THE ISSUE OF TRUST IN COMPUTER MEDIATED INTRODUCTIONS (CMI)

by

Borke Obada-Obieh

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of
MASTER OF COMPUTER SCIENCE

at

Carleton University
Ottawa, Ontario
September 2017

To my dad, my greatest cheerleader. I love you now and forever. Keep singing with the angels.

Table of Contents

List of Tables

List of Figures

Abstract

The problem of trust is one of the more prominent security issues in online communications. In this thesis, we propose a new security threat model, computer mediated introductions (CMI), where individuals are introduced online for the purpose of interacting offline. This is a problem that has not been specifically studied in the literature, even though aspects of it have been covered elsewhere. We therefore critically analyze the issue of trust and reputation in CMIs with the aim of improving trust on these platforms. In one of the most popular forms of CMI today, online dating, our findings show that existing standard mechanisms are not sufficient to establish meaningful trust on the platform. While we propose some potential alternative mechanisms for establishing trust in CMIs, the key contribution of this work is to identify the security challenges that arise in computer mediated introductions as a previously unrecognized class of security problems. We believe CMI has the promise of eventually becoming an independent research area, one that could make a real difference in how people meet, whether for business, fun, friendship, or romance.

Acknowledgements

I want to express my sincere appreciation to my adviser, Anil Somayaji, who has not just been an incredible supervisor but also a great friend. I am truly grateful for the countless hours and efforts he has put into making sure I become a great researcher. He has been a remarkable coach who is always willing to assist me as much as possible. When I first asked Anil to be my supervisor, he knew I had very limited research skills, but he somehow believed in me and decided to invest so much resources towards my growth. Anil saw in me what I didn't even see in myself and he has encouraged me every step of the way. He is intelligently knowledgeable about almost any topic and he always knew how to push me to get things done on time; but with just the needed amount of push such that it's never too much or too little. His diligent approach to work as inspired me over the years and has made me a better person. It is indeed an honor and a privilege to have worked with him.

I will also like to thank Sonia Chiasson in whose usable security class I first fell in love with the concept of usable security and privacy. I birthed this research as a simple idea in her class and it has somehow metamorphosed over the years into such an extensive research. I am thankful to her for taking time to read my write-ups and for her extensive feedbacks. I also thank my defense committee members, Carlisle Adams and Robert Biddle, for their comprehensive reviews and insights during the defense. I also appreciate David Mould for chairing the defense committee. I am also grateful to members of the Carleton Computer Security Lab, especially Nilofar and Ann who were always fun to interact with.

I truly appreciate my mum and siblings, Suror and Kesiena, who have been a huge support network for me. I am thankful to them for the numerous hours spent on the phone with me to ensure I am doing well. I thank my dad also, who inspired me to get a Master's degree in the first place.

Ultimately, I thank God by whose power I live, breathe, and have my being. To Him alone be all the glory.

Chapter 1

Introduction

The issue of trust has been studied for many years and cuts across various disciplines, including mathematics, psychology, computer science, sociology, economics, management, human and computer interaction (HCI), and marketing [39, 85, 91, 90, 125, 144, 214, 221, 244, 282, 126]. Trust can be viewed as a "belief based off the expectation of other's behavior or intention" [229]. It is a notion that "another's action will be favorable to oneself" [87]. Hence the outcome of trust is largely based on the attitude of another. Baier et al. noted that we do not have absolute control over the things we care about the most, such as our lives, the safety of flying in airplanes, our reputations, our emotions, and medical care. We cannot singly and completely take care of those things all the time or determine what happens to them. To make up for this, we must place them in the care of someone who can ruin them or destroy them, as they please. But they, however, must be placed in such positions. The issue of trust therefore is centered on, how do we determine who to trust and what exactly is being entrusted to the care of these individuals [18]. For example, a person walking through the crosswalk after sighting the pedestrian signal has chosen in that instant to entrust her wellbeing to the driver, trusting that the driver will wait and not continue driving.

While trust is important in both online and offline communications, computers have become an important part of interpersonal relationships across the globe [135]. Computer mediated communication (CMC) is essential to how we conduct business and maintain personal relationships [27, 135, 148, 34, 104]. Observable physical cues, even though sometimes ineffective, have been put in place as offline prompts used to detect deception and to determine who to trust and what can be placed in their trust. However, such cues are missing from online interactions. Therefore, when we go online, we must be wary. An attempted e-commerce purchase can lead to fraudulent credit card transactions. Following the wrong link in an email can result

in compromised credentials. Accepting the wrong social media connection request can compromise our privacy.

While all online interactions entail some risk, some interactions are clearly riskier than others. Among the riskiest interactions are ones that cross over from the virtual to the physical. When an online interaction goes bad, we may suffer harm to our bank account or our reputation. When an in-person interaction goes bad, it may end in violence or death. It is therefore natural that we want additional guarantees for potential in-person interactions with strangers we meet online.

Here we define computer mediated introductions (CMI) as a type of computer mediated communication in which online interaction occurs between strangers for the purpose of (eventual) in person interactions. Two classes of CMI are business CMI and personal CMI. Business CMIs involves introducing people online to meet offline for the sole purpose of exchanging goods or services for monetary value. We do not classify periodic subscription for a service that requires monetary exchange as a business CMI. However, if monetary value has to be exchanged each time services or goods are being provided by the CMI, then the CMI is classified as a business CMI. Examples of business CMIs are Airbnb, Uber, and Vayable, amongst others. In personal CMI, monetary value is not attached to the exchange made; instead, people are introduced online and meet offline based on shared interests, hobbies, or to carry out similar activities. Couchsurfing and dating sites are examples of personal CMI. In some cases, some CMI platforms could serve as a means of introducing people for both business and pleasure, thereby serving as a combination of both CMIs. Examples of those include Meetup.com, Craigslist, and Kijiji.

1.1 Motivation

As computers become more and more central to how we interact socially, increasingly computers will be the ones establishing initial social connections [27, 135, 148, 34, 104]. These introductions are key points of vulnerability, leaving individuals subject to attacks on their finances, emotional stability, and physical safety. The purpose of computer mediated introductions is to put in contact people who do not know each other. As a result, identifying unsolicited and spontaneous messages that are the core of traditional anti-fraud online activities does not have any meaning when applied to

CMIs.

