Tsikerdekis, M., & Zeadally, S. (2015). Detecting and Preventing Online Identity Deception in Social Networking Services. IEEE Internet Computing.
http://doi.org/10.1109/MIC.2015.21
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7111875

Detection and Prevention of Online Identity Deception in Social Networking Services (SNSs)

Michail Tsikerdekis and Sherali Zeadally
College of Communication and Information
University of Kentucky, Lexington, KY, 40506

Abstract

The recent decade we observed an explosion of social networking services along with the number of users on them. The nature of these sites make identity deception much easier by offering a quick way of setting up identities, managing them and being able to easily deceive and connect with others. Fighting deception requires a coordinated approach by users and developers to ensure detection and prevention of identity deception in these sites. In this article, we identify the most prevalent approaches in detection and prevention for fighting different types of identity deception from a user's perspective as well as from a developer perspective and evaluate their efficiency in social networking services in order to provide recommendations that can assist towards eradicating this issue.

1. Introduction

Over the last few years, the number of users of Social Networking Services (SNS) has experienced a skyrocketing growth. Currently, Facebook and Twitter have reached 82 percent of world's Internet users which amounts to a staggering 1.2 billion users [1]. It is easier in the social networking environment to deceive others compared to the real world due to factors such as the ease of content and identity manipulation, the absence or feeling of absence of accountability, the perceptually lower moral cost because of the distances involved in computer-mediated communication, and, the lack of many non-verbal cues which would otherwise "leak" towards victims [2]. Deception in SNS continues to be a major concern and its detection and prevention has been attracting a lot of attention by researchers and SNS developers lately. Online deception in SNS provides a new platform for deceivers to use, forge and manipulate an identity with a click of a button. Furthermore, the inherent software design of SNS tends to promote the feeling of no accountability and encourages the loss of inhibition. It is often difficult to trace an account back to a particular individual or verify his/her identity and in some cases a SNS user gets caught after a long time. Detecting online deception becomes even more challenging because humans have been found to be consistently bad deception detectors [3].

In this work, we focus on identity deception and some of the factors that have fueled it in SNS in recent years. We identify several popular techniques that can be used for identity deception detection for both users and developers that currently lack wide-spread implementation. We evaluate techniques that can be applied by both users and developers to help prevent identity deception in the social media environment. Finally, we highlight some of the challenges that must be addressed in the future to address identity deception in SNS.

2. Identity Deception in Social Networking Services

Online identity deception is the deliberate concealment or altering of a sender's true identity in order to convey that false belief to a receiver [4] while a receiver does not anticipate identity tampering by the sender. In addition, for deception to take place, *an individual should not be expecting that all or part of the information in a message will be concealed or altered* [5]. Some of the objectives behind deception include *instrumental (*goal-driven), *relational (*relationship-driven), or *identity* (e.g., protecting one's reputation) [6].

There are three types of identity deception [4]: a) *identity concealment* (Figure 1a) occurs when part of the identity information is omitted or altered, b) *identity theft* (Figure 1b) occurs when a person's identity is stolen, and, c) *identity forgery* (Figure 1c) occurs when a new persona is created along with a new history record. A personal identity usually consists of an *attributed identity* such as the name or place of birth, a *biometric identity* such as fingerprints, and, a *biographical identity* such as a criminal record or credit history [4]. In addition to a personal identity (e.g., social security number, height or fingerprint), a person's identity also contains a social identity (e.g., social relations) [7].

