The Computer Journal Advance Access published July 31, 2014

doi:10.1093/comjnl/bxu066

Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures

Constantinos Patsakis[1]*, Athanasios Zigomitros[1,2], Achilleas Papageorgiou[1] and Agusti Solanas[3]

[1]*Department of Informatics, University of Piraeus, Piraeus, Greece*
[2]*Institute for the Management of Information Systems, 'Athena' Research Center, Marousi, Greece*
[3]*Smart Health Research Group, Department Computer Engineering & Mathematics, Universitat Rovira i Virgili, Catalonia, Spain*
**Corresponding author: kpatsak@unipi.gr*

A key aspect of online social networks (OSNs) is the user-generated multimedia content shared online. OSNs like *Facebook* have to deal with up to 300 million photos uploaded on a daily basis, both video- and audio-related social networks have also started to gain important shares of the market. Although the security and privacy mechanisms deployed by OSNs can cope with several risks and discourage inexperienced users from malicious behaviours, many issues still need to be addressed. Uploaded multimedia content carries information that could be transmitted virally and almost instantaneously within OSNs and beyond. OSNs could be seen as a multimedia heaven for users. However, in many cases they might end up being the user's personal hell with information disclosure or distortion, contrary to his/her will. In this article, we outline the most significant security and privacy issues related to the exposure of multimedia content in OSNs and we discuss possible countermeasures.

Keywords: online social networks; identity theft; privacy; multimedia content management

Received 15 September 2013; revised 17 June 2014
Handling editor: Zhiyong Zhang

1. INTRODUCTION

The dominance of online social networks (OSNs) over the Internet was unimaginable, even a few years ago. Their daily traffic, usage and worldwide acceptance from users indicate that they are here to stay. The digital persona of users has moved from their personal websites to their OSN profiles. A key factor to explain this shift resides in the simplicity that OSNs provide to their users to manage their social lives. As a result, they become more efficient since they can modify the content of their profiles and control which information about themselves is shared. Additionally, this information can be edited or even deleted. Hence, users can present themselves as they want, promoting an idealized version of themselves, just like advertisements, which in many cases bare a little resemblance to the actual persona.

OSNs are being used everyday by millions of users, but the exchanged information is not limited to just messages between friends or typical small talk socializing. Modern OSNs have, to some extent, replaced traditional human resources departments and recruiting agencies, providing not only their up-to-date curriculum vitae, but references and their work experience status. From another perspective, OSNs have also become news distribution platforms. In many cases, events are broadcast in social media before the news appear in common media. Therefore, OSNs have totally changed the way people interact during their everyday lives and have created new communication standards.

While users build their profiles in OSNs, one of the vital ingredients is the multimedia content, after all, humans are very sensitive to visual and audio stimuli. Modern OSNs allow users to upload images, video and sound files, which frequently require extreme storage facilities to provide the requested services just-in-time.

With regard to security and privacy, on the one hand we find malicious users that try to exploit software vulnerabilities of the infrastructure to gain access to sensitive information. Although

this might be very difficult to achieve, attackers may resort to social engineering in order to attack their victims. Tricking users with malicious emails is a very typical approach, not only to steal credentials for OSNs access, but for many other services. On the other hand, we find real users that want to bypass privacy measures and disclose information about their peers. Undoubtedly, one of the reasons that has led to the success of OSNs is the fact that users can snoop into others' profiles without being discovered. Nevertheless, in several cases the disclosed information is not considered adequate and users try to find out more.

Clearly, the information that a user shares in an OSN is not only targeted by malicious entities unrelated to the user. On the contrary, the attacker might be in the user's 'neighbourhood', thus, making defence measures more complex, and the need for customizable privacy policies imminent.

1.1. Contribution of the article

Since the attackers may be everywhere, one of the fundamental questions that arise is: 'To what risks is the user actually exposed?'. The most apparent risks involve the user's privacy, as information may be disclosed to illegitimate entities. Nevertheless, the sources of this disclosure can vary depending on the OSN. Moreover, there are other privacy concerns and risks beyond information leakages.

Managing privacy in OSNs can be viewed from two completely different perspectives that consider different attack scenarios. First, we have privacy breaches, which means that an adversary wants to find as much private information as possible, or bypass the privacy policies of her target, using the publicly available information and the infrastructure of the OSN. Secondly, we have adversaries that try to de-anonymize the datasets that are available. Although the connections between users is an extremely important part of a user's profile, the most significant is not her connections or the aggregated results of some queries, but the actually shared information. If we calculate the amount of information in terms of storage, then the greatest proportion of the shared content is multimedia.

Additionally, many researchers, mainly industrial, try to exploit OSNs, documenting their findings as bug reports. These reports are sent directly to the corresponding OSNs, some of which become publicly disclosed.

In this context, we believe that an article that categorizes the main security and privacy risks that users are exposed to is essential, not only for users and OSNs, but also for researchers. Several of these risks stem from poor implementations, some of which have been patched. However, others are the result of OSN design issues for which researchers should focus on providing secure and efficient solutions.

Since the vast amount of the shared information in OSNs is multimedia content, this article studies the security and privacy exposure that a user might suffer by sharing this kind of content within OSNs. Hence, this article provides an up-to-date categorized mapping of these risks, as currently there are many documented issues, few of which are properly addressed. For some of these issues, we discuss possible solutions and obstacles that might be faced in their implementation.

Another way to approach this work is as a risk assessment for multimedia content in OSNs. Assuming that the asset at stake is the multimedia content that users share on their OSN profiles, we try to explore the risks that it is exposed to. Therefore, we discuss what are the possible entry points that an attacker will try to use, what he will try to extract and how, what are the possible impacts of his actions and the possible remedies. Notwithstanding, since the focus of this work is on multimedia content in OSNs, the economic risk cannot be estimated. The main reason is that reports that focus on this aspect are sparse and share little if any relevant information.

1.2. Structure of the article

The rest of the article is organized as follows: The next section provides an overview of the general privacy and security risks that a user is exposed to in OSNs. Additionally, some quantification methods about users' privacy exposure within OSNs are discussed. In Section 3, we discuss the entry points that an attacker might use to launch his attacks. Section 4 discusses the privacy risks to which a user is exposed from the shared multimedia content in modern OSNs. Afterwards, in Section 5 we discuss the security risks. Section 6 discusses the possible impact of these attacks on the victims. In Section 7, we provide an overview of the most promising solutions to most of these problems and in Section 8 we discuss their cost and applicability. Additionally, we provide some tables that summarize the findings of this article. Finally, we conclude the article in Section 9.

2. RELATED WORK

2.1. Online social networks

In [1], Boyd and Ellison define OSNs as:

> web-based services that allow individuals to:
>
> (1) construct a public or semi-public profile within a bounded system;
> (2) articulate a list of other users with whom they share a connection;
> (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.

While the definition is quite close to what an OSN is commonly considered, it fails to provide the dynamic nature that an OSN

has; therefore, we argue that OSNs could be better defined as follows:

> Online Social Networks are web services that provide their users with mechanisms, subject to specific context constraints, to:
>
> (1) construct and manage the content and visibility of their profiles within their systems;
> (2) define and organize the type of connection with other users;
> (3) interact with other users, sharing content and information or even by altering their profiles.

This new definition highlights some of the key ingredients of the OSNs, their dynamic nature, the interaction, the shared content and the context, which were not highlighted in the previous one.

The success of the OSNs can be attributed to their focus on specific user interests; therefore, we have dating, professional, medical OSNs or OSNs for simple socializing. Moreover, OSNs try to strictly define the type of content that users can share, whether this is multimedia or just text-based information. In this environment, users decide to which users they are related and how, creating the corresponding groups. Depending on their privacy preferences, users define which information is accessible to which groups of users. Moreover, users are allowed to interact by exchanging messages and by contributing content to each other's profile, therefore altering it. Users may add, edit and delete their profiles and shared information whenever they want, according to their desired preferences.

2.2. Attacks on OSNs

The wide use of OSNs has piqued the interest of many researchers as well as malicious users. A wide range of attacks has already been documented targeting the users of OSNs. For the sake of completeness, a brief overview of the most important categories of the attacks, which are not related to multimedia content, is presented.

The infrastructure that is provided by OSNs allows users to communicate, share their thoughts and articles on their interests, and suggest movies, books and music and so on. This kind of data can also be used in order to extract useful information and patterns, which can predict users' behaviour and current trends. This knowledge can be used by OSNs to improve their services by offering better personalization strategies, but also by various researchers and third party applications. To enable the latter, OSNs publish anonymized and aggregated parts of their databases. This way researchers and companies may utilize the given data to find important information. However, the shared data should be anonymous in such a way that no one can infer with great certainty the identity or the attributes of a user [2]. However, as it has been shown that this is not always the case [3]. Currently, there is a lot of effort on anonymizing shared data from OSNs in order to develop more efficient and privacy-aware methods of anonymization [4–6].

