their biographical profiles on social networks and just employ the default privacy settings, which means they are not aware of what aspects of their private lives are exposed on the social network platforms they use. The big companies behind social network platforms leave control of the privacy of their profiles in the hands of the user. An inadequate privacy exposure on digital biographical profiles not only represents a vulnerability for each individual but also for the organizations in which individuals participate (for example, companies where the individual works, and educational and social institutions, both private and public). Therefore, it is necessary for the organizations to which individuals belong, to count with tools for training and awareness of users of digital social networks.

In his book “Permanent Surveillance” (Snowden, 2019), the former agent of the National Security Agency (NSA) Edward Snowden revealed the value of information and the power it has when it is managed by a government entity, for a purpose that goes beyond preventing terrorism, but is used to monitor each person, their relationships, and their environment. He gave up his role as a computer specialist, seeing firsthand “all the information” that passed before his eyes. This decision led him to be exiled from the United States for disclosing sensitive information and alleged cyber espionage plans. Digital network users may be unaware of their vulnerability when it comes to privacy risks. They assume that they are protected by a platform with “certain privacy conditions” in place, but may not realize the potential dangers they face. However, individuals should be the main keepers of their personal information, as they are its owners and, therefore, they should be the main stakeholders in protecting their privacy.

The objective of this work is to propose a conceptual model of digital biographical profiles, publications and exposed attributes, exposure factors, and associated mitigation factors, to serve as a basis for the implementation of informatics tools for user awareness. The proposed model seeks to be used as a strategy to protect the exposure of people on digital social networks, which allows mitigating attacks that compromise their privacy and their environment.

The remainder of this paper is organized as follows. Section 2 presents some background and related work that serves as a context for the proposal. Section 3 presents the conceptual model of privacy exposure on digital social networks and digital biographic profile. Section 4 presents metrics for calculating the level of privacy exposure. Section 5 presents examples that instantiate the concepts involved in the model, and privacy exposure metrics are calculated. In section 6, some possible mitigations for privacy exposure are proposed. Finally, section 7 presents future works and the conclusions.

2 Background and related work

In the history of Digital Social Networks, there have been shocking events that are examples where user privacy was not prioritized by the platforms hosting these networks.

In the world of business and employment-focused social networks, LinkedIn is the star platform. Millions of people create their professional profiles in a digital format similar to a Curriculum Vitae. These profiles help users connect with peers who share similar specialties and work disciplines. Each user has their own digital profile, which is used to showcase their professional and work experience. In some cases, users may unintentionally reveal both their personal information and that of their workplace through a professional DSN. It is not uncommon for users to comment on their current job, position, tasks, technologies used, and internal links within their place of employment. As mentioned in [2], companies should design a strategy to mitigate the exposure of confidential information by their employees in their use of social networks. In this sense, the need to build a policy for the use of social networks and to communicate it periodically is highlighted. In this work, the author mentions that the conduct or behavior of a person in social networks, how he/she exposes him/herself, can exceed the limits of his/her own privacy and and potentially compromise the confidentiality of their work within the organization they belong to.

In 2012, LinkedIn acknowledged that the company suffered unauthorized access and, as a result, approximately 6.5 million user credentials were leaked. In response to this attack, the action taken by the platform was to reset the passwords of those accounts that had been compromised. This was confirmed by the social network itself in an official statement [3]. Subsequently, in 2016 it was discovered that a larger number of user credentials had been exposed on the Internet. Approximately, more than 100 million profile account data have been leaked and published. Upon identifying the compromised users, the company asked them to reset their passwords and, in addition, promote the use of Two-Factor Authentication and the construction of strong passwords. It can be seen that the measures taken by the company consisted of shifting the responsibility for the security of the profiles to the individual users.

Recently, during January 2024, cybersecurity researchers from the companies Cybernews and Security Discovery identified a massive leak with more than 26 billion records with user data from social platforms in which LinkedIn is located. For this platform, a leak of 251 million accounts is mentioned.

On the other hand, the social network Facebook is perhaps the main exponent of the type of platforms in which users create their profiles and share with other people, creating digital societies. In 2014, an event occurred that called into question the extent to which the data provided by users is protected and not used for other purposes. The consulting firm Cambridge Analytica was accused of having obtained information from millions of Facebook users without permission, i.e. violating the policies of use of the social network [4]. To do so, they designed for users an application to answer a series of questions in exchange for the payment of a few dollars and thus learn a little more about their behaviors and preferences. At that point, they had obtained approximately 270000 user profiles with their consent to take the benchmark test. This application needed to be logged into Facebook and granted certain privileges. What happened is that one of the permissions requested by the application was access to the "friends" data. This resulted in a total collection of information from 50 million profiles, although most of them had not given their approval.

The information obtained was sent to the consulting firm Cambridge Analytica, not only for academic purposes (as users had been informed) but to be used for other purposes, for example, for political campaigns. The discovery of these facts led public opinion and government institutions to question the lack of transparency involved in the use of data without the permission of user profiles. This event put this social network in the spotlight, so the platform reviewed and updated its conditions of use and privacy of user data.

In August 2016, WhatsApp updated its privacy policy to allow the sharing of user data with Facebook; as it is quoted, "As part of the Facebook family of companies, WhatsApp receives information from and shares information with this family of companies. We may use the information we receive from them, and they may use the information we share with them, to help operate, pro- vide, improve, understand, customize and market our Services and their offerings, as well as provide support services for our Services.... Facebook and the other companies in the Facebook family may also use our information to improve your experiences with their services...". This policy change led the Spanish Data Protection Agency (AEPD) to impose a fine on the two platforms for considering that the established privacy conditions did not comply with current regulations [6]. In the case of WhatsApp, the agency considered this policy as an intention to provide user data to Facebook without their prior approval, and on the side of Facebook, it was considered the intention to use this information for their own uses and benefits.