The major challenge in CMI is establishing trust in the face of the "slippery virtuality of the online world" [81]. Brym et al. [31] discloses that 89% of their participants were of the opinion that people they meet online may not tell you the truth about themselves, and 85% agreed that "people met online might be hiding something." While the interactions that occur online between two strangers can be likened to those seen offline in a social setting, such as a bar; however, it should be noted that the expectation for people to be truthful in both settings are significantly different. For instance in dating sites, ideally people are involved in online interactions for the purpose of having an offline romantic relationship. As such it is expected that both parties are truthful in their representations of themselves both online and offline. However, in a bar setting there is no such expectation. Also in such a setting it is difficult to lie about things such as a person's weight or height, but online those are easier to fake.

In other CMCs where communication is strictly limited to online interactions, users mainly face the risk of being defrauded; however, CMI users are exposed to risks associated with potential bodily harm. For example, we can contact individuals representing an online company, say for services or deliveries such as Amazon, to have goods returned. But in CMI interactions such as Airbnb, we cannot necessarily 'return' a person coming to spend the night in an Airbnb listing.

Where the online interaction is a continuation of an already existing social relationship, such as members of a community organization in the same social group corresponding via a Facebook page, the risks are lower because nobody is a complete stranger. When people meet for the first time online for social purposes as seen in dating sites, the risks are much more significant. We focus on the importance of building trust in personal CMI, specifically dating sites, because we believe this is the most vulnerable form of CMI. Dating site scammers are known to exploit the vulnerable emotional state of unsuspecting users, making their attacks more effective [69]. Their attacks do not just involve monetary loss but they include emotional trauma, violence, sexual assault, and ultimately death [69]. Therefore developing effective trust mechanisms in dating sites will greatly improve the security of other CMIs.

Online dating platforms themselves, have become increasingly mainstream [237,

89, 236, 225, 203, 43]. As of August 2003 in total about, "40 million unique people visited dating sites" [82] and in 2006, about 7 million had been on dates with someone they met on "online personal advertisements" [147]. In 2013, one in every ten American had used a dating site or application, and 66% of these users had gone a step further to set up dates with people they met on these platforms [237]. In 2014 it was reported that 38% of single adults in the US had used an online dating site [89]. New reports emerged in 2015 that the use of dating sites had increased from 10% in 2013 to 27% among users ranging from 18–24 years old. The use of the platform also doubled from 6% to 12% among users ranging from ages 55–64 [236]. A popular dating service, Plenty of Fish alone, had an estimated 100 million users as of 2015 and 3.5 million active members per day [197]. Rosenfeld et al. and Couch et al. [225, 43] both highlighted the importance of this relatively recent type of interaction. They noted that online dating has partly displaced family gatherings, schools, and parks as places to meet potential partners, and has also taken precedence in the "social lives" of people [81]. Although their precise format and target audience vary widely, their basic format remains the same. Individuals create profiles for other users of the site to browse. While these profiles do not contain an individual's name, address, or other standard identifying information, these profiles do contain demographic information, personal statements, answers to standard questions, and (perhaps most importantly) pictures. Typically, other users of the site can search for and view these profiles. When a suitable profile is found, a user can send the profile's owner a pseudonymous message, thus beginning a conversation. The conversation's goal is to determine whether to proceed to the next step—meeting in person. Online dating sites thus facilitate highly personal interactions between people who otherwise would be strangers. Therefore, the key problem of establishing sufficient trust to move the interaction from online to in person becomes much more crucial on these platforms [69, 43, 31, 66, 111, 215, 35].

1.2 Main Contributions

This thesis makes the following contributions:

1. **Defining computer mediated introductions (CMI) as a threat model and an independent research area.** Research has generalized all forms

of computer mediated communications (CMC) [36], classifying these interactions under regular online communications, and as such implementing standard mechanisms in an attempt to establish trust on these platforms. Our research identifies the area of computer mediated introductions as a separate field of research where better and strategic trust mechanisms need to be put in place as a result of the higher level of possible risks. Some of the standard trust mechanisms are also ineffective when applied to personal CMI, especially online dating sites, due to the nature of interactions that occur on this platform.

2. **Evaluation of trust mechanisms used in CMIs.** We review, compare, and critically analyze the various trust mechanisms employed by different business and personal CMIs, specifically Airbnb, Uber, Meetup.com, Vayable, Couchsurfing, Craigslist and Kijiji. We provide alternative strategies that could be implemented to improve trust on these CMI platforms.

3. **Clearly define the threat model of online dating sites.** We carry out an in-depth analysis of the threat model of a typical online dating site, covering the possible threats that could exist while making use of the platform. We also describe the ideal trust mechanisms of dating sites and compare them with those currently being employed by three popular online dating services, Match.com, Plenty of Fish, and Tinder. We determine if the current mechanisms used are sufficient to establish trust and better secure users of online dating services.

4. **User study showcasing user's strategies for ensuring safety.** We present a user study carried out to evaluate how users develop trust when making use of personal CMIs.

5. **Proposing strategies and alternative mechanisms for the development of a trustworthy dating site model**, which could ultimately lead to better security on other forms of CMI.

6. **We most importantly identify computer mediated introductions as an understudied area of computer security.** We specify the security challenges that arise in computer mediated introductions as a previously unrecognized class of security problems, with the hope that the work will encourage others

to further study this challenge through user studies and the development of technical mechanisms specialized to the CMI problem.

1.3 Organization Of Thesis

The rest of the thesis is organized as follows. We review previous work on the problem of trust in both online and offline interactions in Chapter 2. We evaluate and analyze the trust mechanisms implemented by seven CMIs in Chapter 3. Based on the identified mechanisms, we propose methods that could be implemented in an effort at improving trust in those forms of computer mediated introductions. We present the threat model of dating sites in Chapter 4, identifying both user and dating sites' roles, and furthermore surveying the different scenarios related to the identified threats. In Chapter 5, we present the results of a user study done to find out if dating sites users are able to identify these threats for themselves. We furthermore evaluate the strategies users employ in deciding who to trust when interacting with people introduced through dating sites, and we determine if these mechanisms are effective enough to keep users safe. In Chapter 6 we critically analyze the trust mechanisms used by dating sites administrators. We compare those mechanisms with the ideal mechanisms defined in the threat model in Chapter 4, to determine if dating sites' mechanisms are sufficient to protect their users. We furthermore compare dating sites' trust mechanisms with those carried out by other CMCs, and we define the unique problem of establishing trust in online dating sites. In Chapter 7, we suggest alternative trust mechanisms that could be employed by dating sites and discuss the evaluation of the suggested mechanisms. In Chapter 8, we discuss the main contributions made, limitations, future work and we conclude.