The search capabilities of OSNs have been shown to be vulnerable to crawlers. Automated programmes try to reach as many profiles as possible, by utilizing the open list of connections that several profiles share. In most cases, crawlers are aimed at the contact information of the users, e.g. email addresses. Given that these email addresses were used to create OSN accounts and activate them, they are active. However, in other cases the found contacts are directly used to broadcast spam messages by using the OSN's infrastructure. Several of these attacks have been documented in the literature [7–10].

Another form of spam inside OSNs is the Group Metamorphosis [11]. Groups or Pages are communities inside OSNs for users who share specific ideas and/or interests. It has been documented that when the community has a critical mass of users, then some administrators may transform the group into a spam platform, posting things beyond the scope of the group.

Social phishing can be considered an evolution of spam attacks. In this attack, a malicious user tries to exploit the access to the victim's personal data such as personal interests or connections. Planning a phishing attack on an individual as shown in [12] has a better click-through rate than typical spamming.

Donath [13], stated something that we see very often in social networks:

> One can have, some claim, as many electronic personas as one has time and energy to create.

Sybil attacks [14] can be considered the case when a user creates multiple accounts to manipulate and affect a result as desired by him and his purpose. The goal of the adversary can vary from a simple voting scenario to a de-anonymization attack [4].

A malicious user can also launch an attack to the reputation of a user [15], usually anonymously or/and with the help of a Sybil attack. The attacker spreads, usually false, accusations about the users to draw negative 'publicity' that can hurt the victim's social image. Depending on the way in which the victim handles the situation, even if the event proves to be false, the status or the credibility of the victim can be questioned.

Finally, we find collaborative attacks. OSNs are characterized by the ease of participation, where the user involvement is very important for the success of the OSN. However, a group of many users can easily abuse this ability and demonstrate a series of coordinated reputation attacks on the content of OSNs, profiles or even whole pages. Collaborative attacks are similar to a Sybil attack, just replacing the fake accounts by users with the same goal [16].

2.3. Quantifying exposure

Liu and Terzi made the first attempt to quantify the user's privacy content risk [17].

$$\mathrm{PR}(j) = \sum_{i=1}^{n} \sum_{k=1}^{l} \beta_{ik} V(i, j, k),$$

where $V(i, j, k)$ is the visibility of user j's value for the attribute i to users who are k hops away from j and β_{ik} is the privacy sensitivity of attribute i.

Domingo-Ferrer, using the above quantification of risk, proposed protocols that assist users in making rational decisions about which attributes should be revealed to other users of an OSN [18]. The decisions are based on the utility that the disclosure of an attribute offers to the rest of the users, so that a correlated equilibrium among users is achieved. Going a step further, Domingo-Ferrer proposed the notion of co-privacy or co-operative privacy, where users co-operate into providing each other with feedback on which attributes to disclose to preserve their privacy [19]. The more someone helps others in preserving their privacy, the more his privacy is preserved. Closely related, but more focused on OSNs, is the approach of Hu *et al.* [20], which tries to provide a mechanism that addresses the identification and resolution of privacy conflicts for collaborative data sharing.

In another attempt to alert users about their exposure over OSNs, Talukder *et al.* [21] introduced Privometer. The tool is implemented for Facebook and focuses mainly on reducing the users' exposure by quantifying whether their sex preferences and political view can be infered from their posts.

3. ATTACK VECTORS

In this section, we discuss the origins of the possible attacks.

Multimedia content: It is often said that 'a picture is worth a thousand words' in order to show the vast amount of information an image can have. Modern OSNs store numerous multimedia files on a daily basis, contributing even more information when fused. Furthermore, users share many multimedia files containing sensitive and personal content. Therefore, the multimedia files themselves can be considered a threat to the user.

Malware: Malware, intended to harm users or their computers, can be used to launch an attack. For instance keyloggers, ransomware and other malicious software can be used to exploit vulnerabilities of the user's operating system to leak sensitive information to the attacker.

Misplaced Trust: In OSNs it is not always clear whether a user should trust another, especially due to the anonymous nature of the Internet. Without any verification on identity, people use a naïve approach, by checking information such as profile picture or common friends, before trusting others. This approach just requires a little effort from the adversary side to effectively attack his target. Adding an imposter to the friend list gives him access to much of information and multimedia content that is meant only for trusted users.

Phishing: Phishing is considered a social engineering attack. When an adversary is 'phishing', he sets a legitimate-looking website or email, pretending to represent a legitimate and credible entity that the victim trusts. In the legitimate-looking website the adversary tries to steal the credentials of the victims for the targeted service, for example e-banking, email or OSN account. If the victim falls in the trap, his account is compromised.

Hijacking: An account on OSN is considered hijacked when an attacker breaks into the account and impersonates the owner usually to run a scam or to harm his reputation.

URL redirection: A shortened URL is a short domain name followed by a short unique string that is linked to a long URL. Shortened URLs became very common with the launch of services such as Twitter, which limit the length of the message. The true destination of a shortened URL cannot be determined visually or even by looking at the source code of the webpage; therefore, the user could end up in a legitimate web page, but he could also be led to scams, malicious sites or other sites that he did not intend to visit.

Lack of Policies: Unfortunately, OSNs do not have policies to govern every possible privacy issue or to allow fine-grained user customization. Owing to the wide range of possible scenarios of human interaction, this can be exploited by malicious users. Moreover, as is going to be discussed, often several events, such as content re-uploading, are not handled by any OSN policy, exposing users greatly.

Platform vulnerabilities: OSNs are software platforms and, as often with software, there are bugs that an adversary can exploit to gain access, bypassing users' privacy settings to steal personal data.[1]

Open access: Modern OSNs are based on the 'freemium' model and allow users to register quite easily, as authentication is mainly dependent on email messages to other 'freemium' services. This loophole allows users to exploit it, creating multiple and false accounts. It is estimated that between 5.5 and 11.2% of Facebook accounts are fake.[2] Therefore, malicious users can easily launch their attacks anonymously.

4. PRIVACY ISSUES

Privacy is a fundamental human right,[3] which in many cases is treated as a product from OSNs, as their mass source of

[1] http://www.neowin.net/news/facebook-photo-exploit-allows-you-to-view-any-albums-of-non-friends.

[2] http://investor.fb.com/secfiling.cfm?filingid=1326801-14-7&CIK=1326801.

[3] Universal Declaration of Human Rights—Article 12 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.

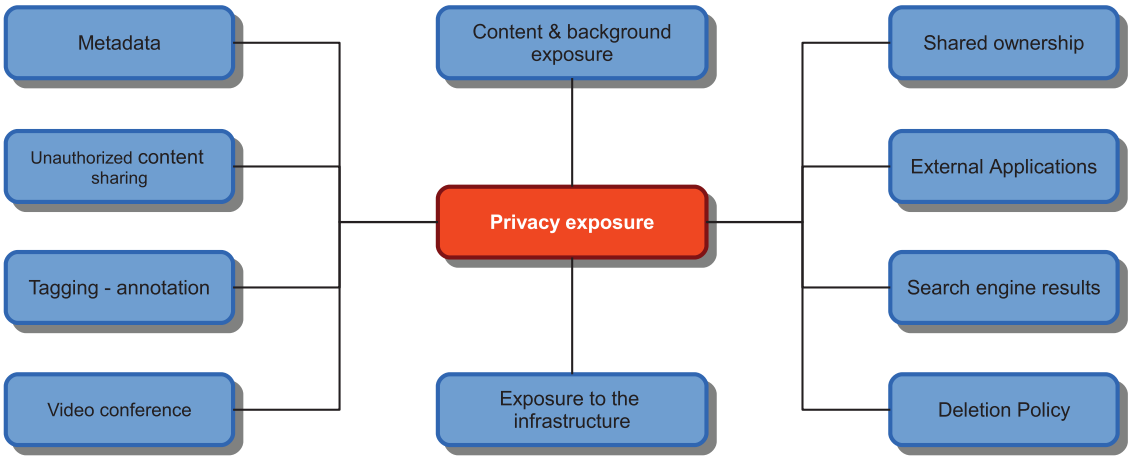

FIGURE 1. Privacy exposure categories.

income derives from selling users' preferences to advertising companies. Since this has been documented in the end-user licence agreement, it can be considered that users agree to this policy, even if fairer models do exist [22, 23].

Houghes [24] defines privacy as follows:

> Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

However, the ability to fuse information from different sources, even heterogeneous, makes the quest for privacy a rather difficult task in today's interconnected world. OSNs may provide a lot of information about users, using as their source the feedback and interaction of other users. Nevertheless, since users share huge amounts of multimedia in their profiles, a lot of information can be leaked and they can be exposed to great privacy risks without being aware of this fact. In an attempt to document their users' privacy exposure due to multimedia sharing, we have categorized and analysed them. A visual representation of these categories is depicted in Fig. 1.

