ORIGINAL PAPER

# Ethical Considerations when Employing Fake Identities in Online Social Networks for Research

Yuval Elovici · Michael Fire · Amir Herzberg ·
Haya Shulman

**Abstract**   Online social networks (OSNs) have rapidly become a prominent and widely used service, offering a wealth of personal and sensitive information with significant security and privacy implications. Hence, OSNs are also an important—and popular—subject for research. To perform research based on real-life evidence, however, researchers may need to access OSN data, such as texts and files uploaded by users and connections among users. This raises significant ethical problems. Currently, there are no clear ethical guidelines, and researchers may end up (unintentionally) performing ethically questionable research, sometimes even when more ethical research alternatives exist. For example, several studies have employed "fake identities" to collect data from OSNs, but fake identities may be used for attacks and are considered a security issue. Is it legitimate to use fake identities for studying OSNs or for collecting OSN data for research? We present a taxonomy of the ethical challenges facing researchers of OSNs and compare different approaches. We demonstrate how ethical considerations have been taken into account in

Y. Elovici · M. Fire (✉)
Telekom Innovation Laboratories, Department of Information Systems Engineering, Ben Gurion University of the Negev, Beer-Sheva, Israel
e-mail: mickyfi@bgu.ac.il

Y. Elovici
e-mail: elovici@bgu.ac.il

A. Herzberg
Department of Computer Science, Bar Ilan University, Ramat Gan, Israel
e-mail: amir.herzberg@gmail.com

H. Shulman
Fachbereich Informatik, Technische Universität Darmstadt/EC-SPRIDE, Darmstadt, Germany
e-mail: haya.shulman@gmail.com

previous studies that used fake identities. In addition, several possible approaches are offered to reduce or avoid ethical misconducts. We hope this work will stimulate the development and use of ethical practices and methods in the research of online social networks.

**Keywords** Online social network · Fake profile · Ethics · Data mining

## Introduction

*Online social networks (OSNs)*, often referred to as *social media*, have rapidly become an integral part of society. They are widely used by many and contain a wealth of information, much of it sensitive and personal. This vast source of pertinent information allows for innovative applications of OSNs, and many of these innovations are designed to benefit both society at large and individuals in particular to identify possible threats to society or individuals. For example, a study on OSNs can assist in the identification of individuals who are inclined to commit suicide or initiate a terror attack, thus enabling a priori prevention. On the other hand, there are also many ways in which OSNs may be abused, resulting in inappropriate or harmful actions.

The widespread use of OSNs, along with their potential for beneficial as well as harmful applications, promotes the study of OSNs and their users. Much research clearly has legitimate motivation, such as the development of new products and services, followed by the evaluation of their acceptance and usage Other research focuses on counteracting harmful applications. In particular, it is important to perform high-quality, experiment-based research to evaluate risks and the effectiveness of different countermeasures (Fire et al. 2012a, b; Rahman et al. 2012).

Online social network research often involves measurements within deployed and operating OSNs, often focusing on the most popular, such as Facebook.[1] Such operational research on deployed OSNs seems to be the best—or even only—method to study important issues which can help in the design and the improvement of OSN products; in identifying threats on OSNs and their users, including the design of defenses; and in understanding social and economic phenomena.

Much of the current OSN research focuses on the following two issues: the *OSN graph* and the *OSN user behavior*. Research on *OSN graphs* analyzes the properties of the OSN relationships graph of connections among OSN users; this can be important for many goals, such as designing a new OSN product. Research on *OSN user behavior* focuses on typical behaviors of OSN users, which can help design and improve products as well as study security and privacy vulnerabilities and defenses.

The collection of data on an operational system, involving data related to real users, raises ethical and even legal concerns and dilemmas. Eynon et al. (2008) identify three basic ethical concepts for research in humans in general, and specifically in relation to the Internet: *confidentiality, anonymity*, and *informed consent*. These concepts are at the core of most institutional and professional research governance.

---

[1] http://www.facebook.com/

Margulies and Herzberg (2013) consider a related topic through their study of usability aspects of systems and ethical problems of such research; they, however, do not consider research specifically on OSNs. Consider the ethical issues and approaches, for example, in the field of *Internet measurements*, which involves real operation systems, similar to OSN research (especially with respect to the OSN graph). Most individuals performing Internet research take privacy and security concerns into consideration. Specifically, studies that expose traffic, e.g., to allow further research on it, normally "sanitize" it by removing any data considered sensitive; this is illustrated in the Cooperative Association for Internet Data Analysis (2012). Similar sanitization of exposed data may be appropriate for OSN research as well.

In this paper, we study the ethics of OSN research as well as potential conflicts between ethical compliance and attaining social benefits from research. Note that OSN research tends to be much more active, with potential impact on both users and OSN providers, compared to other forms of research, such as Internet measurements. This prompts the consideration of an additional ethical concept, which we call *avoid disruption and waste*.

Online social networks raise additional ethical challenges since OSNs normally do not allow such information to be freely available due to the privacy concerns of its users and the OSN terms of use. In fact, the ability to share selected information with only a selected set of peers ("friends") is an important requirement from OSNs.