1.4 Research Publications

During the course of this Masters degree program, the following publications have been produced,

1. Obada-Obieh Borke, Sonia Chiasson, and Anil Somayaji. " 'Don't Break My Heart!': User Security Strategies for Online Dating.", in proceedings of 2017

Workshop on Usable Security (USEC), February 26, 2017, San Diego, California, USA.

2. Obada-Obieh Borke and Anil Somayaji. "Can I believe you? Establishing Trust in Computer Mediated Introductions", in proceedings of 2017 New Security Paradigms Workshop (NSPW), October 1st-4th, 2017, Key West, Florida, USA.

Chapter 2

Background

The challenge with computer mediated introductions is fundamentally one of trust. Research has indicated similarities between online and offline trust [81, 213]. As such, to understand how trust works online, we review research done to establish trust offline and proceed to work on online trust.

This chapter is divided into five sections. In the first section, we review the concept of trust. In the second section, we evaluate the research carried out to ensure trust offline. We review work done in an effort to establish trust online in the third section and we discuss computer mediated introductions in the fourth section. We conclude the chapter in the fifth section.

2.1 The Concept of Trust

Research into security and trust online has been ongoing for over twenty years [86]. Luhmann argues that "humans would not even be able to face the complexities of the world without resorting to trust, because it is with trust that we are able to reason sensibly about the possibilities of everyday life" [142]. There are many definitions of trust; we review some of them here.

One definition of trust is that, "Trust is the willingness to be vulnerable based on positive expectations about the actions of others" [164]. Trust in a social context can also be defined as "the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible" [60].

From a psychological viewpoint, Deutsch explains the concept of trust thus, "An individual is confronted with an ambiguous path, a path that can lead to an event perceived to be beneficial (Va+) or to an event perceived to be harmful (Va-); he perceives that the occurrence of Va+ or Va- is contingent on the behavior of another person; and he perceives that strength of Va- is greater than that strength of Va+.

If he chooses to take an ambiguous path with such properties, I shall say he makes a trusting choice; if he chooses not to take the path, he makes a distrustful choice" [150].

Gambetta and Marsh explained trust from a mathematical perspective. While Marsh proposed a mathematical model for trust [150], Gambetta describes trust thus, "Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action. When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him. Correspondingly when we say that someone is untrustworthy, we imply that that probability is low enough for us to refrain from doing so" [87]. Bacharach and Gambetta further expounds on the concept, "In general, we say that a person 'trusts someone to do X' if she acts on the expectation that he will do X when both know that two conditions obtain: if he fails to do X she would have done better to act otherwise, and her acting in the way she does gives him a selfish reason not to do X" [16].

These definitions indicate that at least two people must be involved before the notion of trust can be put in place [220]. In other words, as Baier et al. [18] explains, for a trust relationship to occur, there is usually the "Trustor" who is the one trusting another, and the "Trusted", who is being trusted. Trust must exist between the "Trustor" and the "Trusted" and in the technology applied to create the sense of trust [182].

Various other definitions exist to better elucidate the concept of trust [60, 62, 61, 226, 227, 228, 18, 97, 94, 146, 284, 184]; however, all the definitions of trust indicate that trust exists because there is the presence of risk [38, 65, 164, 61, 143, 94, 240, 199, 118, 202, 136]. We trust when we cannot predict or foresee the actions of others, and therefore resort to believing that these others will act in our best interest [220]. In trusting we are therefore "choosing to put ourselves in another's hands, in that the behavior of the other determines what we get out of a situation" [150]. It is

accepting "another's possible but not expected ill will toward one with the confidence that another could not harm one, although they could harm one" [18, 65, 60, 137, 61].

The relationship between these parties and the risk involved has been defined thus, "If the level of trust surpasses the threshold of perceived risk, then the trustor will engage in risk-taking in the relationship" [164]. The problem of trust is mainly how to determine who or what services should be trusted, even in the presence of risks. In subsequent sections, we give insight into previous work done to aid the development of trust in both offline and online communications.

2.2 Trust in Physical Environments (Offline Trust)

As illustrated by Marsh et al., in the event that a person's car is broken down on the street and a man dressed in overalls similar to those worn at a car repair company shows up in a company's truck, the person will most likely have the man take a look at his broken down car. However, the person is more likely to ask questions and try to validate the man's identity if the man shows up dressed casually in jeans and a shirt, without the company's truck [150]. In the offline world, based on physical attributes and observable cues, humans decide who to trust and what exactly can be entrusted to their care [60, 62, 61, 226, 227, 228, 18, 97, 94, 146].

Considerable research has been done to determine what cues indicates deception in order to decide who to trust when carrying out physical communications. Ekman and Friesen et al. discovered that deception prompted "guilt, stress and fear of detection" [71]. He explains, "This leads to outward behavioral displays from which a person's true state or deceptive intent can be 'read.'" [71]. These cues could either be verbal [254, 180, 12, 17, 112], or non-verbal [273]. Strategies to detect the presence of deception includes analysis of audio [10], whereby an increase in the pitch of an audio could indicate deception [72, 32, 99, 109, 121, 133]; also analyzing the levels of stress in the voice could indirectly indicate deception[129]. Other signs of physical deception could include negative affect, cognitive load, sweating, arousal, and blinking [291, 241]. Deception could also be detected through linguistic cues, such as mentioning certain words or phrases, or the use of complex or much simpler sentences in spoken words [166, 167, 33, 187, 272, 268, 289]. Deceivers will also try to distance themselves from the lie being told and this can be noted in their use of "pronouns,

verb tense (more past or future tense being used than present tense), passive voice, and modifiers" [26, 105, 187, 265, 177, 109]. Tools are now available for automatically analyzing spoken words or languages for the presence of deception [183, 247, 232].

Zak et al. [288] sought to find out why people trust some people and not others. They wanted to know if there was some form of "neurologic signal" in the brain that indicates when trust should be given. Zak et al. compared humans to rodents, whose brain chemical, oxytocin, indicates that another animal is safe and can be approached. They carried out an experiment that involved people making decisions based on trust, and withdrew blood from the participants' arm before and after that decision was made, to measure the level of oxytocin. The participants were split into trustors and trustee. It was found that the more the trustor's trust was not betrayed by the trustee, the more oxytocin they released. To ensure the change in oxytocin was not coincidental, the researchers administered synthetic oxytocin to the brain of some of the participants and they found that "oxytocin appeared to reduce the fear of trusting a stranger." [288]

Ring & Van de Ven [223] notes that trust could also be established based on reputation. Reputation is the subjective expectation or collective ideology people have about the behavior of another based on the interaction history. It is the "aggregated opinion that people have based on past behaviors of character" [150]. Ring & Van de Ven [223] further emphasizes that trust increases as the number of successful interactions occur between the trustor and the trusted. We can have some trust in interactions with a stranger if we can have some assurance that they have had successful interactions with others. Third parties can vouch for an individual's trustworthiness by attesting to aspects of their reputation.