4.1. Content and background exposure

Users are usually careful when disclosing textual information over social networks. Therefore, there are very few people sharing their home address or their IDs in OSNs. In contrast, people are not that cautious when it comes to sharing multimedia content, revealing a lot of sensitive information. A typical example might be that users will share photographs of their houses, and in many cases their address can be inferred. In other cases, people tweet or post status updates, indicating that they are away from home, e.g. concert, bar, vacations, etc., which is more or less indicating that the house is 'open' to burglars.[4]

[4] http://www.pleaserobme.com.

An uploaded photo from the current activity can indicate the user location and the duration of his stay, providing additional advantages to the intruders.

In the same context, users have to be aware that burglars may scan the shared pictures for valuable assets. Hence valuable objects depicted in photos or videos can trigger unwanted attention from burglars. Even if the users do not have a direct reference to the date and time of the shared photo or video, several estimations can be made, using background information ranging from the sun's location and measuring shadow lengths, or newspapers and people's activity.

In addition to the above, we can find other forms of privacy exposures, which may include the user or other entities, like a photograph that contains other people. A user may upload this photograph without the consent of others who are present in the photograph and without any notification to them. Depending on the content of the photograph, other users' privacy can be violated or they can be socially discriminated for being caught at the wrong place, at the wrong time. Modern techniques using face and speech recognition can expose many people without their consent or any form of notification, i.e. using them in uploaded videos and photographs from public protests, when people share them without anonymizing them on their profiles.

Moreover, user profiling can easily be achieved from the shared content and a lot of sensitive information can be deduced as shown in [25].

4.2. Metadata

One could define metadata as data about data. The reason why they are very useful is because they contain additional information about data, and so they can be more easily consumed by applications. Especially multimedia content files they contain a lot of information. While, this information might be very useful for the user, it might expose him if it is shared.

A typical example of such metadata that can expose users are geolocation tags. Many modern smartphones embed the GPS coordinates in the captured images metadata, which is even more accurate than a street address. This information is rather sensitive as apart from the aforementioned risks, the user's location may disclose many more things about the user, e.g. medical condition, political or religious beliefs etc. Unfortunately, as events have shown, geotagged images may lead even to human casualties.[5] Other image metadata may indicate which camera was used to capture the picture, disclosing its owner and therefore previously unknown connections between users.

Depending on the OSN, the metadata are treated differently.[6] Facebook, for example, erases all metadata, while Google+ keeps them, considering as sensitive information only the GPS coordinates and prompts users to answer whether they would agree to share them. On the other hand, VKontact[7] by default uses the GPS coordinates to tag the location and uses it to show other users photos from the same location.

4.3. Unauthorized content sharing

Sharing content in OSNs means disclosing this information to a certain set of users, which varies according to the user's preferences. If a user shares text information with a group and a member discloses it, then, generally, it cannot be considered valid as it can be easily manipulated. While multimedia content is malleable, if the changes are not made by "professionals", they can easily be traced. Therefore, disclosure of multimedia content is a very tricky issue.

A user may decide to share an image to a predefined group of users; however, this does not stop members of the groups from bypassing the user's privacy settings. Every member of the group can download the shared image and re-upload it based on his new privacy settings. In this way, an image that the first uploader intended to show to a restricted group can be easily made public. Additionally, this action is not only allowed by current OSNs, but the original user may not become aware of it.

4.4. Tagging: annotation

Apart from the multimedia metadata, OSNs use tagging in the shared multimedia content to allow more fine-grained search results and interaction between users. Users have the right to tag images and videos with the tags that they find appropriate, probably linking them with some additional information. This, however, introduces some privacy issues. First, there are several users who do not wish to be visually identified, so they do not upload any picture of themselves. However, their contacts can upload such photographs and, through tagging, identify other users. An extension of the latter is that tagging may allow linking to people who are not members of any OSN and do not wish to publish any of their information.

4.5. Video conference

Thousands of people use OSNs to communicate with others; apart from chat services, many OSNs, such as Facebook, have started supporting video conferences. While this might allow more interaction between users, the problem that arises is that more information can be leaked.

Depending on the underlying protocol, the broadcast stream could be intercepted. Nevertheless, the conference could be easily stored by one of the involved parties to either extort the victim or to manipulate the content and present it accordingly. Additionally, possible vulnerabilities in the protocol, or malware could allow the attacker to arbitrarily access the camera and microphone of the victim without notification.

Experimenting with the latest feature of Facebook to support videoconferences, the authors managed to discover another information leak. Since Facebook is using a plugin from Skype to support the video conferences, not all platforms are currently been supported. Therefore, if someone requests a video conference from the other participant, judging on whether the conference can be initiated or not, the use of Windows-based machines can be deduced. While this may be considered minor, it can be escalated afterwards. If the videoconference initializes, then using the log files, each party can see the other's IP address. If their IPs are not spoofed, e.g. through proxies, something which is a valid assumption for the vast majority of users, then their location is disclosed with great precision, using off-the-shelf software solutions.[8]

4.6. Shared ownership

Multimedia content files, for several reasons, may belong to more than one user. A typical example is the case of two friends who agree to take a photograph together at a social meeting in order to remember the moment. They agree to take the photograph with one of the cameras. Such a photograph should belong to both users; however, co-ownership of the content is not possible at the moment in OSNs. The privacy exposure stems from the fact that only one of the users can set his preferred privacy settings; therefore the content can be distributed only with the policies that one of the users has selected and not with the intersection of their preferences, which would be fairer.

4.7. External applications

OSNs have enabled the development of external applications, to enrich user interaction and engage their users even more.

[5] http://www.bbc.co.uk/news/technology-17311702.
[6] http://www.embeddedmetadata.org/social-media-test-results.php.
[7] http://www.vk.com.
[8] http://www.visualroute.com/.

Malicious applications can be developed [26]. However, other privacy issues are relevant. In the case of Facebook, for example, external developers have created many applications, some of which are very profitable. By installing such applications in many cases users agree to share all their multimedia content, and other data, with the developer. According to the Facebook Terms of Service:

> When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you.

In other words, the application developer is entitled to use shared content from the user's friends, which is something that in most cases can violate the other users' privacy settings. Moreover, in the vast majority of OSNs, the platform is trusting all third party developers, in the sense that their applications will not be malicious, introducing other security issues. However, trust can be considered only theoretical, as there is no restriction on who is allowed to develop an application and the restrictions cannot be enforced, except through litigation related to their Terms of Service agreement.

4.8. Search engine results

Nowadays, many OSNs allow search engines to mine parts of their databases. This functionality is very important, given the amount of information and knowledge that is shared within OSNs. On top of providing OSNs with more recognition, allowing the execution of search engines' queries, an informal link between OSNs can be created. Typically, most OSNs disregard other OSNs and treat them as a completely different ecosystem. While the latter might be correct to some extent, the reality is that since users have many profiles in different OSNs, search engines provide them with an insight into what is happening within other OSNs, to which they are not registered.

While this functionality is very useful, it opens a back door for the users' privacy. The reason is that it allows the activity of registered users within one OSN to become available not only within one OSN, but also to the whole Internet. Therefore, poor privacy policies of a user or even of one of his connections can expose him to the whole Internet.

4.9. Deletion policy

The main source of income for most OSNs is the shared content from their users. Based on the provided information, OSNs can mine for proper profiles and create very specific subsets of users for targeted advertisement. Allowing people to remove information from their profiles is similar to allowing users to remove income from OSNs. Therefore, many OSNs either prohibit users from removing shared content, or they provide the facility with some obstacles (time frames, i.e. a photo will not be immediately removed, i.e. users have to pay to remove content,[9] etc.).

It has to be highlighted that, in everyday living, privacy is achieved not just through non-disclosure. For instance, due to human nature, we are unable to effectively disparate information sources without automation. This results in mixing facts and events, obfuscating the underlying links. Additionally, people tend to forget many things in their everyday lives. Therefore, information about several events cannot be fused to disclose some private information. Moreover, many currently disclosed events might seem trivial, but years later they can be linked to infer something else.

Given that shared information in OSNs does not have expiry dates, unified deletion policies raise a very critical privacy issue: Are the users entitled to be forgotten? If so, under which conditions? The problem is very significant for multimedia content, which contains even more information and accounts for the biggest part of shared information. It becomes apparent that in retrospect users would like to delete much of their content, e.g. funny pictures and videos from their past, with old friends and partners.

4.10. Exposure to the infrastructure

Apart from all the aforementioned privacy risks, there is one more, which might be very obvious, and yet, depending on the OSN, it might have many implications and this is the exposure of the user to the infrastructure. The vast majority of OSNs have the targeted advertisement as their main source of income. This means that they have to mine user-submitted information and fuse it with other information to get more fine-grained results that profile users according to their preferences, beliefs, etc. and by which especially multimedia content can be used to provide even more fine-grained results.

Owing to the recent disclosure about the role of secret agencies in the Internet,[10] the issue becomes even thornier. While this might be a temporary hype, users' private data are greatly exposed to the service provider. For health- and medical-related OSNs this is understandable, but the case is the same for the remaining OSNs, e.g. disclosure of events from Facebook have led to many divorces.[11]

The situation becomes more complicated by the terms of use of many of the service providers. For example, for Google Plus, which is part of the Google services we have that:

> When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate,

[9] http://www.medhelp.org/termsofuse.htm.
[10] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[11] http://www.zdnet.com/blog/facebook/facebook-blamed-for-1-in-5-divorces-in-the-us/359.