There are works in the literature that address the history of how we have reached today's situation where there is an overexposure of people's privacy. Rosenblum et al [8] describe how this began to occur globally through the spread and adoption of DSNs. These authors refer that at the dawn of digital communications, it was possible to express oneself through blogs, to make some videoconferences with the webcam, and to make use of emoticons to show one's feelings. In those early days, the profiles of a person on these websites were limited only to his name, age, city, email and some identifying image. Later, social networks such as Facebook and MySpace (precursors in the beginning), led to the great leap, that is, to allow each user to create their own profile, indicating their preferences for exposure, showing what, in principle, remained at the level of conventional human social networks. It could be said that this "small leap" for digital social networks was a "leap into the void" for the privacy of individuals, giving way to the problem of exposure, and the concept of "online privacy" emerged. The same authors point out in their work that privacy implies confidentiality, and that the user is the sole owner of his or her profile and therefore manages permissions at the highest possible level of granularity. That is, to the greatest detail, topic by topic of their profile space. Given the current challenge, there is a need for collaborative work between social science experts, security communities, industry, and regulations in order to make decisions on how to apply security mechanisms and policies to preserve privacy in digital social networks.

Choi et al [9] analyze the phenomenon of social networks and present an "audience" schema around a DSN user with the following participant roles: "Target user", "Disseminating friends", "Friends of the target user" and "Friends in common". Based on this scheme, they differentiate in the "audience" between Posting Only and Posting with Tagging. In this work, the power of "propagation" of the Target User's profile among the different users and roles that are connected is evidenced. The distinction is made with the propagation mode where users "tag" other users in profile posts. In such cases, exposure is amplified because users are explicitly named by the tags.

To understand the context of digital social networks, the work of Srivastava and Geethakumari [10] is interesting, stating that digital social networks have moved from a niche phenomenon to a mass adoption by the user population. This means that, in the last decade, networks have been used as platforms for users to communicate with each other, exchange information, express their feelings, and build relationships with other Internet members. The authors present the results of a survey in which they inquired about the level of knowledge that people have about how a social network can expose privacy and to what extent users are aware of this level of exposure.

What was obtained as interesting information is that 88% of this group of people would stop using a social network if they found that their sensitive personal data were being used in a way they did not expect. In contrast, according to another question, the majority (63.3%) of users commented that the process of adjusting the privacy of a social network profile generates a waste of time and is complex or difficult to understand. Another relevant result of this work is the "sensitivity calculation". Sensitivity is the property of information that makes it private. Using this concept, it is expected that the higher the level of privacy required, the greater the sensitivity of the information. Therefore, it is sensitive information that must be strongly protected by the users. Concerning this, the authors identified and categorized the attributes of the profiles that make up the sensitivity of the information.

It is important to note that the company Meta, the owner of Instagram, since June 2023, has incorporated a restriction on sending messages to profiles of adolescent and underage users. In that sense, in order to send a direct message, the interested party should first follow the other person, that is, there has to be accepted by the other user . This measure is added to other additional measures that Meta has implemented over time to protect the adolescent public. Along these lines, since January 2024, Instagram automatically began asking users in this time zone to update their privacy conditions in a simplified manner [11, 12].

Furthermore, focusing on the control of Digital Social Networks, in line with what was mentioned by Snowden in [14], there are currently a series of countries in which their governments have blocked access to these platforms for their population. To name a few examples, in North Korea, all digital social networks are prohibited; in China, the blocking is for platforms of Western world area origin; In Russia, Twitter, Facebook, Instagram and LinkedIn are banned [15].

3 Conceptual model

This section presents a conceptual model (Fig. 1) for publications in digital biographical profiles. The model identifies the main concepts and relationships for understanding the privacy domain in social networks and serves as a basis for the implementation of user awareness software tools. It is based on the concept of digital social network (*DigitalSocialNetwork*), which refers to a group of people who are connected to each other by means of a software platform that acts as a mediator and provides the support for each individual to have a defined digital biographic brofile (*Digital Biographic Profile - DBP*) and to be able to communicate with other individuals in the network. This profile constitutes the initial configuration that a user (person) creates to start using the functionalities of the DSN platform. Having a Digital Biographical Profile is the first step to start gaining exposure.