As a result, much of the research using OSNs involves different techniques to collect information, circumventing these OSN limitations. This includes "whitehat" research for legitimate academic and industrial goals, as well as "blackhat/greyhat" research, whose goal is to extract and exploit sensitive information as well as to actively connect to users, provide (fake) information for different goals, and perform similar malicious activities. Such "blackhat/greyhat" research is conducted by criminals, hacktivists, and even organizations involved in cyber-warfare (terrorists, armies, intelligence and law-enforcement agencies).

Indeed, one of the goals of academic (and some industrial) researchers is precisely to study vulnerabilities allowing such greyhat/blackhat research and then design improved defenses for OSNs and their users. However, for such research to be realistic, researchers must base it on actual OSN data. This raises the type of ethical problems we study in this paper. For example, in order to study information leakage by corporate employees in a particular OSN, researchers may want to employ similar methods that industrial espionage attackers will use. Similarly, studying the diffusion of information in a social network requires the monitoring of many OSN members.

An effective and widely used technique to obtain information about an OSN and its users is to establish OSN connections with many users, typically by creating a significant number of OSN accounts under *fake, non-existing identities* and using these to connect to other users. The creation of such accounts has been studied by several researchers (Boshmaf et al. 2011; Elishar et al 2012).

Fake identities are widely used. It is estimated that more than 8.7 % of the identities in Facebook are fake (Facebook Inc. 2012). These identities were created for various purposes with both legitimate and malicious intent. Fake identities may be completely fabricated, or they may be a clone of an actual identity that exists in the real world (Elishar et al. 2012; Kontaxis et al 2011). Recent studies (Boshmaf

et al. 2011; Elishar et al. 2012) show that users tend to accept friendship requests from people that they do not know both in the virtual and physical world; hence, it is relatively easy to connect fake identities to real identities.

Obviously, the creation of fake identities raises serious ethical, and even legal, concerns. Other techniques to collect OSN data also raise ethical concerns. For example, suppose a researcher did not use a fake account, but her own account; would it be ethical for her to publish information that other users shared with her? Is this case a personal issue between the specific researcher and the persons who decided to connect to her, or is it an ethical issue that should be a considered when accepting such a paper for publication?

In this paper, we investigate the dilemma between two social goals: (1) the above-mentioned privacy and security concerns, and (2) the desire to have reliable experimental research on OSNs for socially beneficial or at least legitimate goals, such as to improve OSN products, services, security, and privacy. We explore the need for OSN data for experimental research (In section "Acquiring Online Social Network Information"), we evaluate the ethical concerns (In section "Ethical Considerations"), and we consider some possible solutions (In section "Ethical Research Recommendations".)

Related Work

In recent years with the increasing number of online sources accessible to researchers, such as web blogs, discussion boards, and online social networks, there have been a growing number of studies on OSNs and users' behavior. Several studies have investigated the ethical aspects of acquiring and analyzing online users' information. Eysenbach and Till (2001) and Flicker et al. (2004) examined the ethical issues which may arise when studying online Internet communities. In their research, Flicker et al. presented practical guidelines for resolving ethical dilemmas in these types of studies. Thelwall and Stuart (2006) investigated the ethical dilemmas that arise when researchers use web crawlers to collect information from online sources. Eynon et al. (2009) explored ethical dilemmas, such as the reuse of data from multiple sources, which may occur when studying online virtual environments. Wilkinson and Thelwall (2011) discussed the ethical considerations of extracting personal information from public online sources for research purposes. According to Wilkinson and Thelwall, researchers do not need to ask permission from the text authors when collecting public information; however, steps for ensuring that the text authors are anonymized need to be taken in academic studies. Subsequently, Rosenberg (2010) investigated what data should be perceived as private and what as public; this enables researchers to determine when their study requires an informed consent. Recently, Lucas (2012) demonstrated that ethics does not get enough serious examination in the field of social eco-informatics. Lucas recommended that social eco-informatics researchers include more ethical deliberation in their research.

Indeed, there is a rising awareness regarding the ethical concerns related to OSN research, but it mainly focuses exposing a user's private data. In this work, we discuss ethical problems related to the methods which are deployed when conducting research on an OSN, and we also consider the potential risks and problems which may result, affecting the OSN and its users as well as possible third parties.

Contributions

This work presents the first taxonomy of *ethical* considerations and problems related to the range of techniques and approaches that are employed in studies of online social networks. This significantly expands upon previously published works on ethics in OSN research; for example, we demonstrate that OSN research can have a detrimental impact not only on OSN users but also on the OSN provider and even those indirectly associated.

Organization

The rest of the paper is structured as follows: In section "Acquiring Online Social Network Information" describes how information stored in OSNs can be harvested for research purposes. In section "Ethical Considerations" follows with a discussion of the ethical and legal perspectives related to research on OSNs. In section "Ethical Research Recommendations" discusses several possible approaches to warrant the use of fake identities while complying with ethical considerations. In section "Previous Research and Ethical Considerations" illustrates how ethical considerations were taken in account in previous research that involved fake identities. The paper provides concluding comments in section "Conclusions".