Baier et al. however noted also that sometimes in offline interaction, trust can be given implicitly even when there is no assurance that the person being trusted will act fairly. This can be seen in the case of kings trusting slaves to not poison their drinks, or in the case of a war, whereby there is an implicit trust that once the white flag is shown, the opposing enemy will retreat from fighting. This same trust comes into play when people ask strangers for directions; they trust that they will not be misguided [18]. Asherman et al. notes that sometimes humans give trust because we implicitly believe the person will do us no harm, until proven otherwise

[15]. Diego [87] and Smith [238] also talked about the role of cooperation in trust. Smith wrote, "If there is any society among robbers and murderers, they must at least ... abstain from robbing and murdering one another" [238]. Fukuyama et al., who also did a study of how trust develops in physical communities, believed that "community strongly depends on mutual trust" and that trust happens when "community shares a set of moral values in such a way as to create expectations of regular and honest behavior" [86].

Corritore et al. compared offline and online trust in terms of Generality, Kinds, Degrees, and Stages. They found that both offline and online trust were similar and gave examples under each type of trust [42]. In the next section we discuss research on trust in online communications.

2.3 Trust in CMC (Online Trust)

To foster secured and positive relationships in computer mediated communications, trust must also exist, even if no in-person interaction ever takes place. Corritore et al. specifically defines online trust as "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited" [42]. The question then arises, how can trust be built or improved between two or more strangers in an online virtual community? Research has gone a long way to show that trust is better built face-to-face than over virtual communications. Handy insists that ultimate trust can only be formed by touch [107]. However, this cannot be applied in virtual communities where trust has to be developed in the absence of physical contact. Cues that are normally employed to detect deceit in face-to-face communications may be ineffective when applied to online interactions. People involved in online communications can easily create an ideal persona which Donath et al. [64] refers to as 'online performance'. Therefore, as Castelfranchi et al. explains the problem, "On which signs and qualities do we base our trust in a face-to-face communication, and how can we substitute these properties in electronic interactions?" [56]. Based on offline trust, three main strategies have been implemented in an attempt to solve the problem of trust in online communications. These mechanisms are the use of reputation systems, multimedia-based trust and cryptographic trust. We evaluate the work done in building trust using these mechanisms in CMC.

2.3.1 Reputation Systems

The use of reputation systems is commonplace in online interactions, whereby based on past experience, people tend to predict the future behavior of others. Both reputation and trust are related: trust births good reputation and good reputation leads to trust [218, 63, 217, 290].

Dasgupta et al., who explored the importance of building trust in virtual communities, linked expectation to reputation, explaining that reputation affects users' expectation. They insist that reputation can only be built over time, whereby for reputation to be successfully developed, the trustor must have had previous experiences with the trusted party [58]. There is therefore the problem of how users can form trust in online communications without having had prior encounters with the other party.

While reputation in communities is traditionally mediated by humans, work on trust in e-commerce has centered around how computer systems can serve as trusted third parties for the purposes of maintaining and disseminating reputation information. In early 2000, Zacharia et al. proposed two reputation mechanisms that could be used to address trust problems in e-commerce and other online contexts [287]. The authors proposed Sporas and Histros, which the authors explained can be applied to loosely and highly connected communities respectively. Sporas works such that new users have a standard reputation value and as transactions are being carried out, based on the reputation feedback, the user value either increases or decreases. Histros is a web-of-trust based mechanism where users trust other users because someone they know had trusted them in the past.

Like in offline communications, cooperation in the community was emphasized by Boyd as a major requirement to build mutual trust in CMC [30]. Boyd focused his evaluation on eBay (in 2002), stating that eBay has successfully been able to build mutual trust on their platform. As a result, this has led to better security in the services offered to the community eBay built. This mutual trust according to the author reemphasizes Deutsch's opinion on building trust, which states that "the trustworthy person is aware of being trusted and he is somehow bound by the trust which is invested in him" [60]. The author explains that community trust is the trust that makes eBay stronger. Boyd insists that though safety and security mechanisms

have been introduced such as escrow agents in the online community, the major thing that safely secures eBay users is community, which Weisul in his paper refers to as "creative self-policing" [30]. Boyd claims that when all transactions and interactions are made openly in the clear sight of other users then there is the high probability of people to act justly and fairly [30]. Boyd's research was however conducted fifteen years ago.

Li Xiong et al. also acknowledged the importance of trust to help reduce threats in online e-commerce communities. They introduced PeerTrust, a reputation system to assist in gauging the trustworthiness of those involved in online communication. PeerTrust also employed a feedback-based reputation model whereby peers are made to rate a transaction and the overall rating is the sum of the ratings aggregated in the past six months [283]. The authors' claim that the unique approach used in the development of their model was based on the use of five factors which were, number of transactions, credibility of feedback, feedback received from peers, transaction context factor and community context factor. To achieve a higher value of reputation one must increase the number of transactions done [283]. Carrara et al. also did a thorough evaluation of reputation systems, and explained that the punishment and reward system is a good way to keep people in check when using CMC. The punishment could be a drastic reduction of their ratings on the reputation systems or possibly banning them from using the system [37].

Virtually every platform today that allows providers of goods or services to be matched with customers (e.g., eBay, Amazon) supports some form of online reputation. Buyers rate sellers, and sometimes sellers rate buyers. Low rating can result in loss of business or complete loss of access. Similar mechanisms are even employed in online marketplaces for illicit goods and services [116], with sellers with higher reputation being able to demand higher prices.

2.3.2 Multimedia-based Trust

While people will factor in a reputation score into their decision as to whether to trust a stranger, people also make use of visual and auditory cues online, just as they do in face-to-face interactions—even though those channels are much easier to falsify online. We review this research below.

Bos et al. evaluated the development of trust in four communication modalities: face-to-face communication, video, audio, and text. The authors recruited sixty-six subjects and tested them with a social dilemma game, *Daytrader*. They observed that the group with text communication had the most difficulty building trust, and that the audio and video did almost as well as face-to-face communication. The author found it surprising that the audio and video had similar results even though the video was done in very high definition standards and the audio conversations were carried out using a cheap phone [28].