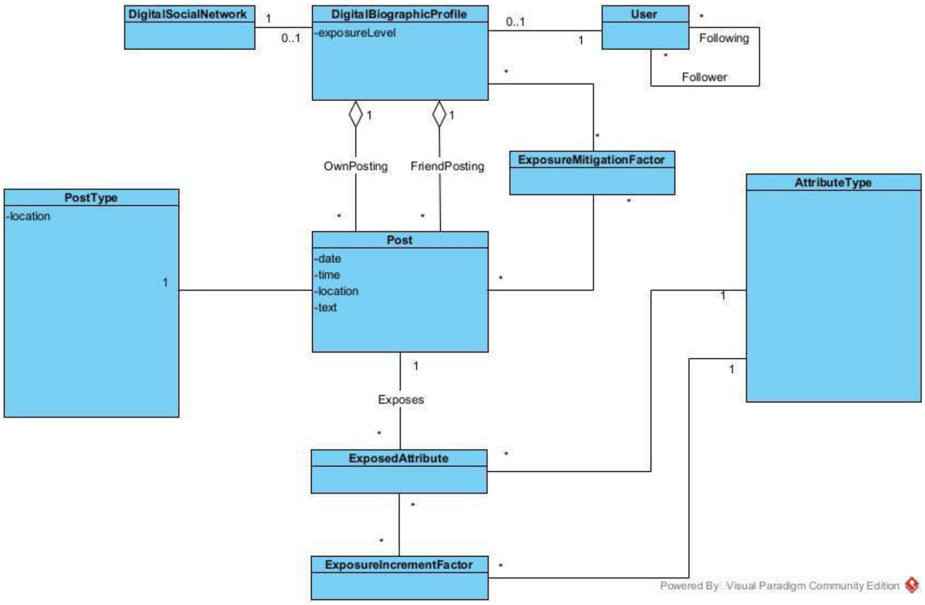

Figure 1. Conceptual Model of Digital Biographical Profile. Main concepts

A *User* of a digital social network has some kind of relationship with other *User*(s) of the same network and can therefore generate interaction and share content as if they were "known". Depending on the DSN, this relationship is known by the term *contact*. In the case of Facebook, contacts are called "Friends". In the case of Instagram, a contact is called a "Follower". In this sense, a given user will have several "Followers" and several "Followed" friends. In the case of Instagram, the type of contact is unidirectional. If a User A requests to follow a User B, and if User B accepts, it does not mean that User B can now see User A's content, i.e. User A becomes User B's Follower. On the other hand, there must be a request from User B to follow User A, and the corresponding acceptance, so that User B becomes a Follower of User A, and thus empowers the access. For the LinkedIn network, contacts are called "Connections". A user can choose to connect with another user to become a contact, start interacting directly, and view published content. Fig. 1 simplifies all these variations by considering a generic

DSN and establishing a relationship between users by indicating the roles *follower* and *followed*.

Continuing with the description of the model (Fig 1), it is observed that, in each DBP, a user begins to make publications (*Post*). They are classified into types (*PostType*) and have a property called *location* that indicates the place or section that has the publication in the DBP.

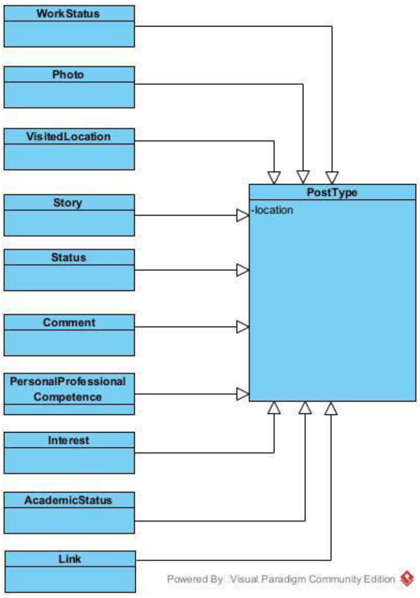

Figure 2. Types of publications in digital social networks (Post).

This classification of *PostType* is presented in Table 1, and the corresponding type is defined as specialization of the concept *PostType* in Fig .2.

Table 1. Types of posts and their attributes.

PostType	Location
1. Comment	1.1. Wall / Profile Main Page
	1.2. In another type of publication (photos)
2. Photo	2.1. Cover
	2.2. Profile
	2.3. Wall / Profile Main Page
3. Links	
4. Interest	4.1. Personal
	4.2. Labor
5. VisitedLocation	
6. Story	
7. Status	
8. WorkStatus	8.1. Current
	8.2. Background

9. AcademicStatus	9.1. Education Level
	9.2. Educational Institution
10. PersonalProfessionalCompetence	

Table 1 also shows the possible values that the *location* property can take according to the type of publication in question. For certain types of publications, the location value is not relevant.

Each *Post* in a *DBP* may involve the exposure of certain attributes or aspects of the *DBP* (represented by *ExposedAttribute*, Fig. 1). For example, when a user posts the cover photo of a profile, a certain exposure will be taking place depending on what is identified in that photo.

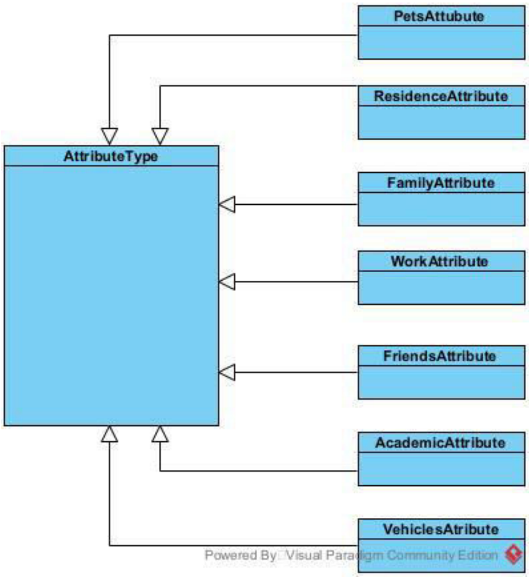

Figure 3. Specialization of Attribute Type

The partial conceptual model in Fig. 3 describes that an *ExposedAttribute* is of a certain type (*AttributeType*). The attribute type indicates to which set of aspects related to the user or his digital biographical profile an attribute corresponds. For example, the name of the user's pet, breed, the veterinarian where it is treated, etc. correspond to the *PetsAttribute* type; the name of the user's children, the school they attend, whether they have a partner or their marital status, data about their parents, etc. correspond to the *FamilyAttribute* type. In order to catalog the possible types of attributes that can be exposed, a typification of the types themselves is proposed. This typification is explained in the first column of Table 2. It should be considered that for a *Post*, more than one type of attribute can be exposed.

It is worth clarifying that, in the scope of this work, it is not of interest to know what private data are exposed (or could be exposed) in a publication, i.e., to know the value of an exposed attribute. What is of interest is what type of data are exposed (or could be exposed) in a publication by the user of a DSN, since the ultimate goal of the conceptual model is to generate tools to alert the users about what types of data they could disclose with a potential publication, and to create awareness of whether it is really his/her will to do so.

On the other hand, an attribute type can be enhanced by various factors that generate an increase in the exposure of that attribute type. In Fig. 1 this is represented by the concept *ExposureIncrementFactor* (*EIF*).