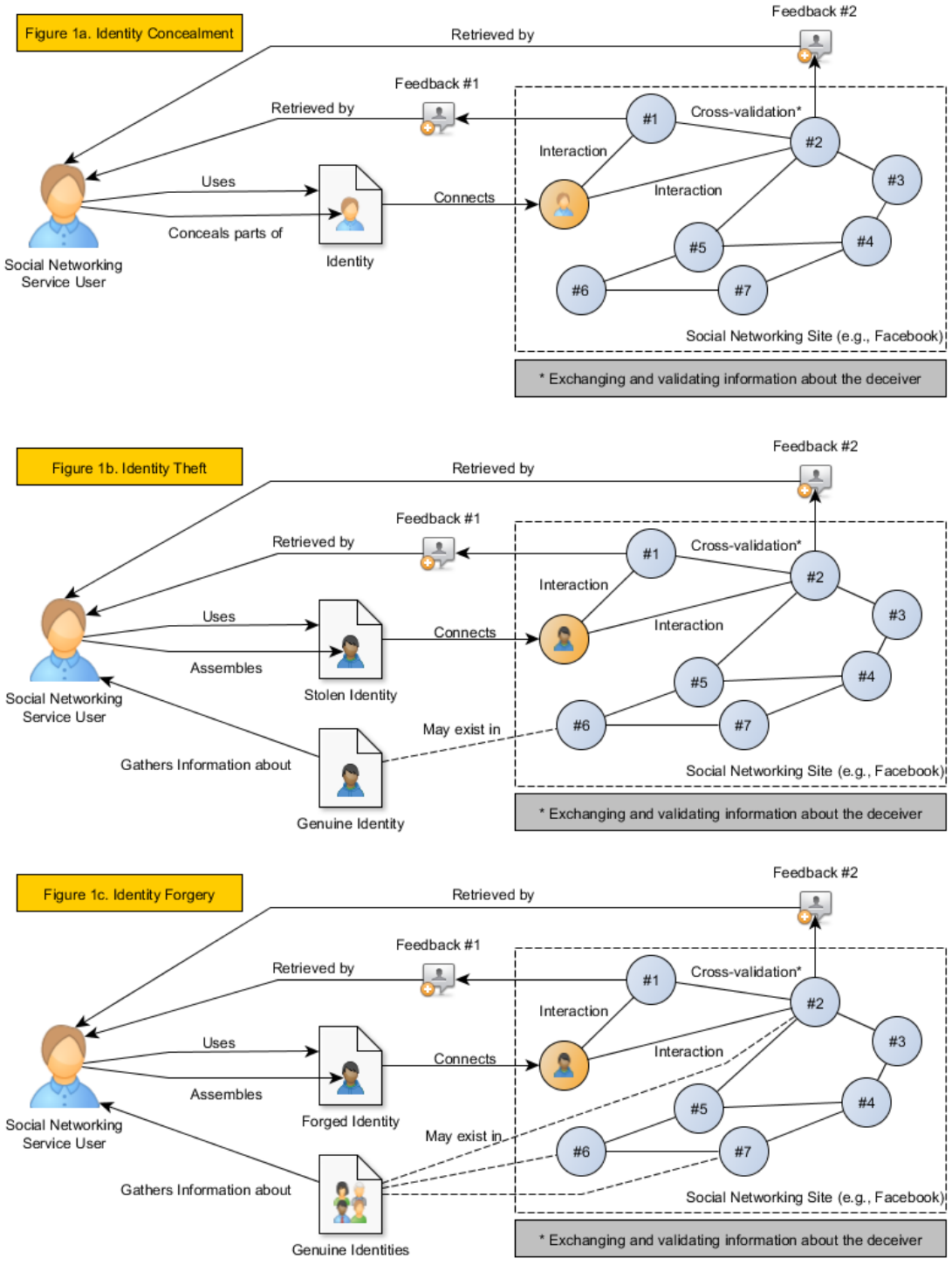

Figure 1: Three types of identity deception

There are various motivations behind deception many of which apply to both online and offline settings. Buller & Burgoon [6] have proposed three categories of motivations behind deception which also apply to identity deception. The motivations include: instrumental (e.g., maintaining power of influence over a victim), relational (e.g., maintaining a relationship), and identity-based (e.g., avoiding embarrassment). Deception is a goal-driven intentional act. Identity deception becomes a tool which aims to satisfy these motivations. Ultimately, the specific motivation in mind will determine the type of identity deception (concealment, theft or forgery).

People using SNS tend to have more online friends than real-life friends. There is no way to verify who is telling the truth and SNS users often share their personal information even when they knowingly admit that there are privacy issues in such virtual spaces [8]. Aside from this user mindset, the design (in terms of the amount of information allowed to be transferred and how) inherently allows deceivers to be more flexible in manipulating profile information and the way they self-present themselves to potential victims. SNS provide users with the opportunity to manage their personal profiles and have access to a level of media richness (the amount of information that can be transferred over a finite time) that is more favorable compared to other types of social media (e.g., collaborative project, blogs, microblogging). In addition, most of these SNS allow for quick registration without or with limited identity confirmation (e.g., Short Messaging Service verification). The lack of identity control and verification mechanisms makes it easy for deceivers to impersonate anyone they want and attempt to connect with people within and outside an identity's existing social network.