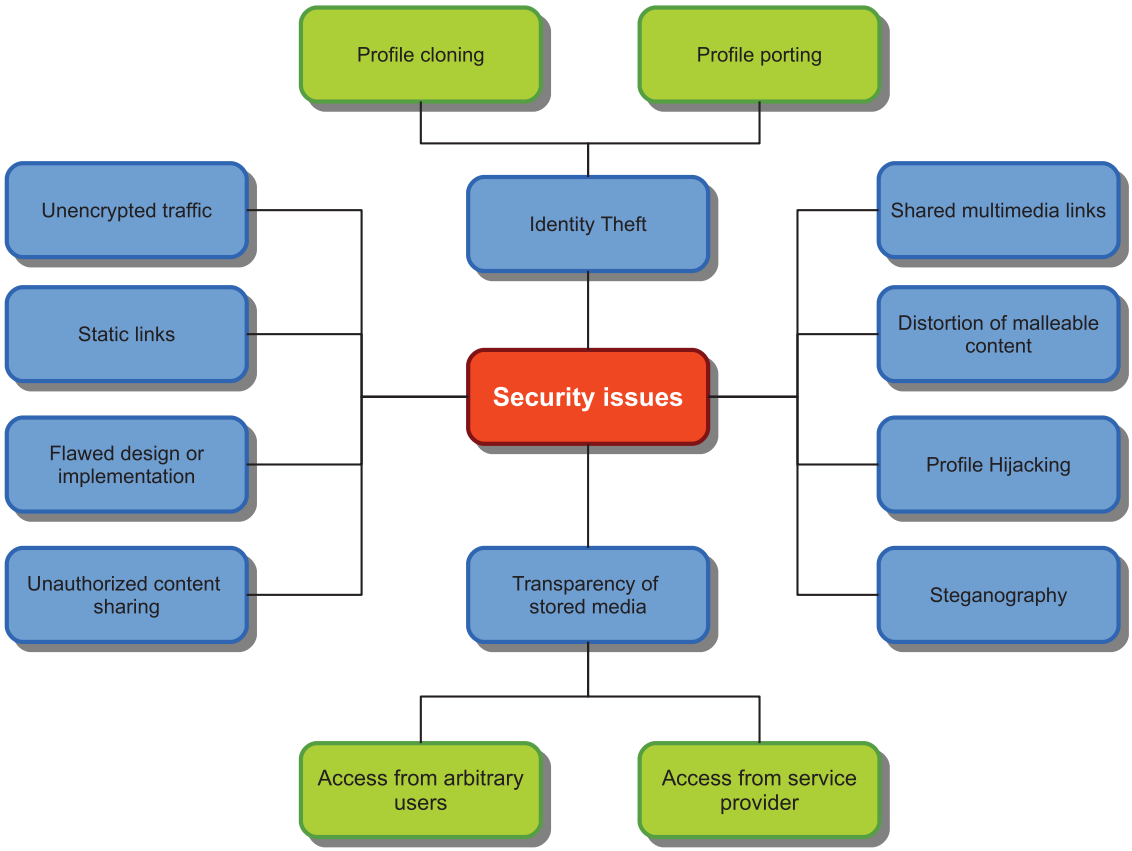

FIGURE 2. Security issues.

publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

In this context, many could argue that user-submitted photos can be published and modified without their knowledge, worldwide, by other non-specifically defined entities without users being able to remove them. Of course, many companies have tried to generalize and simplify the content of their terms of use licenses, nevertheless, such wordings can prove to be double-edged swords, as they open back doors with regard to users' privacy from the service, but to malicious employees as well.

5. SECURITY ISSUES

Apart from privacy issues, which are the first to arise in OSNs, there are also many security issues as well, many of which stem from the use of the shared multimedia content. The security risks to which a user is exposed to from the use of multimedia in OSNs is depicted in Fig. 2.

5.1. Unencrypted traffic

In light of the rise of many tools such as Firesheep[12] that clearly expose the vulnerabilities of plaintext traffic, by intercepting and highjacking user sessions, many OSNs were forced to shift their whole traffic to encrypted, via SSL. Nevertheless, many OSNs are still using unencrypted connections with their users.[13,14] The issue is very serious given that many of these OSNs are related to medical and health issues. It is reported that either they are still using standard unencrypted http connections or they are using SSL just to send user credentials [27, 28]. The sensitive nature of the shared content, as in such networks users may upload scanned versions of their medical exams, makes

[12] http://codebutler.github.io/firesheep/.

[13] http://www.motherjones.com/politics/2013/05/shutterfly-teamsnap-eteamz-ssl-hackers-kids-data.

[14] The Electronic Frontier Foundation had already warned the Council of Europe for the lack of SSL adoption from OSNs and the impact to the privacy of their users (https://www.eff.org/node/58437).

the use of unencrypted traffic a huge security vulnerability that opens the door to a wide range of attacks.

5.2. Static links

The vast majority of OSNs are using static links to access multimedia content. While this policy might be optimal for the case of content distribution, in terms of efficiency, it is certainly not in terms of security and privacy, as it opens a back door to many attacks. By sharing static links, OSNs provide users with a mechanism to bypass their privacy and security measures. If a user shares an image to a restricted group and it is statically linked, then every user that has access to it can share it without any other permission. Even more, users can copy and paste the link to share the content beyond the OSN. While the static links may look random, they are not, and several bugs have been reported allowing people to brute-force such links to recover other multimedia content[15] of the same or other users. Quite interestingly, in many OSN infrastructures, the link to deleted content may remain for several days after the user deletion request. Finally, this policy allows network administrators to be able to see what users are browsing without any effort, as this content is available in their log files.

5.3. Flawed design/implementation

As everything done by humans is expected to have flaws, OSNs do have bugs. The problem is how much can this expose users, how easily can they be exploited and how much effort is needed to trace them. In many cases[16] this can be easily achieved using the shared multimedia content. Targeted attacks can be made on the shared multimedia content from groups of users (real or bots) to disable user accounts [16]. The importance of the aforementioned attack is that many users do not use their real names but nicknames, which indirectly bypass the terms of service of several OSNs, thus their accounts are either disabled or they have to disclose more information, e.g. their real identity, residence, etc. to take back control of their account.

5.4. Transparency of stored media

A big issue that is strongly related to static links is the transparency of stored media, which can be understood in two ways. First, the stored multimedia contents are not encrypted; therefore, if someone has a direct link to them, they can be accessed without the use of any credentials, bypassing any privacy or security policies set by the user or the OSN. Secondly, there is the transparency towards the service provider. Big OSNs such as Facebook or Google+ might have their own data centres, nevertheless, smaller ones do not have this luxury, so they resort to outsourcing their data centres using virtualization or cloud-based technologies. These technologies might reduce scalability and maintenance costs. However, many concerns arise regarding their provided security.[17,18] In any case, the end-user might trust the OSN, but not the cloud service provider which has access to his data.[19] The issue becomes even more thorny due to geospatial and political constraints. Governments and agencies may be granted arbitrary access to foreign citizens' multimedia content without their approval or any kind of notification, as the data centres that host this information do not belong to the same country or even continent.

5.5. Profile Hijacking

This category involves all the attacks where a malicious user tries to take control of another user's profile. This can be achieved in many ways such as brute-force attacks, phishing or social engineering. Since a picture is worth a thousand words, the shared multimedia content may provide the attacker insight into the user's password. Special crafted tools such as CUPP (Common User Passwords Profiler),[20] given the proper input, can provide a very good dictionary for possible user passwords. Additionally, the shared multimedia content must not disclose under any circumstances any information regarding the security questions to any of the users' accounts or other service providers.

5.6. Identity theft

In many attack scenarios a malicious user might not be interested in taking over the account of a user, as in the aforementioned attack, but in misleading other users that he is another user. The attacker tries to masquerade as a legitimate credible user, targeting to cause reputational damage, or to exploit the trust that other users have in his authority and obtain money or credit. By replicating a user's multimedia content from OSNs, especially images, this effort can be achieved more easily. The nature of OSNs can enable malicious users to automate such attacks [29]. Fraudsters can also deduce a lot of information to use in their attack from the shared multimedia content on OSNs. A naï example involves disclosing the date of birth of a user and close connections from a picture of a birthday cake from a user's party. Moreover, since the shared multimedia contents are usually of high quality, they can be used to launch attacks in real life, e.g. print fake ID cards or company passes.

If the attack takes place not in the real world but in the cyberworld, then identity theft can be further categorized to profile cloning and profile porting. In the first case, the attacker

[15] http://www.neowin.net/news/facebook-photo-exploit-allows-you-to-view-any-albums-of-non-friends.

[16] http://www.zdnet.com/blog/btl/facebook-acknowledges-photo-privacy-bug-issues-immediate-fix/64819.