## Acquiring Online Social Network Information

With the exponential growth of online social networks usage during the past several years, many researchers have acquired OSN information for a range of purposes (See Table 1), from studying the characteristics of large-scale online social network graphs (Mislove et al. 2007) to improving road safety (Fire et al. 2012b). The OSN users' information can be divided into two main categories: public and private (see Fig. 1). The public user's information is data that is available to all members of the OSN, while in many cases the user's private information is only accessible to friends of the user. For example, Facebook users' personal information is accessible to other users in the network according to each Facebook user's privacy settings (Liu et al. 2011). In some cases the user's information can be accessed only by his or her Facebook friends, while in other cases the information can be accessed by every member in the network. In order to acquire OSN information, researchers have developed various techniques that aim to collect both OSN users' public and private information. In this section we present the different techniques by which researchers can acquire OSN information. In addition, we also present ethical issues which arise at the end of a study, after completing the acquiring process when, the researchers want to share their acquired information with the academic community.

Public Information

To acquire OSNs users' public information, researchers have primarily used online web crawlers. These web crawlers can obtain the users' information by using the

**Table 1** Various studies using different online social network acquiring methods

| Methods | Studies |
| --- | --- |
| Web crawling | Fire et al. (2011, 2012b, 2012c) |
| Passive fake profiles | Jernigan and Mistree (2009), and Fire et al. (2013) |
| API crawler | Mislove et al. (2007), Kwak et al. (2010), and Pontes et al. (2012) |
| By agreement | Altshuler et al. (2012) |
| Active fake profiles (socialbots) | Boshmaf et al. (2011) and Elishar et al. (2012) |
| Third party application | Fire et al. (2012a) and Rahman et al. (2012) |
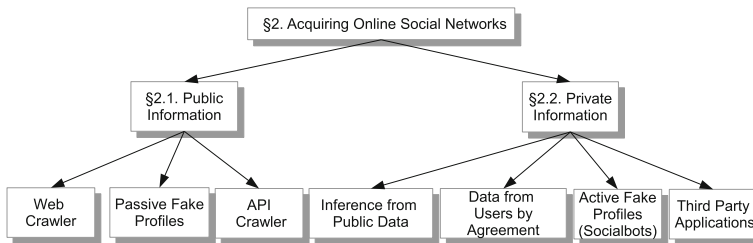


**Fig. 1** Various OSN acquisition techniques

OSN's application programming interface (API) (Mislove et al. 2007; Kwak et al. 2010) or by analyzing the raw data obtained directly from the OSN's web pages (Fire et al. 2011, 2012b). However, in some OSNs like Facebook, it is not possible to collect users' public information without being logged onto the OSN. To overcome this limitation, researchers have created passive fake profiles which are used to obtain access to the OSN public information (Fire et al. 2013; Jernigan and Mistree 2009). These fake profiles do not initiate friend requests to other users in the network and do not intervene in the OSN activity. By using this method, researchers are able to collect the OSN's public information with minimal intervening in the OSN activity and without accessing restricted users' private information. The results obtained from using these methods, however, do not give the researchers a wider picture of the OSN, which is crucial for certain type of studies, such as security and privacy studies. Moreover, some techniques not implemented in the right manner can abuse the OSN infrastructure and negatively affect the overall network performance. For example, using web crawlers, which initiate large amounts of rapid page requests, can create an overload on the OSN's servers, resulting in interference with OSN activity.

Private Information

To acquire OSN users' private information, researchers have developed several techniques. These techniques include requesting private information directly from the users through applications and browser add-ons which integrate with the OSN (Fire et al. 2012a; Rahman et al. 2012); inferencing OSN users' private information

by analyzing information obtained from their friends (Jernigan and Mistree 2009; Mislove et al. 2010); and even activating dynamic fake profiles, also known as socialbots, which initiate a series of friend requests in order to collect users' private information (Boshmaf et al. 2011; Elishar et al. 2012). By using these methods, researchers can obtain a fuller picture of the studied OSN, including private users' information. Moreover, these types of methods are extremely valuable when it comes to analyzing privacy and security issues in OSNs. For example, by using socialbots researchers were able to estimate the amount of private information exposed in Facebook to malicious fake users (Boshmaf et al. 2011). However, using these methods can also influence the OSN behavior and expose personal sensitive user information, such as the user's sexual orientation (Jernigan and Mistree 2009). Moreover, fake profiles created by one research group may influence the research results of another research group that might treat them as real user profiles. Therefore, using these types of methods should be done with great care and with consideration to both the users' privacy and to the OSN's infrastructure.

Sharing the Acquired Information

After the networks' acquisition processes are finished, many researchers want to assist their peers by sharing their acquired datasets with the rest of the world. This is usually done by anonymizing the datasets and uploading them into dedicated websites (BGU Social Networks Security Research Group 2013; Kunegis 2013; Stanford 2013; Zafarani and Liu 2009). However, the sharing and anonymizing process must be done with great care and consideration to the OSNs users' privacy. Using the wrong anonymization methods can result in exposing the OSNs users' private and sometimes sensitive information (Narayanan et al. 2011; Narayanan and Shmatikov 2006; Zimmer 2010). Another ethical issue which needs to be taken into consideration is what to do with the acquired datasets after the study is over. Do the researchers need to delete and destroy the datasets, or can they store them in an encrypted manner for further use? Each action has its own positive and negative sides. If the researchers delete the datasets, they fully protect the OSNs users' privacy. However, they can not use them for further studies, and other researchers will not be able to compare their results to previous studies using the same data. If the researchers keep the datasets, they can jeopardize the OSNs users' privacy, but the datasets can be used for further studies without the need to undertake the extensive acquisition process again. We present our recommendations in section "Ethical Research Recommendations" for these issues.