Table 2. Types of attributes and their Exposure Increment Factors.

Attribute Type	Exposure Increment Factor
1. Residence data (House, Apartment, Work Office, Temporary Location) represented by *ResidenceAttribute.*	1. Existence of doors and/or windows 2. Type of doors and windows 3. Existence of alarm sensors 4. Existence of security cameras 5. Type of room: bedroom, dining room, living room, patio. 6. Number of rooms 7. Type / Style of furniture: by resemblance in different photos, possibility to infer the number of rooms in the house. 8. Logos / Marks on objects and / or clothing deposited in the room.
2. Vehicles Data. Represented by VehiclesAttribute.	1. Brand, model, color. 2. Patent / Domain. 3. Particular unique features (decals, marks, scratches, bumps, etc.). 4. References to cities / locations / companies in the case of a work vehicle. 5. Parking location. E.g., a private parking lot. 6. Surrounding areas of the parking place. 7. Points of reference (businesses, houses, other vehicles).
3. Family Data. Represented by FamilyAttribute.	1. Number of members and possible relationship. 2. Identification of children. 2. Dates and/or particular events (birthdays, weddings, etc.) 3. Locations related to the family (parents' homes, neighbors, etc.) 4. Family pets. 5. Family vehicles. 6. Family-related locations.
4. Friends Data. Represented by FriendsAttribute.	1. Number of friends. 2. Age ranges. 3. Homes and related locations. 4. Family and/or contacts of friends. 5. Friends' vehicles 6. Friends' pets. 7. Places of common use such as clubs, businesses, etc. 8. Events (birthdays, meetings, anniversaries).
5. Pets Data. Represented by PetsAttribute.	1. Amount and type with race. 2. Unique distinctive features: necklace, chains, pendants, caps, special clothing. 3. Pet locations. 4. Behaviors related to walking pets. 5. People with a greater affinity for pets.
6. Work Data. Represented by WorkAttribute	1. Names of other employees of the same company and sector. 2. Presentations with corporate information. 3. Computer desktop, showing the programs in use. 4. Physical spaces of the company and/or users. 5. Institutional software for use among employees. Ex: G-Suite, MS Teams, Cisco.

	6. Email platforms. 7. Software development interfaces. 8. Brand and model of the computer. 9. Operating System. 10. Internet Browser: Open Page URLs. 11. Structure of web pages, sections 12. Corporate Contacts 13. Installed and/or running applications 14. Layout of offices, desks. 15. Types of computers and position according to hallways, windows. 16. People in the same location working: quantity, locations, possible sector identification. 17. Related personnel: maintenance, cleaning, etc. 18. Position of printing machines, scanners, paper shredders, coffee machines, etc. 19. Location of security cameras and alarm/fire sensors. 20. Location of doors, windows and physical access control system. Example: presence of surveillance and use of magnetic card to open doors.
7. Academic Data. Represented by AcademicAttribute.	1. Name and location of academic institutions. 2. Names of teachers and students. 3. Physical layout of the classrooms. 4. Location of the classrooms. 5. Names of personnel belonging to the academic institution. 6. Physical locations of the different departments of the institution: Secretaries, Students, Management, etc. 7. Data presented on classroom blackboards. 8. Arrangement of entrance doors and windows. 9. Existence of security guards. 10. Existence of access control with turnstile or other system. 11. Existence and location of security cameras.

In Table 2, this is detailed in the second column, thus cataloging a set of possible factors that increase exposure by type of attribute.

Different types of attributes that a user exposes on their social network profile can increase the level of exposure for that profile. For instance, when a user selects a cover photo that exposes data related to their family. In this case, this can be represented by a *Post* instance whose type of attribute exposed is *FamilyAttribute*, and the value of *location* property of the is *Cover*.

In addition, users frequently face other factors that increase exposure when other aspects can be identified through the photo (such as the name of the minors in the family, number of members, etc.), which allow obtaining additional information about the family group. In conclusion, from a certain post selected by the user, additional factors can increase the level of exposure of the digital biographic profile, which inherently belong to the type of exposed attribute present in the post. The *ExposedAttribute* concept adds (gathers) all the *ExposureIncrementFactors* instances that may exist for the type of attribute exposed in the publication.

In addition to *Exposure Increment Factors*, other factors impact user posts, attenuating or mitigating the effects of exposure. These are called Exposure Mitigation Factors (EMF), represented in the conceptual model with the concept *ExposureMitigationFactor*, and as can be seen in Fig. 1, it is directly related to *Publication* or the Digital Biographical Profile. For example, publishing a photo and making it only accessible to the user's "friends" is a way to mitigate exposure. These types of mitigations act at the *Post* level in general and at the user's biographical profile level, being configurations specific to each platform.

To minimize exposure in a publication (*Post*), a compromise solution must be reached that tends to cancel the factors that increase exposure, to balance them with the mitigating factors, and achieve adequate exposure. A good practice to achieve an adequate privacy exposure is to favor factors that attenuate exposure and minimize factors that increase exposure when making a post or configuration.

Additionally, the conceptual model proposed allows, based on the *Digital Biographical Profile* concept, to calculate what is called a *Chain Exposure*. This concept means that, by observing the different types of attributes exposed in different publications of a profile, broader user information could be inferred, covering various types of attributes with various factors of increment exposure. An example of chain exposure is the following: a user posts a photo with a group of friends, mentioning the names of each of them. Later, after some time, user posts a new photo showing a location of a club, where this person will do a particular sport. After that publication, later, the same user generates a new photograph of a dinner with the same group of friends where the place can be seen and mentioned. These three photos have *Exposed Attributes* that belong to the *Digital Biographical Profile* of the user, therefore, the individual is providing valuable information for an attacker. Then, the attacker will know: the group of friends with their names, the time and place of the photos, the sport they practice with their friends, the habit of having dinner after sports activity with their friends.