Appearance seems to matter when determining trust. Multiple researchers have observed that the attractiveness of a stranger correlates with how trustworthy they are perceived to be [224, 279, 280, 68]. A photograph of a person with a smile is enough to improve trust in social dilemma games [230]. Steinbrueck et al. [243] found people showed more trust in e-commerce sites when personal pictures were used. More recently, Ert et al. [77] carried out a user study of Airbnb users to discover if users are likely to trust an apartment owner more when personal photos are uploaded on the Airbnb section of their apartment ad. Their results indicated that personal pictures of the host had a greater influence than the host's reputation. Users in the study picked accommodation with places whose owners uploaded cute personal pictures, even if the reputations of those places were low. The effect was still present even when controlling for the hosts' attractiveness.

Other researchers however found that the effect of pictures on trust online is not so straightforward. With online dating sites, overly attractive pictures seem to reduce trust [168]. Scharlemann et al. evaluated the presence of smiles in pictures to find out if this breeds more trust in people. The authors were of the opinion that there were silent cues people unconsciously consider in determining who to trust and one such cue was smiles. To confirm their hypothesis, the authors carried out a user study involving 120 participants where a trust game was played. The results showed users tend to trust and cooperate with strangers whose pictures had a smile. The authors insist that faking a 'real' smile is hard to do and a smile could even lead to a criminal being given a lesser sentence [230]. Riegelsberger et al. also examined the effect of adding pictures of smiling, happy sales assistants to ecommerce sites using 115 subjects and twelve sites (half with good, half with poor reputations). The authors

observed that the reputation of poor sites were increased by the addition of personal photos while the reputation of good sites decreased. The authors concluded that the presence of photos generally seemed to decrease participants' ability to distinguish between trustworthy and untrustworthy parties online [221].

2.3.3 Cryptographic approaches

Although cryptography plays a significant role in securing online interactions, it provides remarkably weak trust guarantees in practice in the context of e-commerce and computer mediated communications. TLS protects communication between back-end services and mobile and web applications; however, TLS is almost never used to authenticate individuals, despite the standard's support for end-user authentication through client certificates. Cryptographers, however, have developed protocols for some online dating-related tasks.

Mikhail and Dukhovni et al. proposed cryptographic protocols to try to solve the Dating Problem. In the Dating Problem, Alice and Bob have a crush on the other, but they are unaware of their mutual interest. They would love to let the other know of their interest only if the other party is interested [181, 67].

Miers et al. also developed a protocol that could help Alice prove her Sexually Transmitted Infection (STI) status to her past match or her potential match Bob, without Bob knowing that such information came from Alice. If Bob was a past match, Bob can decide to get his STI status tested. If he is a potential match, and Bob has no problem with Alice's status and wants to be matched with her, then Alice can reveal her real identity, else she doesn't and Bob never gets to find out who Alice truly was [179].

Lysyanskaya proposed an ideal dating site that could function using cryptography; however, the model does not focus on the issue of trust but the basic functioning of dating sites. In the model, Alice and Bob are matched by a matchmaking service, SophistiCats.com. As a result of using multiparty computation or Secure Function Evaluation (SFE), SophistiCats.com has no idea who Alice and Bob are or that they have even been matched. Alice on the other hand can log on to SophistiCats.com, making use of anonymous authorization that prevents anyone from knowing her identity. After login, Alice uses anonymous channels to contact Bob and vice versa,

which makes it impossible for Alice and Bob's ISP to know that they are accessing the services of SophistiCats.com or the content of the messages being sent. Alice's roommate, Eve, however knows about Alice and Bob's budding relationship as well as the content in some of the messages Bob sent. This is because Alice has discussed some of her messages with Bob and even posted a few on her fridge. However, Eve is incapable of reading the flow of messages between Alice and Bob because they are all encrypted. Also, the digital signatures Alice and Bob uses makes it possible for them to be able to differentiate real messages from fake ones [145].

2.4 Trust in Computer Mediated Introductions (CMI)

CMI are a type of computer mediated communication where the purpose of the communication is to find—be introduced—to other individuals in order to interact in the physical world. Unlike other forms of CMC, communications do not end online but are moved offline. It should be noted that CMI is significantly different from the sharing economy. In the sharing economy, emphasis is placed on the idea of exchanging goods and services. It is defined as an, "economic model based upon the exchange of human or physical resources between two individuals, where a person who needs a good or a service can borrow or rent it from another who has it" [57]. Some examples of the sharing economy cannot be classified as types of CMIs and vice versa. For example, while eBay and Amazon's mechanical turk are examples of the sharing economy, they do not fall under CMIs, because no offline interaction takes place. Also, dating sites cannot be classified as part of the sharing economy. Carpenter noted that the anonymity CMC offers leads to people sharing much more personal intimate information online and at faster rate than face-to-face "because the immediate consequence is much less severe without physically being present" [274, 249, 10]. However, in CMI these people eventually meet in person and may face great consequences if introduced to deceptive people online. The key challenge therefore with CMI is the risk of exploitative, fraudulent, criminal, and even violent interactions when one is introduced to the wrong people. In terms of personal CMIs, specifically online dating, conventional trust mechanisms discussed above may be ineffective due to the nature of the interactions that occur on this platform.

Online dating started with Match.com in 1995, which moved to algorithm-based

matching in 2000 and then to being on handheld devices in 2008 [80]. Before then people seeking potential partners made adverts in the newspaper [140]. However online dating has now become very popular with over 2,500 dating sites becoming operational in the US alone as at 2013 [292, 140]. While some people engage these platforms to carry out online chatting and flirting, majorly the end goal of online dating platforms varies from casual sex to marriage [122, 92, 294], which all involves offline encounters. As of June 2016, the official Apple Store recorded that "8 of the top 150 grossing social networking apps were designed for online dating" [36]. Whitty and Carr et al. predicted that the popularity of online dating platforms will keep growing because of the increase in the population of singles and time demand which prevents people from meeting in the real world [278].

Anderson et al. explains that when people start to share much more personal information online, trust is created and then intimacy [10], and "that the sharing of more personal information leads to stronger feelings" [178]. Problems arise when one of these parties is insincere. With the increasing popularity of dating sites lot of research has been carried out on the platform [152, 281, 106, 252, 293, 211, 74, 108, 122]. None has solely focused on the unique problem of establishing trust in dating sites.