## Ethical Considerations

Online social networks offer a vast amount of data, useful for research in various disciplines for both commercial and academic purposes. In researching online social networks, a number of ethical challenges and dilemmas are introduced with respect to the involved entities. We consider the following as the entities that may be
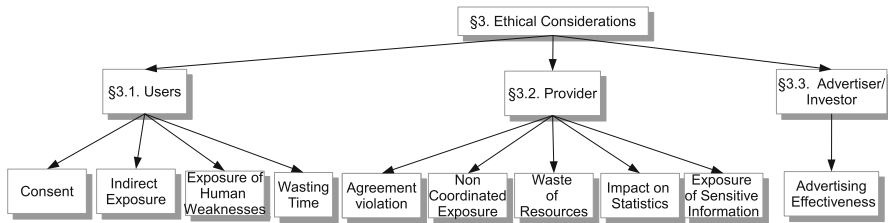
**Fig. 2** Ethical considerations with respect to the user, the OSN, and the advertiser/investor when performing research on an OSN

impacted by OSN research: (1) the *users* of the OSN, (2) the *OSN operator*, and (3) the *advertiser/investor* in OSN.

In this section we identify relevant ethical issues (see Fig. 2). We then map the techniques in section "Acquiring Online Social Network Information" to the ethical problems that they pose (see Table 2).

## The Users

Rightfully, ethical research considerations mostly focus on potential harm to the end users, and this also holds for OSNs. The main ethical issues concerning users involve their consent to participate in the experiment, and in particular, to allow any exposure of their private information. Within online social networks, users share lots of information with their online connections, and may make decisions based upon connections of their connections. This raises another ethical problem, that of indirect exposure, i.e., exposure of a user via a connection. OSN research may also reveal common user weaknesses, which could then be exploited, and they should be reported carefully to avoid being used against the users. Finally, when users are unaware of an OSN experiment, yet affected by it, there can be the ethical concern of potential loss of time. We next review each of these concerns.

*Consent.* A basic ethical question is whether all users should be aware of being involved in an experiment, and if their consent is required to participate in the experiment and allow any resulting exposure of information. In many types of research involving humans, it is considered unethical to perform an experiment without consent. Indeed, many recent studies involve those who have explicitly volunteered, offering access to their personal online information (e.g. Huber et al. 2011a).

On the other hand, many of the experiments on OSNs have not required the prior informing of users or receiving of their consent. In many such cases the research has significantly contributed to society, such as identifying risks to OSN users and allowing the development of countermeasures, and the actual damage to individuals seems negligible. Can this justify performing research without a user's consent?

*Indirect Exposure.* A side effect of transitive trust is exposure of personal data to friends of a friend. In addition, two friends may become connected who might not want to become connected.

EXPOSING THE DATA OF FRIENDS OF A FRIEND. A user's consent, such as for a "friend request" or to participate in research, does not automatically imply the consent of

**Table 2** Mapping between the ethical considerations and the research methods deployed for studies on OSNs

| | Consent | Indirect Exposure | Exposure of Human Weaknesses | Waste of Users' Time | Agreement Violation | Non-Coordinated Exposure | Waste of Resources | Impact on Statistics | Exposure of OSN Sensitive Information | Advertising Effectiveness |
|---|---|---|---|---|---|---|---|---|---|---|
| Web Crawler | | | | | X | X | X | X | X | X |
| API Crawler | | | | | X | X | | | X | |
| Inference from Public Data | X | | | | | | | | | |
| Consent | | X | | | | | X | | | |
| Active Fake Profiles (Socialbots) | X | X | X | X | X | | X | X | | |
| Third Party Applications | X | X | X | X | X | X | X | | X | X |
| Store Acquired Data | X | X | X | | X | | | | X | |

the user's friends. When performing research on an individual's data, the researcher also frequently gains access to personal information about that individual's friends.

CONNECTING 2nd LEVEL FRIENDS. Accepting a friendship request implies becoming visible to new users. Two users may not want to be connected via a third party; they may wish to hide the existence of their virtual profiles or want to keep the information that they post private. During studies, researchers may connect individuals profiles which would otherwise not be connected. For example, consider a bot (attacker controlled profile) that a researcher connects to, not realizing that it is a malicious profile whose goal is to constantly discover new users and to harvest information on these users. This bot now has a second degree access to all of the researcher's OSN friends, exposing their privacy. Furthermore, such a connection may also assist the bot in finding even broader connections, which it otherwise would not have the knowledge or tools to perform. For instance, often to glean users' information, researchers resort to studies from sociology or physiology in order to construct their profile in such a way that increases the chances of other users accepting their friend requests; the attacker does not have the required knowledge to perform such a study on its own.

*Exposure of Human Weaknesses*. Research conclusions and results, if not disclosed carefully, can harm the user. Specifically, when conducting research that employs an OSN, the researcher may discover vulnerabilities pertaining to human weaknesses or to the user-OSN interaction that were not known before. For instance, if a researcher discovers that a friendship request from a profile with a photograph of an attractive female is more likely to be accepted by OSN users, then he should be extremely careful to not disclose this prior to notifying the OSN

provider (see Boshmaf et al. 2011). As a countermeasure, the OSN provider could, for instance, display a warning message to a user when detecting certain profile properties that are known to be suspicious.