[17] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[18] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[19] http://slashdot.org/topic/bi/the-windows-flaw-that-cracks-amazon-web-services/.

[20] http://www.remote-exploit.org/articles/misc_research_amp_code/index.html.

creates an identical copy of the victim's profile, expecting other users to be misled and connect with the malicious profile. In the latter case, however, the attack is more stealthy, as in profile porting the victim does not have an account on the OSN which is used by the attacker, making it more difficult to take precautionary measures.

The Identity Fraud Report of 2013[21] by Javelin Strategy & Research indicates that within the USA alone, 12.6 million consumers, 5.26% of U.S adults, were affected in 2012. These attacks enabled fraudsters to steal more than $21 billion in 2012.

5.7. Distortion of malleable content

While users share vast amounts of multimedia content, they know that a lot of the shared content is malleable. Currently, there is a wide range of powerful tools available to users for image or audio processing. If someone wants to ridicule or harm someone, then personal photographs, for example, can be tampered with, to provide an image that is real looking, as most of the shared content has high resolution. Such tampering is more or less expected for photos; however, new OSNs such as hubbub[22] could be an audio source for attackers.

5.8. Shared multimedia links

Owing to the wide range of multimedia formats, it is almost impossible for one framework to support them all. Additionally, since many formats might be vulnerable to attacks, or they may have content that needs to be manually checked (e.g. interactive flash videos), or even multimedia content that is embedded in other web pages, OSNs do not let users share arbitrary multimedia files. For example, pictures can be shared in PNG and JPEG format, GIFs are not widely supported as they may contain animation. However, users still want to share multimedia content and post links to external content, something that many malicious entities try to exploit. Given that users are redirected, with their consent, outside the OS, they can be easily tricked into installing malicious codecs (i.e. using clickjacking techniques) or visiting sites that perform cross side scripting (XSS) attacks which attempt to steal client cookies, highjack sessions, etc. Moreover, since the links are static and users are redirected, one could change the content of the initial page, either to maliciously redirect users or to harm the social image of the users who shared it.

5.9. Steganography

For centuries people have been hiding information in other media in order not only to hide the content, but to hide its existence as well. The technological advances of the last century have enabled researchers to transform this art, steganography, into a science, which has many legitimate applications. Nevertheless, its ability to cover malicious activities can be used within OSNs. Multimedia content, due to their size, can be used as cover objects.

In [30], the authors illustrate a clear example of a communication protocol between users using photographs uploaded to OSNs with embedded messages, illustrating not only that this is possible, but additionally the overhead is affordable. While the aforementioned work is focused on providing users with more privacy, it nevertheless indicates that this can be exploited by malicious users. Therefore, the embedded messages can range from terrorist messages to child pornography.

Given the nature of the exchanged messages, on the one hand, we have an OSN whose reputation can be jeopardized and, on the other hand, we have legitimate users who can end up being associated with uncommitted crimes, e.g. someone downloads and shares a photo that he likes from another profile, without being aware that it is a cover object. It becomes apparent that OSNs and users are exposed to such risks, by hosting and sharing, respectively, multimedia content within OSNs.

6. IMPACT

In this section, we summarize the possible impact of the aforementioned attacks.

Information Leakage. While users may regard information exposure as a feature, since theoretically they are the ones who dictate which information is exposed, this is not always the case. Given the amount of multimedia information that is shared, a lot of sensitive information can be inferred with great accuracy [31] or through data fusion with other users [32].

Location Awareness. Providing location information to a service can be very helpful in many cases; for instance, by using the GPS service a map can direct you to the nearest gas station. However, this information may also lead to serious privacy breaches. A location-aware OSN allows user's contacts to infer his whereabouts. Trivial information, such as revealing that someone is not currently at his place, can be translated into an invitation to burglars.[23]

Reputation. A person's or company's reputation can be the target of an adversary. Especially for companies, reputation is a valuable asset and needs to keep track of such attacks in order to protect itself.

Account loss. Depending on the nature of the attack, the user might suffer from either having his account locked or even losing it.

[21] https://www.javelinstrategy.com/brochure/276.
[22] http://hubbub.fm/.
[23] http://www.pleaserobme.com/.

Loss of ownership/control of content. When a user submits content to OSNs, even more when it is multimedia content, it is very difficult to predict who may download this content and how it will be shared or republished. Therefore, unauthorized sharing or loss of user's multimedia content, can expose him to great privacy risks without any notification. Malicious users can potentially use this content to steal someone else's identity. While an OSN user profile can be used as an authentication tool for many reasons and mainly for online collaborative activities, discussions, etc., the malicious use of multimedia content in combination with personal information, collected through social engineering, can cause the temporary or the complete loss of control on his online content.

Blackmailing/extortion. Depending on the content that a malicious user has gained access to, the victim might be blackmailed. A lot of shared multimedia content in OSNs is shared from users believing that it will not be leaked to unauthorized users. This trust makes them share a lot of sensitive or even embarrassing content, which, if leaked, can be used as a threat. The threats, depending on the attacker, can impact his economic, social or even personal status.

Cyberbullying. Cyberbullying happens when a teen or a child is threatened, humiliated, harassed or in other words targeted with a malicious purpose by another teen or child, using the Internet. As it becomes apparent, cyberbullying is dependent on the use of OSNs. The problem is quite serious as in several cases it has lead teenagers to extreme acts of violence.

Cyberstalking. A malicious user can use the OSN platform to stalk his victims through the Internet. From the shared content on OSNs, an adversary can infer the victim's beliefs (political, religious, etc.), his whereabouts, his preferences and daily habits. All this information could be used to stalk or harass the victim in real-life attacks [33].

7. POSSIBLE COUNTERMEASURES

7.1. Watermarking

Digital watermarking is the process of embedding information into media in order to prove the ownership of the content. In contrast to steganography whose purpose is the secret communication between trusted entities, watermarking can be visible or invisible and can be traced. Visible watermarks are visibly meaningful patterns, such as a logo of a company embedded in the image that is published. While visible watermarks are difficult to remove, they tend to cover the bulk of the image, noticeably degrading its quality. An example of visible watermarks used in OSNs is the dating site Badoo.[24] On the other hand, invisible watermarking provides techniques so that the quality of the medium remains very high, as the distortion is minimal, while the information is still embedded. Moreover, depending on the application needs, invisible watermarks can be robust, fragile or semi-fragile. Robust watermarks provide the mechanisms such that after common signal processing or malicious attacks, the information can still be retrieved. Fragile watermarks 'break' after any signal processing and cannot be authenticated. Semi-fragile watermarks are a hybrid of the aforementioned, usually applied in tamper detection schemes [34]. In any of these cases, the watermark scheme has to offer enough capacity to store the selected type of watermark. The minimum capacity, that is required, can range from 1 bit, in copy control application, to 44 bits for a 13-digit number, as an ISBN number for copyright application, or even a whole photograph.

Zigomitros *et al.* [35] provide some experimental results that indicate that the most popular OSNs do not apply any invisible watermark to secure their users. Moreover, in their work they propose a framework that uses dual watermarks, which allows users to apply more fine-grained privacy policies within OSNs. The scheme is illustrated in Fig. 3. Briefly, User A uploads a multimedia file that is watermarked with a dual watermark, one robust and one semi-fragile, containing information such as UserID, mediaID, timestamp, etc. The existence of the watermark allows an OSN to trace many events such as other users re-uploading the same image or modifications of it. Therefore, according to the user's settings, the OSN can choose if the information can be uploaded and provide the user with the necessary notifications.

Clearly, the proposed scheme can counter many of the discussed privacy or security attacks related to multimedia content, such as unauthorized content sharing, shared ownership and identity theft. What is important is that users can receive alerts of possible attacks and define more fine-grained security policies.

7.2. Encryption of transmitted media

As discussed is Section 5, several OSNs are either not encrypting their traffic or are partially using SSL. The need for using SSL encrypted traffic for all their interactions is undeniable, as well as the use of secure cookie policies in order to provide the minimum level of security and privacy to their users. In this way, users have a guarantee that when uploading or downloading multimedia content, this content will not be intercepted.

7.3. Storage encryption

As discussed in Section 4, the multimedia content that users are sharing in many cases can be stored in data centres that are not owned by the OSN, and geospatial or political events may

[24] http://www.badoo.com.