2.5 Conclusion

In this Chapter, we reviewed the extensive research done in an attempt to establish trust in a variety of contexts. Note, however, that little of this work applies directly to the trust model of business or personal CMIs. In the next chapter we evaluate the specific trust model of seven CMIs.

Chapter 3

Critical Analysis of Trust Strategies Used in Specific CMIs

To build and maintain trust in users, different mechanisms have been put in place by various online communities. The aim of this chapter is to find out the specific mechanisms that are being employed by CMIs to ensure people feel safe enough to trust that these platforms are introducing them to credible people void of ill intentions. Trust can be said to exist online when there is "mutual confidence that no party to an exchange will exploit another's vulnerabilities" [62, 137]. Morgan and Hunt further explain that trust can be said to exist "when one party has confidence in the exchange partner's reliability and integrity" [184]. Therefore, all mechanisms that have been put in place by these CMIs to ensure users have confidence in the reliability of the CMI's services, both offline and online, will be considered as trust mechanisms.

As explained in Chapter 1, two types of CMIs exist, business CMI and personal CMI. In business CMIs, people are introduced online, solely for the purpose of exchanging goods and services offline, for a monetary value. Examples of such interactions can be found in Uber, Airbnb, and Lyft. In personal CMI, people are introduced online and meet offline based on common hobbies and interests in order to carry out similar activities. No monetary exchange occurs in personal CMIs. Examples include the services offered by an application called Couchsurfing and also dating sites' services. A combination of both business and personal CMI exists and can be seen in the services provided by Craigslist. In this chapter, we evaluate three business CMIs, Airbnb, Uber, and Vayable, and one personal CMI, Couchsurfing. We also analyse three CMIs that offer combined services, which are Meetup.com, Craigslist, and Kijiji.

The rest of this chapter is divided into eight sections. In section one to six, we explain how each CMI platform functions and evaluate the trust mechanisms that have been put in place. In section seven, we analyze the viability of the trust mechanisms and determine how effective these mechanisms have been in developing trust and keeping users safe. We conclude in section eight. It should be noted that the

trust model of online dating sites is not explained in this chapter; this is because of the uniqueness of the type of interactions that occur on the platform. In subsequent chapters, we evaluate the trust mechanisms of dating sites and compare them with those successfully applied by these CMIs.

3.1 Airbnb

Airbnb is an online community marketplace that provides accommodation and events services. These services are mainly patronised by travellers who are either looking for cheaper places to lodge in or those in search of locals with whom they can experience the city [1]. The marketplace is made up of hosts and potential guests. Hosts offer their homes as sources of accommodation for a specified duration of time. The hosts list their homes on the platform, specifying the location, amenities, price, the duration for which it will be available, and house rules. The prices are at a much lower rate than conventional hotel or motel lodging spaces. In most cases the host rents out just a room or rooms in their personal houses; as such, hosts tend to live in the house with the guests for the duration of their stay.

Hosts can also organise events for guests to participate in. Events organized by hosts on Airbnb could either be *immersion*, which take place over a couple of days, or *experiences* that last for a couple of hours [2]. The events are mostly centered on helping people experience the culture of the city and showcase the various activities that can be held during the duration of their stay. Depending on the event, one person or a group of people could sign up to participate at a given time. Events could range from wine tasting to hiking, concerts, sight-seeing, a visit to one's favorite hangout spots, surfing, and various other activities.

The Airbnb platform is a form of business CMI, mainly because goods and services are exchanged for monetary value. The idea of sharing a space and hanging out or staying with a stranger met online has become more commonplace. In 2015 alone, on new year's eve, Airbnb had about 1.2 million guests staying with 300,000 hosts in over 150 countries [188]. On its official website, the Airbnb platform is described as a "trusted community marketplace", with its focus to "build the world's most trusted community" [2]. A look therefore into the efforts made by Airbnb to achieve this goal is relevant to this research.

3.1.1 Mechanisms Used To Develop And Maintain Trust in Airbnb

In a bid to build trust, Airbnb states that they start off by first "beginning with the assumption that people are fundamentally good and, with the right tools in place, we could help overcome the stranger-danger bias" [188]. They further explain, "To do so we needed to remove anonymity, giving guests and hosts an identity in our community. We built profile pages where they could upload pictures of themselves, write a description about who they are, link social media accounts, and highlight feedback from past trips" [188]. We give a breakdown of the various mechanisms Airbnb has put in place to achieve this.

Verification

Verification refers to the process by which CMIs validate the identity of those using the platform. To sign up on Airbnb, users have the option of using their Facebook account, Google, or other email platforms. If users sign up using other email services, a verification link is sent to the email address for confirmation purposes. In addition, both guests and hosts are required to upload a profile picture and verify their phone numbers. Phone numbers are verified either through SMS or calls, in which users are given a four digit code that can be used to verify their phone number.

Airbnb also offers an additional Verified ID option for both guests and hosts. If a user fulfills the requirements contained in the Verified ID option, a verified icon is added to the user's profile, indicating that the user has been verified by Airbnb. Under the Verified ID option, users can be verified by Government ID, Personal Information, or both depending on the country of residence [2].

Verification by Government ID involves the user taking a picture of their government issued ID, such as visa, passport, national ID card, or driver's license, with the Airbnb online verification camera. The pictures taken of the ID must also include the unique identification number of the ID for the verification to be valid. The user at the same time is also required to take a selfie and upload on the verification platform. This selfie must be a live photograph that is taken while the verification process is being carried out. The selfie will be compared with the picture on the government ID in order to validate that both pictures are the same person. Airbnb guarantees that the picture on the Government ID will not be used to replace the person's profile

picture, and neither will the name on the ID replace profile names, as users sometime use nicknames as their profile names [2].

Verification by Personal Information involves users answering personal questions whose answers are mostly known to only the individual. Questions such as a person's former street address or credit card information can be asked [119, 88, 19]. When all the questions have been answered correctly the person is assigned a verified icon in their profile.

Making use of the Verified ID as a means of verification is not a requirement for hosts and guests to be able to book and interact. As long as both parties have their email addresses and phone numbers verified, they are not restricted in the activities they can carry out in the site. However, hosts usually strive to get the verified symbol as this increases guests' trust in the host [222, 253, 200]. Hosts can also make a request for additional verification from specific guests, other than relying solely on guest's email address and phone number verification status. Verification can only be requested from the guest making the booking even if other people may be accompanying the guest.