*Wasting Time*. The process of luring a user into accepting friend requests may be time-consuming not only for the researcher but also for the user.

The OSN Operator

Using the platform that an OSN provides for research may stand in violation of the OSN's terms of service. This may further result in potential harm to the OSN or to its users, e.g., due to wasted resources, exposure to competition, or a reduced customer base. Several ethical considerations relating to OSN operators are described below.

*Agreement Violation*. Creating fake accounts often stands as a violation of conditions of an OSN, which forbids creating more than one account or using fake accounts. Fake accounts may expose the OSN to lawsuits or harm its reputation.

*Non-Coordinated Exposure*. OSN platforms may have vulnerabilities and can even be used as a vector in launching attacks, thus harming users, hurting other networks and services on the Internet, and exhausting the resources of the OSN. For instance, Huber et al. (2011b) discovered a new attack: the friend-in-the-middle attack that can be used to harvest social data in an automated fashion. When conducting a study on online social networks, researchers often discover such vulnerabilities. It is important, therefore, to establish a procedure whereby the researchers can publish the OSN vulnerabilities and attacks and take the necessary precautions, e.g., contacting the OSN and allowing it to patch the exploit to prevent abuse by malicious parties. If a vulnerability is exposed without coordination with the OSN, it may be subsequently exploited by attackers to compromise the OSN and its users.

As an example, recently Athanasopoulos et al. (2008) showed that malicious users can take control of the social network visitors by remotely manipulating their browsers through legitimate web control functionality, e.g., using image-loading HTML tags. They also demonstrated that Facebook users can be exploited as a vector in launching a denial of service attacks. Clickjack attacks can hijack users' web sessions (Rydstedt et al. 2010) if the OSN does not employ sufficient countermeasures.

It is important to emphasize that research on OSNs is clearly valuable and should be encouraged since weaknesses as described above may be exploited by malicious attackers without the awareness of the OSN, the users, or the research community. Furthermore, research allows the development of patches and countermeasures to preventing the vulnerabilities from being exploited.

*Waste of Resources*. Creating fake profiles consumes resources on the OSN, including storage, communication, and processing.

*Impact on Statistics*. Fake accounts bias statistics and may provide misleading information on trends, resulting in wide-ranging commercial implications.

*Exposure of Sensitive Information*. While running a study, researchers may discover sensitive information pertaining to the OSN, such as the way its algorithms

work. Exposure of this information may benefit the OSN's competitors and consequently harm the OSN and produce a negative commercial impact.

The Advertiser/Investor

Fake accounts, created during a research study, may influence the perceived popularity of an online social network; that is, the experiment may increase the OSN's share value through impressing the shareholders, or it may influence the effectiveness of advertising on the OSN, which may not translate into a profitable and sustainable business. According to the analytics service of Limited Run, an online shopping platform provider, the ad system on Facebook is not reliable, and 80 % of the ad clicks come from fake accounts or bots, which drive up the advertising costs (Taylor 2012). Furthermore, if the investor (or the advertiser) pays per profile, fake accounts artificially inflate the value of the OSN. For instance, in August 2012 Facebook was reported to have more than 83 million fake profiles, which are about 8.7 % of the total number of profiles (Facebook Inc. 2012); this indicates a notable growth of fake accounts from 6.0 % in March 2012.

## Ethical Research Recommendations

In the previous section, we discussed a large set of ethical issues with OSN research methodologies. In this section, we explore different solutions, balancing the ethical principles of *confidentiality*, *anonymity*, *informed consent*, and *avoidance of disruption and waste*, with the benefits from experimental research on deployed OSNs.

The ethical concerns presented in section "Ethical Considerations" can be divided among *concerns related to the harvesting* of data from the OSN; *concerns related to the exposure of data*; *concerns about the impact on the structure, availability, and security* of the OSN; and finally *concerns about the conduct of researchers*. We discuss each of these sets in the following subsections; before that, in the next subsection, we discuss the specific issue of consent.

Consent

We begin with some general recommendations, observations, and proposals.

We first discuss the *informed consent* concern and possible remedies. Obtaining user consent in OSN research has two main challenges: (1) researchers may be unable to know the real age of the user in order to verify that the user is of age (for informed consent), and (2) the very awareness of having informed consent may influence a user's behavior, impacting the subsequent research on user behavior itself.

We do not know of a truly reliable solution to the age problem since many OSNs only allow adult users, yet many under age users register anyway, simply providing an incorrect age. We believe this issue is not specific to research, as this problem

relates to the actual provision of OSN services; therefore it is reasonable to ignore this concern and for researchers to use the stated age of the user (usually available).

The user-awareness problem is much more severe for research related to user behavior. We suggest two solutions:

*Long-Term Research*. A user's awareness of having been measured in some experiment is quickly eroded after using a system for some "real" purpose. Hence, the effect of user awareness can be minimal in research that is long term. This was confirmed by Herzberg and Margulies (2011) and used in experiments in secure usability.