3. Detection of Identity Deception in Social Networking Services

Deception detection in SNS can be achieved from two perspectives: a user's ability to detect deception and a developer's ability to implement detection mechanisms in a SNS. The latter can be applied as a detection technology that enhances human deception detection or can be fully automated.

3.1 Identity Deception Detection in SNS by Users

Users in SNS have a limited ability to detect identity deception. They can pick up cues from the environment in which interaction takes place that have been manipulated (e.g., a photograph that looks edited) by a deceiver and interpret these by understanding a deceiver's goals. Previous research has demonstrated that detection using this method by users has a success of around 50 percent while other studies obtained an even lower success of 34 percent [3].

One of the biggest factors in detecting deception is time. A study involving respondents who had to recall detecting a lie in their lifetime and then answer a set of questions found that detection is a process that takes anywhere from a few days to months [9]. This can be the case in SNS where identity verification is not possible and the asynchronous nature of the medium of communication may result in significant delays for a user to detect deceptive cues. However, SNS provide a historical record and connections to others to triangulate and verify information retrieved by a potential deceiver. In the same study, individuals relied on third parties and physical evidence to uncover the truth; this is a major benefit in SNS where historical records are kept potentially indefinitely. The challenge, however, remains that detection rates still remain low by users.

Given the above, users who allow for more time to pass before trusting another user and who use their social network connections to verify a potential third party are more likely to detect

deception. Furthermore, one of the factors that affect the difficulty in achieving deception for a deceiver is his/her Information and Communication Technology (ICT) literacy [2]. Therefore, it is in the best interest of users to increase their understanding of ICT and in this context, SNS should provide educational content (e.g., what is a secure http connection and what can and cannot protect us from) for users.

3.2 Identity Deception Detection in Social Networking Services by Developers

Over the years, deception detection techniques have been focusing on theories and methods that detect *leakage cues* and *strategic decisions* [10]. Leakage cues describe identifiable signals that are unknowingly broadcasted by the deceiver due to a cognitive overload (trying to achieve multiple objectives at the same time). Strategic decisions are choices that are intentionally made by a deceiver in an attempt to deceive others and they provide detectable deviations from a non-deceiver baseline behavior. Both approaches aim to detect deception through *verbal* [4], [11], [12], *non-verbal* [13] and *physiological* cues [14]. Verbal communication includes text and auditory data.

We argue that given the design of SNS, developers will find it a challenge in identifying physiological and non-verbal cues in an online environment and translate them into useful data for deception detection. In contrast, in the real world, deception detection methods that use physiological cues such as a polygraph are widespread and even more advanced applications such as brain imaging [15], facial thermal imagining [16] are considered. Many of these biometric deception detection techniques are considered unobtrusive and therefore preferable [14]. To the best of our knowledge, there are no commercially available SNS that incorporate physiological responses (e.g., measuring heartbeat or sweating) for individuals at the moment,

however, in the future such biometrics may become available and they could be used for deception detection. While physiological cues are limited, there are currently opportunities for non-verbal cues in cases where video is incorporated or by measuring user activity on a SNS which can also be considered as a non-verbal behavior.

One of our first suggestions on detecting deception is to focus on non-verbal behavior cues available through video. Deception detection with non-verbal cues such as the use of video capturing technology has been used in the real world with encouraging results. Blob analysis for head and hand movements has been used experimentally with positive results [13]. We argue that the method could be used in SNS as an aid tool to detect movements that are too subtle for the human eye to detect. It is computationally inefficient and requires a training sample from which one could establish some baseline. As stated by the authors of the study, given the continuous improvements in computing technologies, this method may be feasible to implement in large-scale projects in the near future. However, a deceiver is likely to avoid providing individuals with video evidence unless the goal is identity forgery (e.g., the creation of a brand new identity) where no previous visual characteristics are associated with an identity.

We argue that, given the ease of uploading images to social networking profiles and evidence of past cases where people have uploaded fake pictures on their social networking profiles, identity concealment or identity theft is more likely to involve the use of images. Digital image forgery has been made readily available to users through software that can produce almost indistinguishable images. In effect, an individual can obtain publicly available images of their victim and post-edit them to enhance their identity deception. Technology that can help detect forged images is already available and has a high success rate. Methods for evaluating forged images exist that detect inconsistencies created by resampling images without any watermarks present or by looking at inconsistencies in the compression artifacts [17], [18]. Such methods

demonstrate that detection of forged images is possible and computationally feasible to be implemented on small-scale SNS.