In 2013, Airbnb made it mandatory for some of their guests to upload their Government ID in order to be able to complete a booking of services with a host. The platform introduced this additional verification step for twenty-five percent of its guests, with plans to possibly make the verification step compulsory for all guests on their platform [19, 88]. This extra verification process only shows up after guests are done paying for their booking. Money can be refunded if guests are unable to successfully provide a picture of their Government ID.

The Airbnb platform also encourages users to connect their Airbnb account to an online platform or social media account, such as LinkedIn, Google, or Facebook, to enhance verification of their profiles.

The various verification mechanisms help users to develop trust in the credibility of the people they interact with on the platform [102].

Privacy

For all information provided by users on the platform, Airbnb assures users that the information is transferred on the internet using encryption techniques employed by

credit card companies. They explain that they will never disclose the billing and payout information of guests to hosts. They also state that the information gathered from their users will not be compromised and will only be shared when needed with third parties such as marketers.

In addition, information about a person's government ID is stored in an encrypted form, with a very small number of people having access to the original records. If knowledge-based personal questions are used for verification, the questions and corresponding answers are not stored. They further explain that third parties use the stored information in accordance with Airbnb's policies. This could help users trust that their information is well protected. It can also encourage users to share more information in order to aid verification processes [2].

Background Checks

For users in the US, where applicable by law, Airbnb may sometimes run background checks using the names and date of birth provided in the ID. This is done to verify that the user has not been involved in criminal or sex offenses in the past. This check can sometimes be carried out on users outside the US as well, if Airbnb can obtain a localized version of the report under applicable laws. Airbnb however states that they cannot guarantee that these checks have been run on every host and guest. In addition, they do not run checks on additional people that may be accompanying the guests booking the requests.

Review Conversations

According to their privacy policy, Airbnb could occasionally review conversations carried out on the platform, either directly or through third parties. This can be done in an attempt to hide references made to other sites or as a means of preventing users from being lured to make payment on other sites. They could also store conversations as they see fit, and use them to aid investigations if needed [4].

Listing of Profiles to be Included on Search Engines

By default, Airbnb ensures users' public profiles and their listing are all included in search engines' results. This could help hosts and guests trust more in the credibility

of the site.

Reviews and References

After a trip has been completed, both hosts and guests are given the option to write reviews. Each review is limited to five hundred words and must be completed within fourteen days after the trip. After a review has been written, users have forty-eight hours to edit their review, except if the other party has already written a review. Reviews are made public only after hosts and guests have written a review about each other or after the fourteen days wait period. Airbnb can, at its discretion, remove or edit any review that is not in line with its review guidelines as stated in its terms of use [2].

Airbnb also make use of references which are quite different from reviews. References are usually written by a person's friend or family member, in a bid to enhance the person's profile and to make others know more about the person than just the basics. Airbnb includes a reference in a person's profile only after the person has approved the reference written for them. As previous research has shown, this helps users to increase their trust in the listing provided by the website [210, 141, 57].

Delayed Disclosure of Phone Numbers

Airbnb does not share guest or host's phone number until after booking has been confirmed. Prior to completing a booking, if a host needs to contact the guest and vice versa, Airbnb calls the guest number and connects them with the host, without sharing phone numbers [2].

Linking to Other Online Platforms

In the event that a user decides to link their Airbnb account to their online social media platform such as Facebook, the activities carried out on Airbnb as well as some of the user's information may be shown to the user's social media friends. Airbnb may also link up the user's social media profile to Airbnb profile, and include a link to their social media platform, on the user's Airbnb profile. Also, friends on the user's Airbnb account will be able to see mutual friends on the user's social media platform. The information provided from these accounts can also be stored, transmitted, or

processed by Airbnb [2]. Airbnb also encourages guests to look for hosts that have their social media account linked to their Airbnb profiles. This form of transparency could build a sense of confidence and trust in users.

Safety Tips

In an attempt to have a safe community, Airbnb has a set of safety tips for hosts and guests. As previous research has shown, [234, 132], when users know what to do and how to go about carrying out such safety tasks they are more likely to have confidence in carrying out these tasks. Hence, having safety precautionary measures on the site helps to boost users' trust in the site and in the services provided.

Stating Offenses

In the event that a background check is conducted, Airbnb lists the offenses that could result in the removal of a person's profile from the platform. These offenses include [2]:

1. A violent crime
2. Certain sexual offenses, including serious sex offenses and prostitution
3. Felony drug-related offense
4. Certain fraud and dishonesty offenses, including identity theft
5. Certain theft offenses
6. Offenses involving certain types of property damage
7. Certain invasion of privacy offenses

Messaging Platform

Airbnb also provides a messaging platform for guests and hosts such that email exchange can be carried out without either party knowing the real email address of the other. The platform provides a temporary Airbnb email address that masks the

real email address used to send messages, and does not reveal it, even after booking has been confirmed. If an interaction or transaction doesn't work as planned, communication can easily be cut off between hosts and guests.

Payment

Airbnb encourages people to make payment to hosts using their platform and not through other means specified by the hosts [2]. The funds paid are only released to the host, twenty four hours after the guest checks in. This is done to give guests the opportunity to notify Airbnb if something is off about the booking [188].

Levels and Superhost

Airbnb assigns levels to users based on their activities in the site and on their community forums. When users ask questions on forums, the response given by people with a higher level number are rated higher than those with a lower level [3].

Airbnb also assigns superhost status to hosts who have met some specific criteria. For host to get a superhost status they must have successfully carried out at least ten trips in a year, have a five star review with at least eighty percent of their reviews, have a response to messages rate of at least ninety percent and above, and must rarely ever cancel reservations made [5]. Every superhost has a badge, hence it is quite easy for people to identify superhosts. Users tend to trust superhosts more than hosts, and are likely to make more bookings with them [131].

Flagging

While Airbnb does not allow users to block each other, suspicious messages, profiles, and listings can be flagged to notify Airbnb to look into those activities [7].

24/7 Customer Support and a Dedicated Team

While Airbnb advises users to contact the local police and emergency should something go wrong while staying with a host, they also let users know that 24/7 customer support is available to them in different languages. Airbnb also state that they have

a team "dedicated to monitor unusual activities in the platform."[2] All of these mechanisms help build user trust.