*Post-Research Informing/Compensating*. Another option is to inform users of their involvement in research *after* the measurements have been completed, even though the users did not express their (informed) consent. It may be appropriate to also offer some token of compensation as well as an explanation of the need to use this method (instead of informed consent) and to emphasize the social value of the research.

This is clearly not as ethical as proper informed consent. However, this method may still have some advantages, in particular: (1) users have the ability to provide feedback, providing some indication of the amount of harm, if any, that they have experienced, and (2) this provides a *negative training function*, helping users to become more savvy at detecting OSN fraud; see Herzberg and Margulies (2011).

Harvesting Process

As described in section "Ethical Considerations", the harvesting process can affect OSN performance, influence an OSN's reputation, and threaten users' privacy. The harvesting is performed directly by crawlers or indirectly by fake identities. One of the first ways to reduce the ethical concerns related to harvesting is to improve the sharing of datasets among the researchers such that not every researcher will harvest his own data. Currently, the information retrieval community has created many datasets that are being shared by all the researchers in the community (Microsoft-Research 2013). The social network research community should adopt this strategy in order to reduce harvesting as much as possible. Alternatively, perhaps the social network operators should create datasets specifically for researchers ("if you cannot fight them, join them") after informing their users about the new policy. The social network operators are in a better position to apply advanced anonymization techniques than any small research group.

Research Results

Research results may influence both the users and operators of OSNs as described previously. As with many types of research, vulnerabilities are routinely discovered and often disclosed before the operators have had the chance to patch up the problem. This issue is exacerbated with respect to OSN platforms and their users since each weakness has the potential to affect an enormous number of parties, with detrimental results. Due to the importance of the potential data exposure, we recommend setting up a coordinated emergency response team (CERT) for

vulnerability disclosures. Such an entity will allow all of the involved parties to be quickly notified, and it will give them an opportunity to patch the problem before the exploit becomes public. Researchers should also suggests countermeasures to the attack and inform the operators accordingly.

Experiments that involve human subjects should require a lengthy approval process, whereby it is verified that the research can cause no harm. Since OSN research involves human subjects, or more specifically their data, an approval process should be required for cases in which new research methods are being implemented.

A potential reaction of the OSN operator, e.g., due to concern for legal actions against it, may be to prevent any kind of research on the OSN. However, we caution against this reaction, noting that such a *security by obscurity* is risky and can endanger both the users of the OSN and the OSN platform (as well as other potential third parties). Vulnerabilities may be discovered and abused by malicious attackers, instead of used beneficially by legitimate researchers. Attackers do not publish the vulnerabilities and attacks; researchers, on the other hand, create awareness and provide solutions to these vulnerabilities. Therefore, we recommend that the OSN operators address these issues and recognize the legitimate need for research to provide appropriate, beneficial contributions.

Influence on the Network

In general, OSN operators need to accept the fact that researchers will undoubtedly continue to create fake profiles, and the operators' algorithms will never be able to detect all of them. Therefore, the OSN operator should allow fake profiles to be created, but it should also offer a specified procedure whereby a researcher can notify the OSN and request approval (possibly anonymously) for introducing profiles that are fake and dedicated to a specific study, indicating relevant information such as the duration of the study and purpose of the research. The OSN should have an approval (or alternately, rejection) procedure for each profile, along with an appropriate method to notify the researcher. The OSN may also request an approval or certificate from the researcher, stating that the study is "ethical." It is important to note that the proposed procedure would allow researchers to spend fewer resources on having to generate fake profiles that cannot be detected by the OSN operator.

We recommend that generally the OSN should allow the requests since good research will help protect the OSN platform and its users. However, it may be reasonable to limit the number of fake profiles to some pre-determined threshold at any one time.

Researchers' Conduct

We recommend that researchers use the online social networks' APIs when possible, and then resort to fake *passive* profiles (instead of active) if needed. The identifiers of the profile (e.g., a photo) should not expose the identity of the individual. When the study concludes, the researcher should remove the fake profile

and, if possible, inform users connected to that profile that it was a fake profile for research purposes. When possible, the researcher should also provide information and token compensation, and allow users to provide feedback. This has multiple benefits: (1) fairness to users; (2) better awareness of the possible harm to users, allowing improved ethical decisions in future research; (3) reduction in harm to users; (4) potentially highly significant negative training to users, teaching them to be more cautious and to be able to identify fake identities in the future (see Herzberg and Margulies 2011).

Researchers should use cryptographic and other techniques for anonymization of the data as well as for confidentiality. The researchers should handle the study data, as well as the findings, with great care. Following the research, the data should be removed, or if it is required for future research, it should be stored encrypted. When sharing the data, we recommend applying appropriate anonymization techniques which remove all identifying data that can leak information when combined with other sources. See (Zimmer 2010) for further information on such deanonymisation attacks. When transferring the data over the network and when accessing the OSN, encryption should be used. When conducting the study, the researchers should also consider the load on the OSN and the overhead to users. Finally, the researchers should maintain precise and accurate records of the data collected, the profiles created, the people involved in research, and any other pertinent information. This must be preserved in a secure manner.

## Previous Research and Ethical Considerations

In this section, we will use previous studies that employed fake identities to illustrate that it is possible to achieve similar research results, but with lower impact to the OSN members' privacy and to the OSN operator resources.