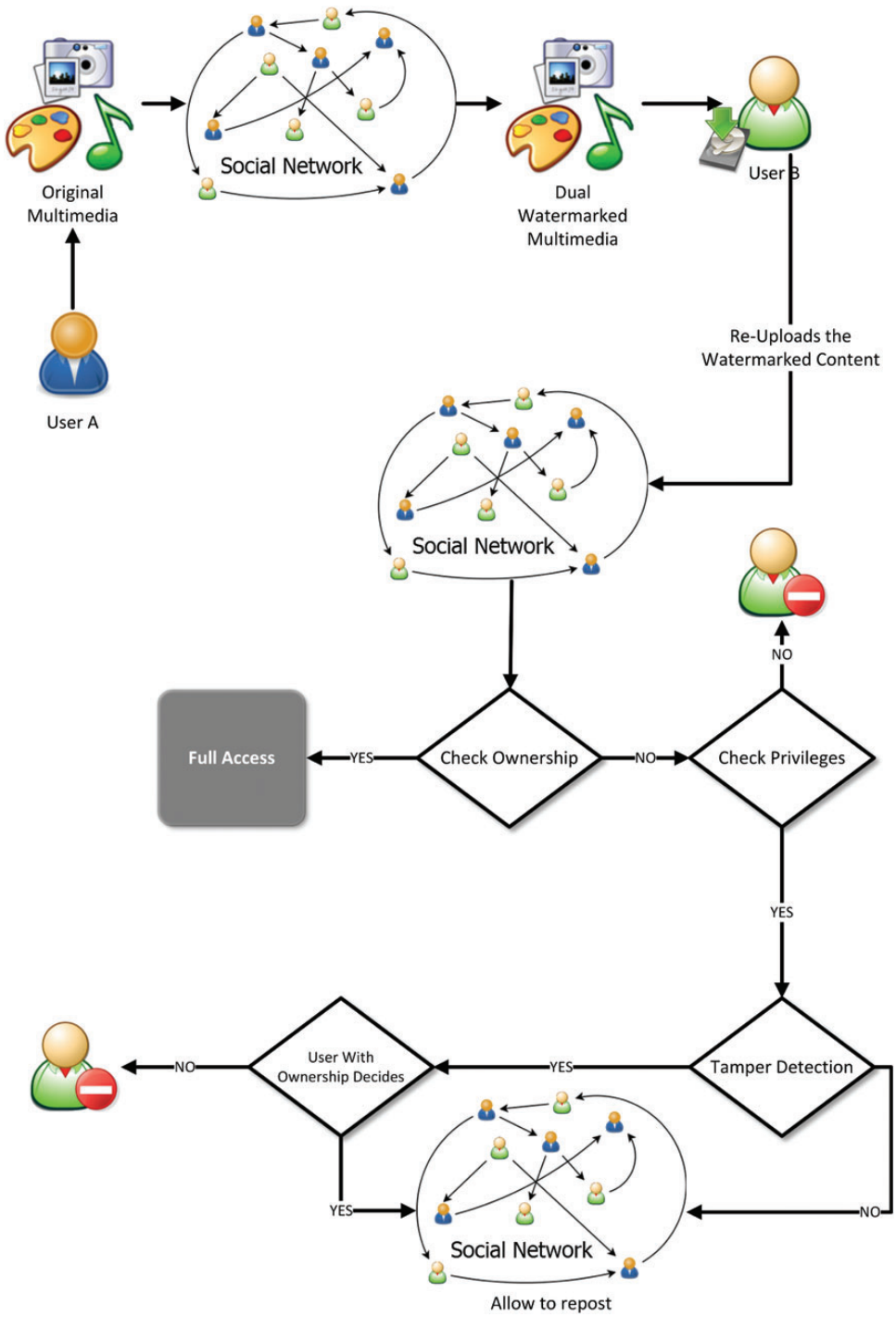

FIGURE 3. Watermarking scheme.

expose a lot of users to agencies without their will or any type of notification. The issue is very important given that there are currently many health and medical-related OSNs and the shared information is very sensitive. Therefore, whether the user has to be protected from foreign agencies, malicious providers or developers working for the providers, their data should be stored encrypted. There are many cryptographic solutions, mainly based on public-key algorithms, which can provide users of OSNs with the required functionality to store and efficiently recover their users' files, without leaking any information to

TABLE 1. Privacy and security risks and their solutions.

	Watermarking	Encryption of transmitted media	Storage encryption	Steganalysis	Co-ownership	Dynamic links to content	Metadata and background removal	Digital oblivion
Privacy issues								
Content and background exposure							✓	✓
Metadata							✓	
Unauthorized content sharing	✓	✓	✓			✓		
Tagging—annotation					✓			
Video conference		✓						
Shared ownership					✓			
External applications		✓						
Search engine results		✓	✓				✓	
Deletion policy								✓
Exposure to the infrastructure			✓					
Security issues								
Unencrypted traffic		✓						
Static links			✓			✓		
Flawed design/implementation								
Transparency of stored media			✓					
Profile Hijacking		✓						
Identity theft	✓						✓	
Distortion of malleable content	✓							
Shared multimedia links								✓
Steganography				✓				

the cloud service provider [36–38]. Additionally, proxy re-encryption-based schemes [39] can guarantee that the users' information will not be leaked within the OSN infrastructure.

Another approach, more focused on multimedia, would be the encryption of the multimedia content. While the previous methodology provides arbitrary encryption of data, there exist more focused solutions such as [40]. The advantage of such solutions is that even if someone manages to get a direct link to the shared multimedia content, the content will not be available, unless the user holds the proper decryption key.

7.4. Steganalysis

Modern cameras and OSNs enable users to upload high-resolution images, which are large files without raising any suspicions. However, as previously discussed, they can be used as cover objects to distribute malicious content. Therefore, the use of steganalytic software on user multimedia content is considered essential. Experiments conducted by the authors indicate that such mechanisms do not seem to exist currently in the bulk of major OSNs, or at least their output is not reported to the user. Many OSNs, such as Facebook, may forbid users to use such methods in their terms of service; however, they do not seem to block such actions, something that can be exploited. A typical example of the latter is SecretBook,[25] a Chrome extension that allows users to exchange secret messages within Facebook, through steganographic methods.

7.5. Co-ownership

To allow users to apply privacy settings, which are closer to their preferences and real-life scenarios, OSNs should apply co-ownership models [41, 42]. Such models could allow more than one user to enforce their privacy policies on the co-owned photos, videos, etc., so that the permissions and restrictions on media are not dictated by the choices of one user and the privacy of all involved users is respected.

7.6. Dynamic links to content

As highlighted in Section 5, the use of static links exposes users to many risks. Given that the aforementioned solutions,

[25] https://chrome.google.com/webstore/detail/secretbook/plglafijddgpenmohgiemalpcfgjjbph.

which are based on encryption, might be very demanding in terms of processing, dynamic links should be used to allow users to access multimedia content. For instance, by creating dynamic links to photographs when they are requested, that are subject to the time of the request, the IP and MAC of the user and his credentials, arbitrary access to content by users within and beyond the OSN could be minimized. The cost of such solutions can be considered minimal as they involve encryption and decryption of small texts.

7.7. Metadata and background removal

While many OSNs provide tools to embellish the shared photographs, from simple cropping to applying filters, they do not provide additional functionalities that could help in giving additional privacy to other people. Typical examples are photos from public demonstrations that are uploaded, disclosing the location and political or even religious beliefs of many people. OSNs could provide the functionality for automated detection and removal of faces through, e.g. blurring, while keeping the necessary information intact. The same functionality could be extended to blurring objects in the background in case the user is interested in hiding some background context.

Additionally, given that not all OSNs follow the same policy toward metadata, all uploaded multimedia files should be stripped of the embedded data, unless the user indicates that some of it should be disclosed.

7.8. Digital oblivion

In an attempt to offer digital oblivion, several solutions have been proposed. Mayer-Schönberger [43] argues that the use of expiration dates is enough to enforce digital forgetting. Moreover, he proposes the implementation of storage devices that can store information with a predetermined limited lifetime, so that after the lapse of that time frame, the information is automatically deleted.

X-pire! [44] is a software solution whose aim is to allow OSNs' users to store their photos along with an expiration date, after which the images can no longer be accessed.

Another approach in which cryptographic primitives are used is proposed in [45]. Using public-key locally decodable codes, the author proposes the gradual decay of the content from a trusted server, so that after a certain point in time, or after a certain usage, the content cannot be correctly decrypted and therefore becomes inaccessible.

Domingo-Ferrer [46] proposes a set of protocols where the content creator embeds an expiration date in the content, publishes it and can trace whether someone is using and/or transferring the content after the expiration date. To achieve this, each asset is fingerprinted and the protocols force each entity to co-operate in order to apply the protocol to other assets, as by doing so, they know that they are indirectly helping themselves.

TABLE 2. Security and privacy issues.

	Privacy related risk	Security related risk
De-anonymization of OSN	✓	
Spam		✓
Social phishing	✓	✓
Sybil attack	*	✓
Attacks on reputation and trust	*	✓
Collaborative attack	*	✓
Content and background exposure	✓	
Metadata	✓	
Unauthorized content sharing	✓	
Tagging—annotation	✓	
Video conference	✓	
Shared ownership	✓	
External applications	✓	✓
Search engine results	✓	
Deletion policy	✓	
Exposure to the infrastructure	✓	
Unencrypted traffic		✓
Static links		✓
Flawed design/implementation		✓
Transparency of stored media		✓
Profile Hijacking	*	✓
Identity theft	*	✓
Distortion of malleable content	✓	
Shared multimedia links		✓
Steganography		✓

*Denotes the existence of security/privacy threat with an extension of the attack.