Another type of non-verbal user activity to use for deception detection in SNS is the social context (e.g., employment history or social connections of individuals which can be used as evidence of a user's identity). A study has demonstrated that the accuracy of deception detection increases when a user's social context features are included in the detection analysis [7]. Furthermore, an additional potential source for deception detection is a user's network and in particular family ties can be used to determine the hereditary predisposition to lying. Findings on a genetic origin for lying discovered that some of the variance in the tendency for deception can be attributed to family ties [19] and genetics [20]. SNS not only can use past deception incidents to keep a history on individuals but also transfer a weighted score to their offspring which can be monitored closely by detection software. Furthermore, there are several computationally feasible solutions especially for small SNS [2]. The presence of social networking data provides new opportunities for detecting deceivers.

To date, non-verbal user activity has not been explored as a possible solution for identity deception detection in SNS. User non-verbal activity is the interaction that the user has in the virtual social networking environment and any interaction with it (e.g., number of messages sent in the past 6 hours). Just like in the offline world, we assert that these aforementioned activities can be identified and a baseline can be built using Expectancy Violations Theory (EVT) to support deception detection. EVT describes how people have expected behaviors and deviations from these behaviors can be seen as indicators of deception. By establishing models using these baselines, deviations can be detected. A recent study has demonstrated that this approach can provide near human predictive accuracy in detecting fake accounts in Wikipedia [21]. Furthermore, SNS users are less aware that this activity is monitored and therefore are

less likely to adjust their behavior which may increase detection accuracy when the behaviors deviate from the baseline.

Unlike the previous solutions we have proposed which have not been tested in SNS, *verbal communication* (e.g., audio or text) is a good candidate source for deception detection. While audio implementation in SNS is limited, deceivers may use it to convey their message. One method for detecting deception through an audio channel is by listening to acoustic/prosodic features (e.g., pitch, energy, speaking rate, etc.). The same method can be implemented in SNS that make use of audio communication for their users. Audio data can also be converted into text using voice recognition software to which additional deception detection analyses can be applied. A combined approach of using lexical features (transcribed speech) as well as acoustic/prosodic features has been used with promising results in terms of detecting deceivers [22]. The method can potentially be implemented in a SNS as an assistive tool for administrators when investigating suspect cases of identity deception.

In recent years, most research efforts [4], [11], [12], [23] on deception detection have focused on text. SNS make it easy to manipulate text-based content and identity deception can be quite successful. Textual analysis involves detecting leakage cues or strategic decisions made by deceivers who leave traces behind. One of the methods used for deception detection is by applying similarity analysis on various texts [11]. This is achieved by analyzing texts that came from two different authors using natural language processing and then evaluating the percentage of common text features. Individuals operating two accounts (e.g., one for valid purposes while the other for deception) were identified by analyzing text-based features (e.g., parentheses count, punctuation count) [11]. The technique has shown 68 percent accuracy in detecting identity deception. However, similarity analyses incur high computational overheads ($O(N^2)$) and they do not address issues where a deceiver is not part of the SNS or has not

delivered enough content on one of his/her accounts. In such cases, detecting deceptive cues in the text such as those found in phishing emails may prove to be a more successful strategy.

All methods we have discussed in this section have an associated cost. Detection is a computationally intensive task with large amounts of information that need to be processed (ideally) in real time. Identifying the optimum solution between efficiency and performance may be the most challenging task for developers.

4. Prevention of Identity Deception in Social Networking Services

Another issue that has not been previously addressed by the deception literature is identity deception prevention in SNS. In this work, we focus on deception prevention from a user and developer perspective. By taking a proactive approach both users and developers can discourage identity deception.

4.1 Identity Deception Prevention from a Developer Perspective

SNS developers have the option to implement security measures in the design of a SNS or use design elements to apply psychological pressure to deceivers that can help decrease the likelihood for identity deception.

4.1.1 Prevention through Secure Design of –Social Networking Services from a Developer View

The policies and design of SNS can have a significant impact on the detection of online identity deception in these sites. The lack of verifiability and accountability of user accounts has prominently altered users' mentality and perception of what these services ought to be.

SNS are supported by user-generated content and a constant participation by current users. Today, anyone can register a new account on a SNS without verifying his/her identity (with some minor exceptions such as name change which requires some government identification document in many cases for Facebook). The success of identity theft may not be long term because incidents are reported and dealt with; identity forgery is a lot easier because of the inherent design of SNS allowing people to freely create new identities by registering new accounts.