Fire et al. (2013) presented a method for mining an organization's topology through the use of passive fake identities which collected employees' public information from their Facebook profiles. Elishar et al. (2012) employed active fake identities to achieve the same goal of mining organizational topology. Elishar et al. (2012) initiated friend requests to Facebook users who worked in a targeted organization. Upon accepting these friend requests, users unknowingly exposed information about themselves and about their workplace. This technique was tested on two real organizations and successfully infiltrated both. Compared to the passive fake identity method, the technique utilizing active fake identities, was able to discover up to 13.55 % more employees and up to 18.29 % more informal organizational links. However, similar results were achieved from both studies when identifying leadership roles using different centrality measures. Hence, it is possible to infer leadership roles without the need to employ active fake profiles, which can compromise the OSN users' privacy and impact the OSN operator resources.

Fire et al. (2012c) presented a novel method for the detection of fake identities in OSNs by using only the social network's own topological features. Reliance on these features alone ensures that the proposed method is generic enough to be

applied on a range of social networks. In order to train a machine learning classier, training had to be created and collected. The training set had to include labeled fake identities. One way to create a training set is to add fake identities to an OSN and then collect the modified network as a labeled training set. To avoid modifying the OSN itself, which will create a negative impact on the OSN operator, a different approach was taken. To create positive examples for the classifiers, Fire et al developed a code which simulated the infiltration of a single fake identity (or a group of fake identities) to social networks. For each social network, the simulator loaded the topology graph and inserted 100 new nodes, which represented 100 fake identities. The insertion process of each fake identity into the graph was done by simulating a series of "follow" requests sent to random users in the network. Each fake user had a limit on the number of friend requests in order to comply with a reality in which many social networks limit the number of user requests allowed for new members (exactly for the purpose of blocking spammers and socialbots).

## Conclusions

Research involving the operation of widely-used online social networks the behavior of OSN users, is vital to the design of improved OSNs, OSN applications, and especially OSN privacy and security mechanisms. Indeed, research on online social networks and OSN data can be useful in various research disciplines, such as the study of social behavior and the design of secure and usable social networks. It can also have value and applications in real life and; for example, it can facilitate detection and a priori prevention of terror attacks, theft, coercion, and other critical situation.

Many commonly used research techniques, however, raise ethical concerns, which are rarely even considered by researchers or the community at large. For instance, such research can jeopardize users' privacy as well as expose potential vulnerabilities of the OSN platform to abuse by malicious attackers. A trivial solution is to limit such research to use on simulated environments. However, in order for research on OSNs to be of practical relevance and maximum usefulness it must be conducted under realistic conditions, using real users' data. In particular, in contrast to other research topics, studying a simulated OSN may not yield realistic results, especially if the entire research goal is to analyze and test real users' data and interactions.

With this paper, we strive to draw attention to this important issue and initiate a discussion within the OSN research community to encourage the adoption of an appropriate code of ethics, which can then be utilized in agreements and technical standards. This code would be a means to facilitate good research, with acceptable trade-offs between ethical considerations and the social benefits of precise, available, and timely research on these important issues. As we point out in this work, an effort from both the research community and industry is required to define and standardize mechanisms that will enable this legitimate and significant research while ensuring privacy of OSN users and their data. A number of such mechanisms that can facilitate ethical research on OSNs have been outlined. As online social

networks continue to gain prominence, ethical considerations become increasingly critical.

# References

Altshuler, Y., Pan, W., & Pentland, A. S. (2012). Trends prediction using social diffusion models. In *Social computing, behavioral-cultural modeling and prediction* (pp. 97–104). Springer.

Athanasopoulos, E., Makridakis, A., Antonatos, S., Antoniades, D., Ioannidis, S., Anagnostakis, K., et al. (2008). *Antisocial networks: Turning a social network into a botnet. Information security* (pp. 146–160).

BGU Social Networks Security Research Group. (2013). BGU social networks dataset collection. http://proj.ise.bgu.ac.il/sns/datasets.html.

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). The socialbot network: When bots socialize for fame and money. In *Proceedings of the 27th annual computer security applications conference, ACM* (pp. 93–102).

CAIDA. (2012). Anonymized Internet Traces 2012 Dataset. http://www.caida.org/data/passive/passive_2012_dataset.xml.

Elishar, A., Fire, M., Kagan, D., & Elovici, Y. (2012). Organizational intrusion: Organization mining using socialbots. In *Proceedings of ASE international conference on social informatics*, Washington DC, USA, December.

Eynon, R., Fry, J., & Schroeder, R. (2008). The ethics of internet research. In *Handbook of online research methods* (pp. 23–42). Sage, London.

Eynon, R., Schroeder, R., & Fry, J. (2009). New techniques in online research: Challenges for research ethics. *Twenty-First Century Society, 4*(2), 187–199.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *BMJ, 323*(7321), 1103–1105.

Facebook Inc. (2012). Quarterly report pursuant to section 13 or 15(d) of the securities exchange act of 1934. http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm.

Fire, M., Tenenboim, L., Lesser, O., Puzis, R., Rokach, L., & Elovici, Y. (2011). Link prediction in social networks using computationally efficient topological features. In *IEEE third international conference on privacy, security, risk and trust (PASSAT) and IEEE third international conference on social computing (SocialCom)* (pp. 73–80). IEEE.