The model also allows us to infer the condition of *Passive Exposed Subjec*t for a DBP. In this case, through the presence of instances of publications with high exposure made by friends of a DBP, it would be possible to infer that a user has a certain level of exposure due to publications in which they are tagged.

4 Metrics proposed to quantify the exposure of a digital biographical profile.

In the conceptual model for *DigitalBiographicProfile*, the exposure level attribute (*ExposureLevel*) was defined. To calculate the value of this attribute, a set of metrics are defined that are based on the concepts represented.

1) Metric to calculate the exposure value of an attribute *i* in a post p

*EV_ip = ExposedAttibute_i * Summation(EIF_ip)/Total Amount of EIF for the attribute type of i.*

ExposedAttribute_i takes a value of 1 or 0, whether or not there is presence of that type of attribute in the publication p. It is calculated as the sum of all the exposure increment factors that the exposed attribute has, divided by the number of possible exposure increment factors per type of attribute.

It is assumed that if this metric is calculated it is because publication p exposes the attribute *ExposedAttribute_*i . Otherwise, the value of the metric is 0.

Interpretation: a value between 0 and 1 is obtained, the closer to 1, the greater the exposure of the type of attribute exposed.

2) Metric to calculate the exposure value in a post p

*EV_p = EMF_p * Summation(*EV*_ip) / Total Amount of AttibuteType*

EMF_p takes value 1 or 0 if a mitigation factor is applied or not for publication p. This mitigation value is applied as a product to a sum. The sum is calculated on the results obtained in the calculation of all *EV_ip* metrics for all exposed attributes *i* by publication p, obtaining an exposure value for the post (publication). If there is mitigation, the value of *EV_p* is nullified, otherwise it will be greater than zero. Since the types of possible attributes are typed, the total number of them is known. Dividing the sum by this amount, a value between 0 and 1 is obtained.

Interpretation: the closer the value of *EV_p* is to 1, the more aspects of user privacy are exposed in the publication.

3) Metric to calculate the exposure level of a DBP *dbp*

*EV_ dbp = EMF_dbp * (Summation(EV_p) + Summation(EV_pp))*

EMF_dbp takes a value of 1 or 0 if a mitigation factor is applied or not to the digital biographical profile. This mitigation factor is applied to the sum of two sums. The first sum is calculated on the results obtained in the calculation of all *EV_p* metrics for all publications p of a digital biographical profile *dbp*, obtaining an exposure value for the *dbp*. The second sum is calculated on the results obtained in the calculation of all the *EV_p* metrics for all the *pp* publications of the friends of the digital biographical profile *dbp* in which it has been tagged, obtaining an exposure value for the *dbp* as a subject exposed passive. If a mitigation is applied at the *DBP* level, the value of *EV_dbp* is canceled (or decreased), otherwise, it will be greater than zero. Given that the number of publications of a profile is variable, the interpretation of this metric is: the value of *EV_dbp* can be 0, if mitigation is correctly applied, or greater than 0 if mitigation is not applied, being higher as the number of publications with exposed attributes increases.

A variation of this metric could be proposed if it is considered that there is more than one possible mitigation level *EMF_dbp*, taking values between 0 and 1.

The *EV_dbp* metric is the one used to calculate the Exposure Level/Value (EV) of a *DBP*. Ranges can be defined to indicate High, Medium, and Low exposure levels.

5 Case studies

As a proof of concept, five case studies were developed on the social network Facebook.

Scenario 1: Residence data post

The first example (Fig. 4) presents a DBP that contains a post of type *Photo*, whose location attribute value is the user's *Wall*. The object diagram for this DBP based on the conceptual model is also presented. From the photograph, the following types of exposed attributes can be identified: *AResidence1:ResidenceAttribute* (value equal to 1) and *AVehicle1:VehicleAttribute* (value equal to 1).

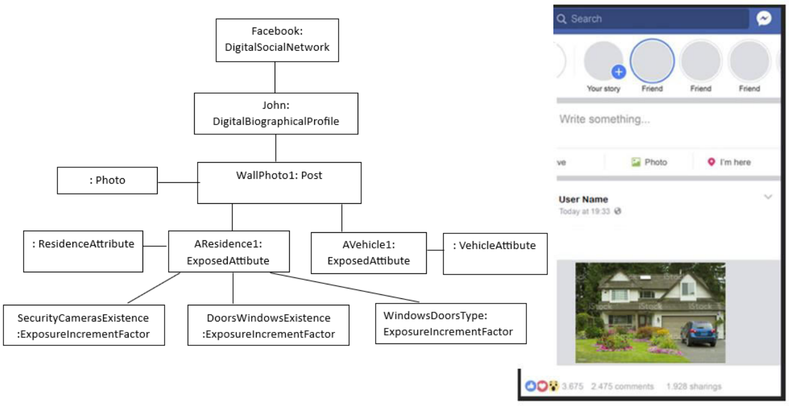

Figure 4. Instances involved in a Facebook post with a photo on the wall. Source[1]

Next, Fig. 5 identifies the exposure increment factors that can be identified for the exposed attribute *AResidence1* (*ResidenceAttribute*).

- EIF_ AResidence1_1: Existence of Security Cameras (Description: two security cameras are detected in the front of the house)
- EIF_ AResidence1_2: Existence of Doors and Windows (Description: 5 windows and 2 doors are detected (one gate included).
- EIF_3_AResidence1_3: Type of Doors and Windows (Description: wooden doors/gates are detected. In addition, door and window materials, type of gate, the lack of bars and/or lattices, among other things, are distinguished).