Even if mechanisms for detection are placed into a SNS, the computational load incurred by detection mechanisms along with having users creating new accounts with limited verification (usually just email verification) will make detection an infeasible strategy. One possible solution is to use preventive mechanisms in conjunction with detection mechanisms. For instance, Facebook has implemented additional security features where Short Message Service (SMS) verification is required to activate additional features on a Facebook account. Accounts not fully activated could be monitored closely for deception. A phone number can be associated to only one account and needs to be from the country where the user registered for the SNS service. However, we note that such measures may inadvertently confuse users, reduce the number of users registering and can be easily bypassed using disposable phones as well as web SMS services.

One possible strategy we have identified is to gradually give more permissions to users (e.g. ability to connect to more than two users) once they satisfy certain criteria or a certain amount of

time has passed. Many online communities use the principles of gamification (providing users with awards and levels) to not only encourage participation but to also provide control over individuals wanting to do damage. Incorporating security features along with such measures will not only increase the difficulty for deceivers but also reduce the impact of identity deception to other users. In addition, empowering users to moderate SNS elements can have a preventive effect for identity deception. For example, lists on Facebook (groups) tend to have less irrelevant content (posted by fake accounts) than lists on twitter (posts based on associated tags) in part due to the ability to assign multiple authorized users to moderate them.

Furthermore, biometric authentication may be used in the future for deception prevention especially with recent advances in the field of Virtual Reality (VR). A combination of non-verbal physiological responses such as eye tracking or keyboard strokes may become available for developers to experiment with for identity deception prevention [24], [25]. Iris recognition in particular is a system that can be used for deception prevention although efforts need to be made to address the potential for the system to be deceived by fake irises [26]. Such digital fingerprint methods can be used to evaluate if the content has truly originated from the right identity and generates a complete user profile "fingerprint." Another application which can be used at the point of authorization is also facial recognition however deceiving such a system is currently possible with changes to appearance such as modifications to one's haircut [15].

4.1.2 Prevention by Applying Psychological Pressure from a Developer View

Elements in the design of SNS can help inhibit deception. The most important aspect of social media is their media richness which can be described as the amount of information allowed to be transferred through a medium in a given time interval. SNS exhibit a higher media richness

(providing more cues and reducing ambiguity) than other types of social media. Media richness has been found experimentally to be linked indirectly with the accuracy of human deception detection [27]. This is achieved by affecting a potential victim's degree of suspicion for deception and also his or her truth-bias (the expectation that people are truthful). By increasing media richness (e.g., incorporating more features to allow for synchronous communication as well as asynchronous) a SNS developer will increase a user's suspicion and in turn the ability to detect deception.

However, increasing suspicion has an additional effect on inhibiting deception. Buller & Burgoon have argued that a potential victim's degree of suspicion will affect the behavior of the deceiver [6]. This can lead to a deceiver giving away more cues of deception or discouraging them in engaging in deceptive behavior. Deception and its detection have an evolutionary basis in many species to ensure strategic advantage over others [19]. Animals seek targets that are easy to be deceived. Similarly, we can expect that most deceivers in our species will not consider pursuing deception with difficult targets (e.g., individuals who are suspicious for deception due to their technological expertise). As the difficulty in achieving deception rises, so does the likelihood of engaging in deception. We propose that a developer of a SNS may make it more difficult for deceivers to succeed by increasing the suspicion levels of their potential victims (effectively increasing pressure on deceivers). By incorporating tracking on who is viewing one's profile, victims will appear to be investigating a deceiver's profile (raising pressure on the deceiver) and deceivers will be more exposed when investigating victim profiles (risking raising suspicion to their potential victims). Deceivers may find deception to be more difficult due to the overall increased exposure (e.g., more channels of communication and being more pressured by realizing that people look at their forged profiles). Furthermore, the increased pressure is also likely to lead a deceiver in making errors and raising suspicion on potential victims. Even the thought that a deceiver may be monitored by their target victim will raise the difficulty in

achieving deception forcing the deceiver to abandon plans or leading him/her to give away more cues of their deception which in turn will alert the victim.