Fire, M., Katz, G., & Elovici, Y. (2012). Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. *Human Journal, 1*(1), 26–39.

Fire, M., Kagan, D., Elishar, A., & Elovici, Y. (2012a). Social privacy protector—protecting users' privacy in social networks. In *SOTICS 2012, the second international conference on social eco-informatics* (pp. 46–50).

Fire, M., Kagan, D., Puzis, R., Rokach, L., & Elovici, Y. (2012b). Data mining opportunities in geosocial networks for improving road safety. In *IEEE 27th convention of electrical and electronics engineers in Israel (IEEEI), 2012* (pp. 1–4). IEEE.

Fire, M., Puzis, R., & Elovici, Y. (2013). Organization mining using online social networks. ArXiv preprint arXiv:13033741.

Flicker, S., Haans, D., & Skinner, H. (2004). Ethical dilemmas in research on internet communities. *Qualitative Health Research, 14*(1), 124–134.

Herzberg, A., & Margulies, R. (2011). Forcing johnny to login safely—long-term user study of forcing and training login mechanisms. In V. Atluri, C. Díaz (Ed.), *ESORICS, lecture notes in computer science* (vol. 6879, pp. 452–471). Springer, Berlin

Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., & Goluch, S. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. *Internet Computing, IEEE, 15*(3), 28–34.

Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., & Weippl, E. (2011a). Social snapshots: Digital forensics for online social networks. In *Proceedings of the 27th annual computer security applications conference* (pp. 113–122). ACM.

Jernigan, C., & Mistree, B. F. (2009). Gaydar: Facebook friendships expose sexual orientation. *First Monday, 14*(10).

Kontaxis, G., Polakis, I., Ioannidis, S., & Markatos E. P. (2011). Detecting social network profile cloning. In *IEEE international conference on pervasive computing and communications workshops (PERCOM workshops)* (pp. 295–300). IEEE

Kunegis, J. (2013). KONECT—the Koblenz Network Collection. http://konect.uni-koblenz.de.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010). What is twitter, a social network or a news media? In *Proceedings of the 19th international conference on world wide web* (pp. 591–600). ACM.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: User expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on internet measurement conference* (pp. 61–70). ACM.

Lucas, R. (2012). Ethics and social eco-informatics. In *SOTICS 2012, the second international conference on social eco-informatics* (pp. 1–6).

Margulies, R., & Herzberg, A. (2013). Conducting ethical yet realistic usable security studies. In *Cyber-security research ethics dialog and strategy workshop (CREDS)*.

Microsoft-Research. (2013). LETOR: Learning to rank for information retrieval. http://research.microsoft.com/en-us/projects/mslr/.

Mislove, A., Marcon, M., Gummadi, K. P., Druschel, P., & Bhattacharjee, B. (2007). Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* (pp. 29–42). ACM.

Mislove, A., Viswanath, B., Gummadi, K. P., & Druschel, P. (2010). You are who you know: Inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on web search and data mining* (pp. 251–260). ACM.

Narayanan, A., & Shmatikov, V. (2006). How to break anonymity of the netflix prize dataset. ArXiv preprint cs/0610105.

Narayanan, A., Shi, E., & Rubinstein, B. I. (2011). Link prediction by de-anonymization: How we won the kaggle social network challenge. In *The 2011 international joint conference on neural networks (IJCNN)* (pp. 1825–1834). IEEE.

Pontes, T., Vasconcelos, M. A., Almeida, J. M., Kumaraguru, P., & Almeida, V. (2012). We know where you live: Privacy characterization of foursquare behavior. In *UbiComp* (pp. 898–905).

Rahman, M. S., Huang, T. K., Madhyastha, H. V., & Faloutsos, M. (2012). Efficient and scalable socware detection in online social networks. In *Proceedings of the 21st USENIX conference on Security symposium, USENIX Association* (pp. 32–32).

Rosenberg, A. (2010). Virtual world research ethics and the private/public distinction. *International Journal of Internet Research Ethics, 3*(12), 23–36.

Rydstedt, G., Bursztein, E., Boneh, D., & Jackson, C. (2010). Busting frame busting: a study of clickjacking vulnerabilities at popular sites. In *IEEE Oakland Web 2*.

Stanford. (2013). Stanford large network dataset collection. http://snap.stanford.edu/data/.

Taylor, C. (2012). Startup claims 80 bots. http://techcrunch.com/2012/07/30/startup-claims-80-of-its-facebook-ad-clicks-are-coming-from-bots/.

Thelwall, M., & Stuart, D. (2006). Web crawling ethics revisited: Cost, privacy, and denial of service. *Journal of the American Society for Information Science and Technology, 57*(13), 1771–1779.

Wilkinson, D., & Thelwall, M. (2011). Researching personal information on the public web methods and ethics. *Social Science Computer Review, 29*(4), 387–401.

Zafarani, R., & Liu, H. (2009). Social computing data repository at asu. http://socialcomputing.asu.edu, Arizona State University, School of Computing, Informatics and Decision Systems Engineering.

Zimmer, M. (2010). But the data is already public: On the ethics of research in Facebook. *Ethics and Information Technology, 12*(4), 313–325.