[1] Photo´s source: Hermosos Casa Y Jardín Foto de stock y más banco de imágenes de Coche - Coche, Camino de entrada, Casa - iStock (istockphoto.com)

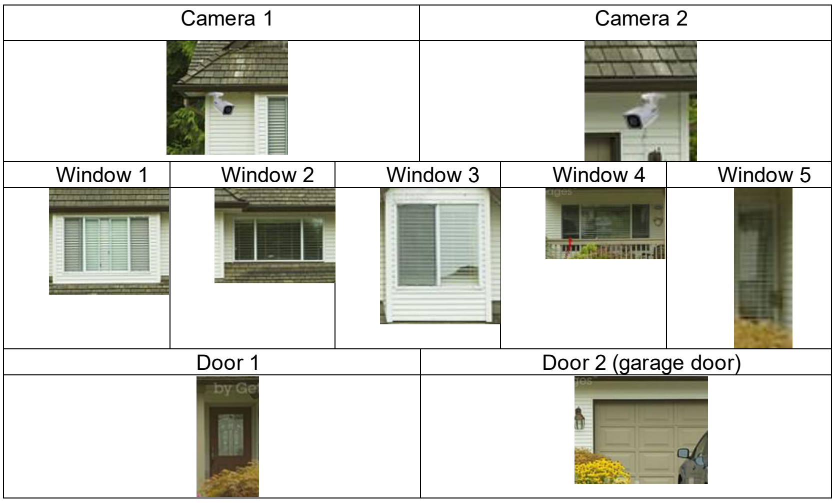

Figure 5. Example of Exposure Increment Factors in the post.

On the other hand, for the exposed attribute *AVehicule1* (of type *VehicleAttribute*) the exposure increment factors are identified: *EIF_ AVehicle1*_1: Brand, color and model, and *EIF_ AVehicle1_2*: *Patent* / *Domain* (Fig. 4).

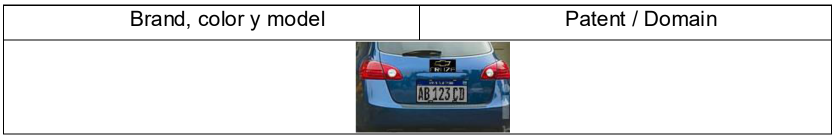

Figure 6. Example of Exposure Increment Factors in the post.

Next, the metrics defined for the case study are applied:

- Metric to calculate the exposure value of attribute "AResidence1:ResidenceAttribute" in WallPPhoto1 publication.

EV_ResidenceAttribute_WallPhoto1 = *AResidence1:ResidenceAttribute* * Summation(*EIF_i_ ResidenceAttribute_WallPhoto1*)/*Total Amount of EIF for attribute type of ResidenceAttribute* = 1 * 3 / 8 = **0,375**

- Metric to calculate the exposure value of attribute "AVehicle1:VehicleAttribute" in WallPhoto 1 post.

EV_VehicleAttribute_WallPhoto1 = *AVehicle:VehicleAttribute* *

Summation(*EIF_i_VehicleAttribute_WallPhoto1*) / *Total Amount of EIF for attribute type VehicleAttribute* = WallPhoto1 = 1 * 2 / 7 **= 0,285**

- Metric to calculate the exposure value in the WallPhoto1 post

For the calculation, *EIF_WallPhoto* is considered to be 1, that is, the photo was published publicly, without access restriction. The results of the previously calculated metrics are also used.

*EV_*WallPhoto*1 = EIF_WallPhoto1 * (EV_ResideceAttribute1_WallPhoto1 + EV_VehicleAttribute_WallPhoto1) / Total Amount of AttributeType*
*= 1 * (* 0,375 + 0,285*) / 7* = 0,66 / 7= **0,09**

After presenting this first case, below, two similar scenarios are shared under the same concept: analysis of photo posts within a certain profile of a digital social network.

Scenario 2: Work Data (Fig. 7 and Fig. 8)

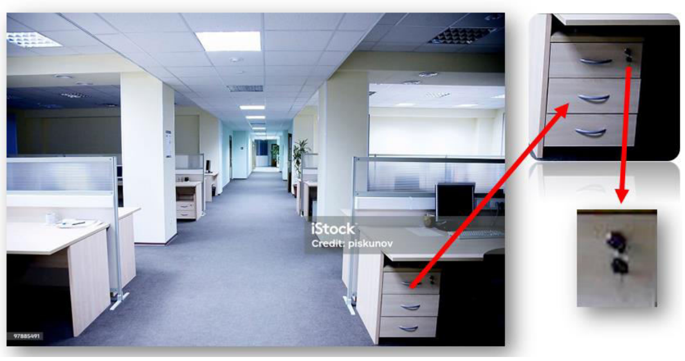

Figure 7. Example photo for Case 2 including Factor 1 and 2.
(Source: https://www.istockphoto.com/es)

- Exposure Increment Factor #1
  — *Physical spaces of the company and/or users.*

- Exposure Increment Factor #2:
  — *Layout of offices, desks.*

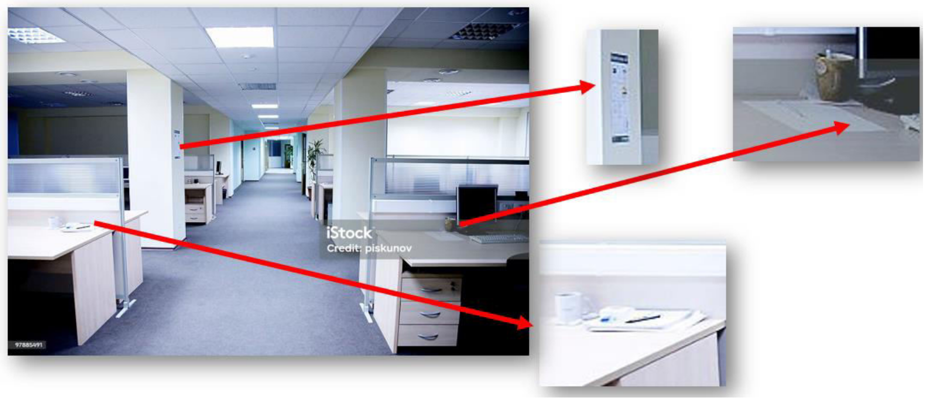

Figure 8. Example photo for Case 2 including Factor 3
(Source: https://www.istockphoto.com/es)

- Exposure Increment Factor #3:
  - *Documentation on desks, printers, meeting tables, panels.*

- Attribute exposure value: “AWork1:WorkAttribute” in case Fig. 7 and Fig. 8.