Finally, an approach that targets OSNs, but does not depend on their collaboration, is proposed in [47]. The authors propose the use of a P2P agent community, where the agents negotiate each time which content should be 'forgotten' and the content becomes invisible to the users of the OSN.

8. DISCUSSION

OSNs and their users are currently exposed to many risks. An aggregated overview of the risks that stem from sharing multimedia content is illustrated in Table 2. It is quite clear that the vast amount of possible threats stems from the way that multimedia content is shared within OSNs. In Table 3, we illustrate the possible impact that the privacy and security attacks can have on the victim, while Table 4 illustrates their difficulty and nature.

One could argue that most of these attacks could be dealt with very well-known solutions. Surely, encryption or digital watermarks, to name two, cannot be considered novelties; nevertheless, the fact that they are not being used as much as

TABLE 3. Attack impact.

	Information leakage	Location awareness	Reputation	Account loss	Ownership loss	Blackmail extorsion	Cyberbullying	Cyberstalking
Privacy issues								
Content and background exposure	✓	✓	✓				✓	✓
Metadata	✓	✓						✓
Unauthorized content sharing	✓	✓	✓		✓	✓	✓	✓
Tagging—annotation	✓	✓	✓				✓	✓
Video conference	✓	✓	✓			✓	✓	
Shared ownership					✓			
External applications	✓	✓		✓	✓			
Search engine results	✓		✓		✓		✓	✓
Deletion policy	✓		✓		✓			
Exposure to the infrastructure	✓				✓			
Security issues								
Unencrypted traffic	✓	✓	✓	✓				✓
Static links	✓							
Flawed design/implementation	✓	✓		✓	✓			✓
Transparency of stored media	✓		✓		✓			
Profile Hijacking	✓		✓	✓	✓		✓	
Identity theft			✓		✓		✓	
Distortion of malleable content			✓				✓	
Shared multimedia links			✓	✓				
Steganography			✓					

TABLE 4. Difficulty and nature of attack.

	Difficulty	Automated	Manual
Privacy issues			
Content and background exposure	Low		✓
Metadata	Low	✓	
Unauthorized content sharing	Low		✓
Tagging—annotation	Low	✓	
Video conference	Medium		✓
Shared ownership	Low		✓
External applications	High		✓
Search engine results	Low	✓	
Deletion policy	Low	✓	✓
Exposure to the infrastructure	Low	✓	
Security issues			
Unencrypted traffic	Medium		✓
Static links	Low	✓	
Flawed design/implementation	High		✓
Transparency of stored media	Low	✓	
Profile Hijacking	High		✓
Identity theft	Low		✓
Distortion of malleable content	Low		✓
Shared multimedia links	Low	✓	
Steganography	Medium		✓

they should is, for certain, puzzling. These two solutions, as well as the others, do not come without a cost. The processing cost is quite high; for example only the cost of using SSL for all transactions reduces the server performance by a factor of around 6 [48, 49]. While this cost is very considerable, the adoption of SSL is a common practice and it is considered to be default nowadays from many webpages and services. Therefore, the fact that it is not fully adopted by all health-related OSNs is unacceptable, as the shared information is very sensitive.

Watermarking and steganalysis of the uploaded content introduce another processing cost, which becomes even bigger if one considers that it has to be applied to all the uploaded multimedia content.

Given that most of these services are working under the 'freemium' model, a big part of the cost could be reduced either by subscriptions that offer such services as extras, or by elevating the trust to the service, therefore extending their users and customers.

Certainly, user awareness is a major issue and users should be warned by OSNs of the exposure that they have and possible threats they might face. Third party solutions might already have been used; nevertheless, their status in terms of acceptance and maturity cannot be considered adequate. OSNs are not expected to provide mechanisms to warn users that what they are about to share will disclose a specific additional information about them,

as this is their main source of income. Nevertheless, agents that are developed from third parties could certainly help in this direction, creating a new market and a new line of products.

To facilitate the reader, we have summarized several of the results in table format. Table 1 illustrates how the problems that have been stated could be addressed by existing solutions. As it becomes apparent, the only problem that cannot be tackled by the proposed solutions is the flawed design or implementation. As already discussed, this problem is inherent to almost every software solution; nevertheless, such problems should be quickly resolved when reported and the developers should try to follow common coding standards and principles such as 'privacy by design'. Table 2 provides an overview of the categorization of the privacy and security issues that are reported in the article. In Table 3, we illustrate the impact that each of the reported attacks can have. It is clear that depending on the attacker, the same attack may lead to a completely different impact. Finally, Table 4 depicts the difficulty of the attacker to launch an attack to the victim and whether this attack is manual or it can be automated. We should highlight here that the reported difficulty (low, medium, high) is relative to the attacker. For instance, an attack that is based on the exposure of the user to OSN's infrastructure cannot be launched by any attacker, but from the OSN itself. In this context, the OSN has to allocate little resources to launch the attack. On the contrary, for an unencrypted traffic attack or for a video conference attack, the attacker is considered to be an average user, which is expected to have limited resources and knowledge. Therefore, the reported difficulty is medium.

9. CONCLUSIONS

Undoubtedly OSNs have established a big market share of the Internet. Millions of users are using them daily and their traffic as well as their influence are continuously growing. Whether these networks are related to simple communication or medical issues, user-generated content exposes users greatly, both to the service provider and selected groups of users. While this is well known and it can be considered a calculated risk on the part of the user who decides to join such a network, other security and privacy issues are relevant as well. Numerous studies have already highlighted many of these issues; however, few of them are focused on the core of the shared information, the multimedia content.

This article has explored the risks to which a user is exposed by his shared multimedia content in terms of security and privacy, many of which are indirect or often disregarded by the majority of users. For many of the issues that have been discussed in this work, there are already solutions which can be used to solve them, some of which with considerable cost. Nevertheless, what this article has outlined is that even if many actions have been taken by OSNs to provide security and privacy to their users, justifiably, it cannot be claimed that the current level is adequate. On the other side, users must understand that they cannot arbitrarily share content with other users and services. This content can be used in many ways, many of which can be proved to be malicious. The problem might not arise from one particular post, but from the fusion of others, or from the background information regarding that post. User awareness through proper notifications might help in this direction, but clearly more media coverage and education can greatly help in this aspect.

As future work we would like to quantify the economic impact of these attacks, an aspect of the problem that is not covered in this article. The topic is rather challenging and can indicate why these attacks are launched. The money flow could possibly lead to the people that resort to these attacks. However, Internet companies in general and OSNs in particular are quite reluctant to share information about the attacks they suffer and the economic cost that they suppose, even if in several cases they are forced by law. On the other hand, it is quite difficult to quantify the economical impact for individuals, who quite often will not report it or prosecute the offenders.

FUNDING

A.S. is partly funded by La Caixa Foundation through project 'SIMPATIC: Intelligent, Autonomous and Private Monitoring System based on ICT' RECERCAIXA'12, and by the Government of Catalonia under grant 2009 SGR 1135. He is also supported by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-0004 'ARES', and project TIN2011-27076-C03-01 'CO-PRIVACY'.

REFERENCES

[1] Ellison, N.B. (2007) Social network sites: definition, history, and scholarship. *J. Comput.-Mediat. Commun.*, **13**, 210–230.

[2] Chester, S. and Srivastava, G. (2011) Social Network Privacy for Attribute Disclosure Attacks. *Int. Conf. on Advances in Social Networks Analysis and Mining (ASONAM)*, Kaohsiung City, Taiwan, pp. 445–449. IEEE.

[3] Zhou, B., Pei, J. and Luk, W. (2008) A brief survey on anonymization techniques for privacy preserving publishing of social network data. *ACM SIGKDD Explorations Newsl.*, **10**, 12–22.

[4] Backstrom, L., Dwork, C. and Kleinberg, J. (2007) Wherefore Art Thou r3579x?: Anonymized Social Networks, Hidden Patterns, and Structural Steganography. *Proc. 16th Int. Conf. on World Wide Web*, Banff, Alberta, Canada, pp. 181–190. ACM.

[5] Wondracek, G., Holz, T., Kirda, E. and Kruegel, C. (2010) A Practical Attack to De-anonymize Social Network Users. *31st IEEE Symposium on Security and Privacy*, Berleley/Oakland, California, USA, pp. 223–238. IEEE.

[6] Narayanan, A. and Shmatikov, V. (2009) De-anonymizing Social Networks. *30th IEEE Symposium on Security and Privacy*, Oakland, California, USA, pp. 173–187. IEEE.

[7] Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K. (2008) Social Networks and Context-Aware Spam. *Proc. 2008 ACM Conf. on Computer Supported Cooperative Work*, San Diego, California, USA, pp. 403–412. ACM.

[8] Huber, M., Mulazzani, M., Weippl, E., Kitzler, G. and Goluch, S. (2011) Friend-in-the-middle attacks: exploiting social networking sites for spam. *Internet Comput.*, **15**, 28–34.