4.2 Prevention of Deception in Social Networking Services by Users

For deception prevention for users we focus on measures that can uncover deception before they are deceived. This happens before the critical point when an individual makes a choice on accepting or rejecting a request for connection with a deceiver. Beyond that, if the result of the choice is acceptance with a trust provided to a deceiver's target information then they have been deceived and are likely to endure some loss (due to information that a deceiver obtains from the newly initiated connection). There may be connections that users do not attach the same level of trust as others, however, from a deceiver's perspective once the necessary level of trust has been achieved to obtain target information then deception has been a success. The goal of prevention is to identify identity deception before that loss occurs (before a connection with attached trust has been initiated).

Users can take measures to help prevent from falling victims of identity deception. One effective strategy we have identified is to use multiple resources (different SNS) to establish whether an identity is valid before accepting a connection. This cross-validation can be effective especially if one considers that many profiles today overlap between different SNS. For example, a young adult is likely to maintain profiles in multiple SNS. By verifying an identity's validity, an individual can prevent himself/herself from being deceived.

Another strategy that can be used by SNS users can be based on the signaling theory [28]. Signaling theory posits that there are assessment signals (evidence that are hard to fake such

as a government identification) and conventional signals (evidence easier to fake such as marital status on one's social networking profile). There is prevalence on the Internet for conventional signals and having the mindset that a conventional signal is sufficient to verify one's identity could lead to erroneous conclusions. Instead, we suggest that users should understand the difference between these two types of signals and ask for additional evidence (preferably assessment signals).

Finally, users can utilize their social capital (e.g., their social connections) to verify the identity of a potential new connection. This is a successful strategy in the offline world in terms of deception detection [9] but it can also be used proactively for prevention. For example, an individual may employ a strategy where new friend requests would not be accepted until another person in their social network has verified the new friend or the friend's request is submitted using a referral. Currently, Facebook does allow individuals to suggest their friends to others.

5. The Need for a Coordinated Effort

There are several issues that arise with identity deception in SNS. Some of these include damage to one's social health, financial loss from information obtained through identity deception as well as life threatening consequences for victims (e.g., using identity deception to stalk and eventually prey on victims). Deceivers have a plethora of tools at their disposal and can abuse the system by masquerading as legitimate users. To detect and prevent identity deception, we need to develop simple and easy-to-use and cost effective techniques.

It becomes apparent that one single solution cannot address the issue of identity deception and that we cannot talk about prevention without understanding detection and vice versa. A

summary of all detection and prevention strategies presented in this article is provided in table 1.

Detection		Prevention		
User	Developer	Developer		User
		Security	Psychology	
Content monitoring and time is required for successful detection	Analyzing video for non-verbal deception cues	Identity verification measures upon registration	Increasing media richness through design	Verifying identity and information of recipient through multiple sources
Detection through third parties and triangulating information	Detecting forged or manipulated images	Gradually enabling features based on score increments gained through participation on SNS	Increasing user suspicion on others through design	Requiring additional evidence that are not conventional signals
Training	Social network analysis and node attributes analysis	Biometrics and Digital Fingerprinting	Increasing perception of suspicion in the eyes of deceiver through design	Using individuals within social network to verify identity of a new party
Requiring additional evidence and applying critical thinking	Analyzing non-verbal user activity		Enabling user authorized moderation on SNS elements	
	Audio analysis for abnormalities (e.g., voice pitch)			
	Text analysis using techniques (e.g., Natural Language Processing)			
	Similarity analysis to detect multiple accounts meant for identity deception			

Table 1: Summary of techniques to detect and prevent identity deception in SNS from a user perspective and a developer perspective.

Prevention methods may have unexpected adverse effects on SNSs in which they are implemented. Identity verification may drive away users from SNSs which rely on user-generated content to sustain operations. The gradual enabling of services may similarly drive away users who would not have an opportunity to appreciate the full range of options given to the users by a SNS. Putting psychological pressure on users has the potential to enhance user aversion to a service. In cultures where surveillance issues are prevalent users may even react negatively against these protective measures. In contrast, enabling users by training to protect their privacy, may also lead to user hostility and reduce trust among users. A SNS that may gain the reputation of a network infested with deceivers may disrupt interaction between users. These effects have not been studied in the context of deception prevention in SNS and more research is needed.

The cost of implementation for deception detection and prevention needs to be considered. Informing users and making them more aware is presumably cheaper than having to develop detection algorithms or do a complete redesign of the software. Most of the techniques described here would need a substantial development and implementation effort because at moment ready to implement code for these solutions is scarce. Future research directions should examine and evaluate the efficiency of these solutions directly in the SNS environment or examine the potential for detection and prevention strategies to be provided by third parties. The latter, should also include a discussion on privacy concerns.