*EV_WorkAttribute_Case2 = AWork1:WorkAttribute * Summation(EIF_i_WorkAttribute_Cas2)/Total Amount for attribute type of* ***Work.***

*EV_WorkAttribute_Case2 = 1 * (3 / 20) = 0,15*

Scenario 3: Family Data (Fig. 9)

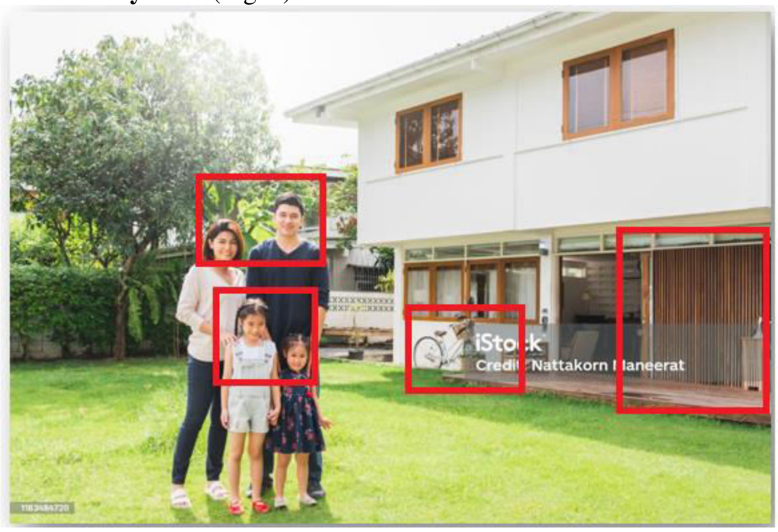

Figure 9. Example photo for Case 3 including Factor 1, 2, 3 and 4.
(Source: https://www.istockphoto.com/es)

- Exposure Increment Factor #1:
  - Number of family members and possible relationship.

- Exposure Increment Factor #2:
  - Identification of minors / children.

- Exposure Increment Factor #3:
  - Related locations.

- Exposure Increment Factor #4:
  - Family vehicles.

- Attribute exposure value: “AFamily1:FamilyAttribute” in Case 3.

EV_FamilyAttribute_Case3 = AFamily1:FamilyAttribute * Summation(EIF_i_ FamilyAttribute_Case3)/Total Amount of EIF for attribute type of Family.

EV_FamilyAttribute_Case3 = 1 * (4 / 8) = 0,5

6 Mitigations

When users create a profile and share information on digital social networks, they should be aware that they are entering a publicly accessible platform. This means that their profile will be available on the internet, making them more vulnerable to attacks. Therefore, it is important to take appropriate measures to protect the information shared on digital social networks and control privacy to minimize exposure.

As a first mitigation measure, the device used to access the social network profile and the specific login to the platform must be protected. It is worth considering that Information Security acts in layers, implementing security measures at different levels to protect from various angles. This way, if an attacker manages to overcome one barrier, there are still others to overcome.

The concept of security layers applies to the protection of access to the Social Network for users. The following security layers must be considered:

1) **Device Level Security:**

A. Ensure that your operating system is current, supported, and updated. Check that the latest updates have been applied.

B. Keep your applications updated with versions currently supported by the manufacturer.

C. Use secure login methods for your operating system, such as username/password, PIN, biometric access, or pattern.

D. Enable session lock when your device is unattended. Ensure your computer, notebook, or cell phone is locked when not in use.

E. Avoid writing passwords down on paper or in visible places as memory aids. Use secure methods for storing and managing passwords.

2) Social Network Security:

A. Enable Multi-Factor Authentication (MFA) for login. This adds additional factors to the password to confirm users' identity.

B. Use different passwords for each social network. Avoid using repeated patterns such as the month of the year, day number, year, etc.

C. Consider using a Password Management platform. These programs allow you to store all your passwords securely and use only one master password in conjunction with MFA to access them. They also offer tools to generate strong passwords.

D. Avoid storing login passwords in your device's web browser.

E. Always log out of your Social Network session when you stop using it on the device.

3) Social Network "use" Security

To mitigate the exposure of a profile, a series of practices must be applied to help "cleanse" the exposure on a digital social network. These practices aim to control the factors contributing to the profile's exposure. This concept, also known as "sanitization," involves implementing the necessary measures and changes to achieve an appropriate level of exposure.

It's important to note that once information is published, the user loses control over its lifecycle. Exposure cannot be completely eliminated in such cases. To achieve maximum sanitization, one should consider deleting their entire social network profile.

Therefore, when considering a digital biographical profile, the following sanitization practices should be considered:

A. The "contacts" or "friends" on Facebook may not necessarily be the same as those on Instagram. Therefore, it is important to conduct a thorough review of each contact on each social network and take appropriate actions accordingly.

B. From reviewing each social network profile, focus on identifying the exposure attributes of the profile. Once these attributes are identified, determine the factors that could increase the exposure level.

C. As a result of the previous step, proceed to remove any information that has been identified as having exposure. Use this opportunity to raise awareness among users, including the user's social network contacts. An effective mitigation strategy is to replace the posts that had exposure with messages promoting good practices and recommendations on how to prevent exposure-related attacks.