[9] Abu-Nimeh, S., Chen, T.M. and Alzubi, O. (2011) Malicious and spam posts in online social networks. *Computer*, **44**, 23–28.

[10] Huber, M., Mulazzani, M., Weippl, E., Kitzler, G. and Goluch, S. (2010) Exploiting Social Networking Sites for Spam. *Proc. 17th ACM Conf. on Computer and Communications Security, CCS'10*, Chicago, Illinois, USA, pp. 693–695. ACM.

[11] Cutillo, L.A., Manulis, M. and Strufe, T. (2010) Security and Privacy in Online Social Networks. *Handbook of Social Network Technologies and Applications*, pp. 497–522. Springer.

[12] Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007) Social phishing. *Commun. ACM*, **50**, 94–100.

[13] Donath, J.S. (1999) Identity and Deception in the Virtual Community. In Kollock, P. and Smith, M. (eds), *Communities in Cyberspace*, pp. 29–59. Routledge.

[14] Douceur, J. (2002) The Sybil Attack. In Druschel, P., Kaashoek, F. and Rowstron, A. (eds), *Peer-to-Peer Systems*, Lecture Notes in Computer Science 2429, pp. 251–260. Springer, Berlin.

[15] Hoffman, K., Zage, D. and Nita-Rotaru, C. (2009) A survey of attack and defense techniques for reputation systems. *ACM Comput. Surv. (CSUR)*, **42**, 1–31.

[16] Trabelsi, S. and Bouafif, H. (2013) Abusing Social Networks with Abuse Reports—A Coalition Attack for Social Networks. *Proc. 10th Int. Conf. on Security and Cryptography*. Reykjavik, Iceland.

[17] Liu, K. and Terzi, E. (2010) A framework for computing the privacy scores of users in online social networks. *ACM Trans. Knowl. Discov. Data*, **5**, 6:1–6:30.

[18] Domingo-Ferrer, J. (2010) Rational Privacy Disclosure in Social Networks. *Proc. 7th Int. Conf. on Modeling Decisions for Artificial Intelligence (MDAI)*, Perpignan, France, October 27–29, pp. 255–265. Springer.

[19] Domingo-Ferrer, J. (2011) Coprivacy: Towards A Theory of Sustainable Privacy. *Privacy in Statistical Databases*, pp. 258–268. Springer.

[20] Hu, H., Ahn, G.-J. and Jorgensen, J. (2011) Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks. *Proc. 27th Annual Computer Security Applications Conf.*, Orlando, Florida, USA, pp. 103–112. ACM.

[21] Talukder, N., Ouzzani, M., Elmagarmid, A.K., Elmeleegy, H. and Yakout, M. (2010) Privometer: Privacy Protection in Social Networks. *IEEE 26th Int. Conf. on Data Engineering Workshops (ICDEW)*, Long Beach, California, USA, pp. 266–269. IEEE.

[22] Patsakis, C. and Solanas, A. (2013) Privacy as a Product: A Case Study in the m-Health Sector. *4th Int. Conf. on Information, Intelligence, Systems and Applications (IISA)*, Piraeus, Greece, pp. 1–6. IEEE.

[23] Patsakis, C. and Solanas, A. (2013) Trading Privacy in the Cloud: A Fairer Way to Share Private Information. *10th IEEE Int. Conf. on e-Business Engineering (ICEBE)*, Coventry, UK, pp. 413–418. IEEE.

[24] Hughes, E. (1993). A cypherpunk's manifesto. http://www.activism.net/cypherpunk/manifesto.html.

[25] Kandias, M., Mitrou, L., Stavrou, V. and Gritzalis, D. (2013) Which Side are You On? A New Panopticon vs. Privacy. *Proc. 10th Int. Conf. on Security and Cryptography (SECRYPT)*, Reykjavik, Iceland, pp. 98–110.

[26] Patsakis, C., Asthenidis, A. and Chatzidimitriou, A. (2009) Social Networks as an Attack Platform: Facebook Case Study. *8th Int. Conf. on Networks (ICN'09)*, Guadeloupe, France, pp. 245–247. IEEE.

[27] Rabkin, A. (2008) Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook. *Proc. 4th Symposium on Usable Privacy and Security*, Pittsburgh, USA, pp. 13–23. ACM.

[28] Savla, P. and Martino, L.D. (2012) Content Analysis of Privacy Policies for Health Social Networks. *Proc. 2012 IEEE Int. Symposium on Policies for Distributed Systems and Networks*, University of North Carolina, Chapel Hill, USA, pp. 94–101. IEEE.

[29] Bilge, L., Strufe, T., Balzarotti, D. and Kirda, E. (2009) All Your Contacts are Belong to Us: Automated Identity Theft Attacks on Social Networks. *Proc. 18th Int. Conf. on World Wide Web*, Madrid, Spain, pp. 551–560. ACM.

[30] Viejo, A., Castella-Roca, J. and Rufián, G. (2013) Preserving the User's Privacy in Social Networking Sites. *Trust, Privacy, and Security in Digital Business*, pp. 62–73. Springer.

[31] Kosinski, M., Stillwell, D. and Graepel, T. (2013) Private Traits and Attributes are Predictable from Digital Records of Human Behavior. *Proc. Natl Acad. Sci.*, **110**, 5802–5805.

[32] Lam, I.-F., Chen, K.-T. and Chen, L.-J. (2008) Involuntary Information Leakage in Social Network Services. *Advances in Information and Computer Security*, pp. 167–183. Springer.

[33] Qin, G., Patsakis, C. and Bouroche, M. (2014) Playing Hide and Seek with Mobile Dating Applications. In Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A. and Sans, T. (eds), *ICT Systems Security and Privacy Protection*, IFIP Advances in Information and Communication Technology 428, pp. 185–196. Springer, Berlin.

[34] Wayner, P. (2009) *Disappearing Cryptography: Information Hiding: Steganography & Watermarking*. Morgan Kaufmann.

[35] Zigomitros, A., Papageorgiou, A. and Patsakis, C. (2012) Social Network Content Management through Watermarking. *IEEE 11th Int. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Liverpool, UK, pp. 1381–1386. IEEE.

[36] Wang, G., Liu, Q. and Wu, J. (2010) Hierarchical Attribute-based Encryption for Fine-grained Access Control in Cloud Storage Services. *Proc. 17th ACM Conf. on Computer and Communications Security*, Chicago, Illinois, USA, pp. 735–737. ACM.

[37] Yu, S., Wang, C., Ren, K. and Lou, W. (2010) Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. *Proc. IEEE INFOCOM, 2010*, San Diego, California, USA, pp. 1–9. IEEE.

[38] Park, N. (2011) Secure Data Access Control Scheme using Type-based Re-encryption in Cloud Environment. *Semantic Methods for Knowledge Management and Communication*, pp. 319–327. Springer.

[39] Ateniese, G., Fu, K., Green, M. and Hohenberger, S. (2006) Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.*, **9**, 1–30.

[40] Shi, C. and Bhargava, B. (1998) A Fast MPEG Video Encryption Algorithm. *Proc. 6th ACM Int. Conf. on Multimedia*, Bristol, UK, pp. 81–88. ACM.

[41] Squicciarini, A.C., Shehab, M. and Wede, J. (2010) Privacy policies for shared content in social network sites. *VLDB J.*, **19**, 777–796.

[42] Squicciarini, A.C., Shehab, M. and Paci, F. (2009) Collective Privacy Management in Social Networks. *Proc. 18th Int. Conf. on World Wide Web, WWW'09*, Madrid, Spain, pp. 521–530.

[43] Mayer-Schönberger, V. (2011) *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.

[44] Backes, J., Backes, M., Dürmuth, M., Gerling, S. and Lorenz, S. (2011) X-pire!-a digital expiration date for images in social networks. CoRR/1112.2649.

[45] Patsakis, C. (2012) Encrypt to Forget. *XII Spanish Meeting on Cryptology and Information Security (RECSI 2012)*, Donostia-San Sebastian, Spain.

[46] Domingo-Ferrer, J. (2011) Rational Enforcement of Digital Oblivion. *Proc. 4th Int. Workshop on Privacy and Anonymity in the Information Society, PAIS'11*, Uppsala, Sweden, pp. 2:1–2:8. ACM.

[47] Stokes, K. and Carlsson, N. (2013) A Peer-to-Peer Agent Community for Digital Oblivion in Online Social Networks. *11th Annual Int. Conf. on Privacy, Security and Trust (PST)*, Tarragona, Spain, pp. 103–110. IEEE.

[48] Kant, K., Iyer, R. and Mohapatra, P. (2000) Architectural Impact of Secure Socket Layer on Internet Servers. *Proc. Int. Conf. on Computer Design*, Austin, Texas, USA, pp. 7–14. IEEE.

[49] Zhao, L., Iyer, R., Makineni, S. and Bhuyan, L. (2005) Anatomy and Performance of SSL Processing. *IEEE Int. Symposium on Performance Analysis of Systems and Software (ISPASS 2005)*, Austin, Texas, USA, pp. 197–206. IEEE.