Finally, some of these solutions may be implement at an end user's device with no additional concerns but company's privacy policy and terms and conditions. Other solutions, however, may

require change in the infrastructure and industry leaders taking a lead in promoting such solutions. For example, we could allow for pinpoint accuracy of an IP address through an ISP's customer record. This can potentially eliminate identity deception but such a measure can conflict with many of the ideals of what a "free" internet should be. Activist groups will effectively be silenced through such a change. Additionally, this measure also comes into conflicts with users that access the Internet through proxies or virtual private networks or even anonymity networks such as Tor. Making users more identifiable online will be seen as moving backwards in terms of our technological advances in modern networks. However, other solutions may be supported by industry leaders if users demand them. For example, identity theft may be preventable if individuals may choose to contribute to a database their real names, location a set of photos along with other unique data that identify them. The database can cross-reference with existing records to verify that no duplicates exist (similar to the approach used by [4]) and provide users with a unique login. This login can be used then by social networking sites. The feature can alo be optional with social networking sites occasionally verify users using the identifier data provided by such a system (such as personal photos) and detection techniques (e.g., facial recognition) to verify that no other users are attempting to use another's identity. However, promoting such a system can pose significant challenges for the industry if lessons are to be learned by attempts such as OpenID or ORCID.

6. Conclusion

Detecting deception in SNS and preventing it continue to be a challenge for developers. Over the last decade online identity concealment, identity theft and especially identity forgery have been made possible to virtually anyone who has Internet access. Attackers are always striving to develop innovative techniques to deceive their victims or gain access to people's social networks and attack neighboring targets in those social networks. While we are focusing on

securing our devices and infrastructure we cannot ignore the fact that humans keep operating them. The stakes of deception are high not just for the individuals and their personal lives but for organizations as well which may be at risk from the information obtained through online identity deception. We have made some progress in detecting deception in SNS with recent computing advances which have made some methods computationally feasible. The number of SNS users keeps increasing daily and users will continue to be at risk of falling victims to identity deception. As a result, we need to continue to explore novel, cost-effective, scalable detection deception techniques and SNS designs aimed at protecting users of these SNS.

7. Acknowledgements

We express our gratitude to Hilarie Orman for the time she has spent on early drafts of this paper and for her valuable comments and feedback on various parts of this work. We would also like to thank the anonymous reviewers for their useful feedback which help us improve the quality and presentation of this paper.

References

[1] X. (Sherman) Shen, “Security and privacy in mobile social network [Editor’s Note],” *IEEE Netw.*, vol. 27, no. 5, pp. 2–3, Sep. 2013.

[2] M. Tsikerdekis and S. Zeadally, “Online Deception in Social Media,” *Commun. ACM*, vol. 57, no. 9, pp. 72–80, 2014.

[3] T. R. Levine, R. K. Kim, H. Sun Park, and M. Hughes, “Deception Detection Accuracy is a Predictable Linear Function of Message Veracity Base-Rate: A Formal Test of Park and Levine’s Probability Model,” *Commun. Monogr.*, vol. 73, no. 3, pp. 243–260, Sep. 2006.

[4] G. A. Wang, H. Chen, J. J. Xu, and H. Atabakhsh, “Automatically detecting criminal identity deception: an adaptive detection algorithm,” *IEEE Trans. Syst. Man Cybern. Part A Syst. Humans*, vol. 36, no. 5, pp. 988–999, 2006.

[5] P. Ekman, “Deception, Lying, and Demeanor,” in *States of Mind : American and Post-Soviet Perspectives on Contemporary Issues in Psychology: American and Post-Soviet*

Perspectives on Contemporary Issues in Psychology, D. F. Halpern and A. E. Voiskounsky, Eds. Oxford University Press, 1997, pp. 93–105.

[6] D. B. Buller and J. K. Burgoon, “Interpersonal Deception Theory,” *Commun. Theory*, vol. 6, no. 3, pp. 203–242, Aug. 1996.

[7] J. Li, G. A. Wang, and H. Chen, “PRM-based identity matching using social context,” in *Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*, 2008, pp. 150–155.

[8] A. C. Squicciarini and C. Griffin, “An Informed Model of Personal Information Release in Social Networking Sites,” in *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, 2012, pp. 636–645.

[9] H. S. Park, T. Levine, S. McCornack, K. Morrison, and M. Ferrara, “How people really detect lies,” *Commun. Monogr.*, vol. 69, no. 2, pp. 144–157, Jun. 2002.