D. Search for the user's name on each of the social networks using a search engine. The results will display any mention of the user, including instances where the user has been tagged in photos or posts. This step helps identify Passive Exposed Subjects, which may include the user themselves or other individuals who are being exposed, potentially without their consent.

7 Conclusions

An important aspect to consider is the behavior of users on digital social networks. Regardless of the security measures implemented by each platform and the privacy settings applied to digital profiles, users are the responsible for the level of exposure they choose.

Individuals are the owners of their publications and thus have the authority to decide what information to share, which constitute their digital biographic profile. While tools may assist in understanding the level of exposure a publication may have, the final decision rests with the user. Therefore, it is crucial to raise awareness among users about managing their exposure on digital social networks and the potential consequences of inappropriate information use.

This work proposes an awareness layer for social network users to monitor the exposure level of their publications, allowing them to maintain their desired level of privacy. To achieve this, commonly exposed attributes were identified, and a set of metrics were proposed that aim to strengthen actions that protect digital profiles.

In addition, this work aims to ensure that users actively choose to preserve their privacy and when they decide to publish information on a Digital Social Network, they do so by applying mitigations that mitigate their level of exposure and trusting that they will show what they want to show accurately.

As a starting point for an awareness program for users, it will be necessary to conduct a survey on a certain sample to investigate the behaviors present on Digital Social Networks. The survey should investigate people's knowledge of the Privacy Policies of each of the platforms. That is, if they know of their existence and if they take them into account when reading or if they are omitted directly.

Future lines of work for this research are listed below:

1. Develop a tool that integrates with web browsers to alert users of possible inappropriate exposure when uploading a photo to a digital biographical profile.
2. Validate the tool as a means of raising awareness for both individuals and organizations.
3. Define rules to automate the detection of exposure factors or passive exposed users.
4. Explore the possibility of using image recognition technologies.
5. Incorporate a set of Object Constraint Language (OCL) constraints to validate different instance models and add queries to infer the existence of *Chain Exposure* in a *Digital Biographical Profile,* or to identify users that are *Passive Exposed Subjects*.

The future tool is intended to complement web browsers as an extension, that could be employed when the user accesses a Digital Social Network such as Facebook, Instagram, or LinkedIn, and decides to make a post. The tool can be used to analyze the level of privacy exposure for a post and its users in an anticipated way, raising alerts and indicating potential privacy risks. In an initial version, the tool can focus on analyzing "photo" type publications. A more advanced version will include the ability to upload a photo and, by means of image recognition technology, detect and categorize the publication based on the corresponding exposed attributes. It will also present possible factors that could increase exposure to the user, allowing them to create a checklist, obtain an estimated level of exposure for the potential publication, and decide whether or not to proceed with the post.

In order to explore the possibility of using image recognition technology for the tool, the authors will explore several image object detection libraries, such as:

1. Azure AI | Vision Studio:
   https://portal.vision.cognitive.azure.com/demo/generic-object-detection
2. Google Cloud - API de Cloud Vision:
   https://cloud.google.com/vision/docs/object-localizer?hl=es-419
3. Image Recognize:
   https://imagerecognize.com/
4. Astica
   https://www.astica.org/vision/object-detection/

A tool that helps in this process is a great ally. However, we must not lose sight of why it is important for individuals to consciously and safely manage their privacy when using social media platforms. Managing a profile on a digital social network by a user carries great responsibility. It depends on how vulnerable your privacy and that of your environment will be.

Besides Digital social media platforms have settings to mitigate exposure, the only one who has the control to decide how to display their information is the user. They are fully responsible for taking care of their exposure and that of those close to them. In conclusion, people are the main custodians of their personal information, and, therefore, they are the main interested parties in protecting their privacy and that of their environment.

References

1. Stalman, A.: Humanoffon. Ediciones Deusto (2016).
2. Wu He.: A review of social media security risks and mitigation techniques. In: Journal of Systems and InformationTechnology Vol. 14, pp. 171 – 180 (2012).
3. LinkedIn Blog Page, https://blog.linkedin.com/2016/05/18/protecting-our-members, last accessed: 2020/05/23.
4. Infobae Homepage, https://www.infobae.com/america/tecno/2018/03/20/7-datos-para-entender-el-escandalo-de-facebook-y-cambridge-analytica/, last accessed: 2020/05/23.
5. WhatsApp Homepage, https://www.whatsapp.com/unsupportedbrowser?doc=privacy-policy&version=20160825, last accessed: 2020/05/23.
6. AEPD Homepage, https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar, last accessed: 2020/05/23.
7. Twitter Blog Page, https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html, last accessed: 2020/06/21.
8. Rosenblum D.: What Anyone Can Know: The Privacy Risks of Social Networking Sites. In: IEEE Security & Privacy, vol. 5, no. 3, pp. 40-49 (2007).
9. Choi, B. C. F., Jiang, Z. (Jack), Xiao, B., & Kim, S. S.: Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding. In: Information Systems Research, pp. 675–694 (2015).

10. Srivastava A., Geethakumari G.: Measuring privacy leaks in Online Social Networks. In: 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2095-2100 (2013).
11. F. Company y Meta, https://about.fb.com/news/2023/06/parental-supervision-and-teen-time-management-on-metas-apps/amp/, last accessed 2024/01/27.
12. F. Company y Meta, https://about.fb.com/news/2024/01/teen-protections-age-appropriate-experiences-on-our-apps/, last accessed 2024/01/27.
13. Télam, https://www.lavoz.com.ar/tecnologia/detectaron-una-megafiltracion-de-datos-en-linkedin-twitter-y-otras-redes/, last accessed 2024/01/27.
14. E. Snowden: Vigilancia permanente. Editorial Planeta (2019).
15. A. Groenewald, https://www.cyberghostvpn.com/es_ES/privacyhub/countries-ban-social-media/, last accessed 2024/02/03.