[10] S. L. Humpherys, K. C. Moffitt, M. B. Burns, J. K. Burgoon, and W. F. Felix, “Identification of fraudulent financial statements using linguistic credibility analysis,” *Decis. Support Syst.*, vol. 50, no. 3, pp. 585–594, Feb. 2011.

[11] T. Solorio, R. Hasan, and M. Mizan, “A Case Study of Sockpuppet Detection in Wikipedia,” in *Proceedings of the Workshop on Language Analysis in Social Media*, 2013, pp. 59–68.

[12] C. E. Lamb and D. B. Skillicorn, “Detecting deception in interrogation settings,” in *Intelligence and Security Informatics (ISI), 2013 IEEE International Conference on*, 2013, pp. 160–162.

[13] G. Tsechpenakis, D. N. Metaxas, M. L. Jensen, and J. Kruse, “Blob Analysis of the Head and Hands: A Method for Deception Detection,” in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 2005, p. 20c–20c.

[14] A. Elkins, S. Zafeiriou, M. Pantic, and J. Burgoon, “Unobtrusive Deception Detection,” in *The Oxford Handbook of Affective Computing*, R. Calvo, S. K. D’Mello, J. Gratch, and A. Kappas, Eds. Oxford University Press, 2014.

[15] B. S. Kumar, M. Gudavalli, and P. Radhika, “Emerging Applications of Face Biometrics and Its Deception,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 6, pp. 5492–5496, 2012.

[16] I. Pavlidis and J. Levine, “Thermal Facial Screening for Deception Detection,” in *Prcceedings of the Second Joint EMBSEIMES Conference*, 2002, pp. 1143–1144.

[17] S. Ye, Q. Sun, and E.-C. Chang, “Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact,” *Multimedia and Expo, 2007 IEEE International Conference on*. pp. 12–15, 2007.

[18] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting traces of resampling,” *Signal Processing, IEEE Transactions on*, vol. 53, no. 2. pp. 758–767, 2005.

[19] C. Bond Jr. and M. Robinson, “The evolution of deception,” *J. Nonverbal Behav.*, vol. 12, no. 4, pp. 295–307, 1988.

[20] P. J. Loewen, C. T. Dawes, N. Mazar, M. Johannesson, P. Koellinger, and P. K. E. Magnusson, “The heritability of moral standards for everyday dishonesty,” *J. Econ. Behav. Organ.*, vol. 93, pp. 363–366, Sep. 2013.

[21] M. Tsikerdekis and S. Zeadally, “Multiple Account Identity Deception Detection in Social Media Using Non-Verbal Behavior,” *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 8, pp. 1311–1321, 2014.

[22] J. Hirschberg, S. Benus, J. M. Brenier, F. Enos, S. Friedman, S. Gilman, C. Girand, M. Graciarena, A. Kathol, and L. Michaelis, “Distinguishing deceptive from non-deceptive speech,” in *Interspeech 2005*, 2005, pp. 1833–1836.

[23] T. Qin, J. K. Burgoon, and J. F. Nunamaker Jr., “An Exploratory Study on Promising Cues in Deception Detection and Application of Decision Tree,” in *Proceedings of the 37th Annual Hawaii International Conference of System Science*, 2004.

[24] D. Bhattacharyya, R. Ranjan, A. A. Farkhod, and M. Choi, “Biometric Authentication: A Review,” *Int. J. u- e- Serv. Sci. Technol.*, vol. 2, no. 3, pp. 13–28, 2009.

[25] J. L. Wayman, “Digital signal processing in biometric identification: a review,” *Image Processing. 2002. Proceedings. 2002 International Conference on*, vol. 1. pp. I–37–I–40 vol.1, 2002.

[26] M. Kanematsu, H. Takano, and K. Nakamura, “Highly Reliable Liveness Detection Method for Iris Recognition,” in *SICE Annual Conference 2007*, 2007, pp. 361–364.

[27] R. J. Boyle and C. P. Ruppel, “The Impact of Media Richness, Suspicion, and Perceived Truth Bias on Deception Detection,” in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 2005, p. 20a–20a.

[28] A. Zahavi, “The Fallacy of Conventional Signalling,” *Philos. Trans. R. Soc. London. Ser. B Biol. Sci.*, vol. 340, no. 1292, pp. 227–230, May 1993.