3.2 Uber

Uber is a business CMI that enables easy connection of drivers to riders through the use of either their mobile application or mobile site [257]. Uber is different from the typical taxi service because Uber drivers do not make use of standard company cars, but rather make use of their own cars in order to provide transportation services. To make use of Uber services, potential drivers and riders sign up either on Uber's website or through the application. After sign up, riders can make a request for a ride, to which Uber displays the total amount for the requested trip. If the rider confirms to pay for the trip, Uber then locates the closest driver available to pick up the rider and sends a request to the driver. The request contains a notification that a rider wants to be picked up; however, the driver is unable to see the picture of the potential rider. The driver has the option of accepting or declining a request. Should a request be accepted, riders are notified by the Uber application that a driver will be picking them up shortly. The riders can also view the driver's name, picture and car license plate number as well as the reviews and ratings of the driver.

Uber also notifies riders of the amount of time it will require for drivers to arrive at the rider's pickup location. Uber provides both riders and drivers a map view on the application that shows the exact place both parties are, and how long it will take to arrive there. Once the driver arrives at the rider's location, the trip is started; it ends when the rider arrives at their destination. In most cases riders' bank card information or PayPal details is linked to their Uber account, hence the ride is automatically paid for without the rider having to pay using cash.

Listed below are the various trust mechanisms Uber employs.

3.2.1 Mechanisms Used To Develop And Maintain Trust in Uber

Verification

In order to sign up for Uber services, users require a valid email address and phone number. After filling in personal details and preferred language, an SMS is sent

to the phone number to confirm the number exists, after which users are required to fill out payment details. In some countries, Uber requires users to have a valid credit, debit card, or some 3rd party services such as PayPal to facilitate collection of required funds [260]. In other countries, Uber allows the collection of cash payment [258, 248, 189]. Uber sends receipts of trips made to the email address provided during sign up.

Masking of Phone Numbers

Uber has on record the phone numbers of both the drivers and riders. If contact has to be after a trip has been requested, Uber anonymises the phone numbers of both parties, such that the riders and the drivers do not have the real phone number of the other.

Safety Tips

In order to further protect users from fraudsters, Uber gives a list of safety tips that users can adhere to, such as, "Follow your intuition, Trust your instincts, Use your best judgment when riding with Uber " [262].

Transparency

When users request rides, riders are able to see the name of the driver, the car license number, picture of the driver, reviews, and ratings. This way, riders are able to know ahead of time who will be picking them up. They are also able to decide, based on the information they have, if they would rather cancel the request and make a request for another driver.

Sharing of Trip Information

Riders are also able to share the status of their entire trip with their family and friends. The status report normally contains the driver's name, location, license plate number, and photo. They are also able to share their estimated time of arrival with their friends and family members. This way, if something goes wrong during their trip, their friends and family can be made aware of it sooner rather than later.

Map

Riders can watch the trip's progress in real time on the map provided by Uber. They can be able to tell if the driver is following the best route provided by Uber or if the driver is off track. Uber also provides a service known as uberPOOL, where riders can share a ride with others to reduce cost. When riders make use of uberPOOL, Uber's map gives riders information about the other people they are sharing a trip with. This way, riders are not riding with complete strangers.

Tracking

Uber also states that for every trip made they collect the GPS data. This is to ensure they have a record of where all drivers and riders are at any point during the trip and to make sure drivers are taking the best route to a destination [256].

Ratings and Feedback

Both drivers and riders can leave reviews and ratings for the other after a ride is completed. Uber also assures users that they review all feedback left by riders and drivers to ensure safety on the platform.

24/7 Email Services

Uber boasts of having a 24/7 customer support in terms of emails services for riders, whereby riders can reach them with questions and concerns through email at any time of the day.

Legal Issues

Uber stores information acquired from users, which can be used to assist in legal processes, should the need arise.

No Sex Rule

Uber has a no sex rule between riders and drivers which it states in it's community guideline, *"No sexual conduct between drivers and riders, no matter what."* [259].

Security Checks for Uber Drivers

Uber requires all drivers to provide their full name, social security number, driver's car license number, a copy of their driver's license, vehicle registration, and proof that complete vehicle inspection has been carried out. Uber also carries out some form of checks to verify its drivers. The intensity and credibility of these checks vary from country to country. For instance, in Canada, Uber requires all drivers to submit a police record check annually [255].

In the US, Uber makes use of *Hirease* and *Checkr* to carry out background checks on its drivers [59, 138]. In the case of *Checkr*, if a criminal record is found Uber sends someone in person to check the record in the courthouse [138].

In Nigeria, Uber previously required all drivers to carry out a four-stage verification process which included submission of "police reports, guarantors, address checks and previous employer" [261]. However, in 2016, Uber resorted to carrying out checks making use of "psychometric analysis", which checks for "driver's integrity, truth score, acuity, honesty and character." This test is completed just once and does not have to be repeated [261].

3.3 Meetup.com

Meetup.com is an online community where people are introduced through the internet to set up a meeting offline, based on common interests. Similar interests could range from biking to wine tasting, writing, religious beliefs, technology, reading, dancing and many more. To join a meetup group, interested people sign up on the website, based on their location. After sign up, users choose groups they are interested in, join the group, and meet offline for the group's planned meetups and events. Users do not pay to sign up on Meetup.com; however, every Meetup group organizer must pay a monthly subscription fee for their group to be hosted on the site. Meetup.com's group organizers, at their own discretion, can decide to charge membership dues for users to join their Meetup groups or event fees for users to attend any event organised [170, 175, 174, 171]. Some group organizers allow new members to attend a limited number of events for free in order to try out the meetup group, after which they are required to pay for every other event attended with the group [173]. Since monetary

exchange can sometimes be involved in the interactions made offline, we therefore classify Meetup.com has a mix of both personal and business CMIs.

Here are the trust mechanisms being used by Meetup.com,

3.3.1 Mechanisms Used To Develop And Maintain Trust in Meetup.com

Report Abuse

Users are advised to report members of the site or a group that may be violating their terms of use by sending an email to Meetup.com. The site encourages everyone to submit a report if the meetup group had events carried out that were against the terms of use, or if users encounter something unusual [173].

Safety Tips

Meetup.com has a list of safety tips for users to adhere to. They also advise users to contact a law enforcement agency should people behave inappropriately during meetups. The platform also provides a list of legal resources users can make use of. They encourage people to consult their lawyers for specific problems associated with meetups, as well as send an email to the website.

Blocking of members

Users also have the option to block other members that may be acting against the site's terms of use. If a user blocks a member, they will be unable to send messages or receive messages from such members.

Reviews and Ratings

On Meetup.com, members can leave reviews about a Meetup group or event [172]. The platform also makes use of ratings which could be Star Ratings or Rating Comments [176]. Star Ratings of past Meetup events are left anonymously, however Rating Comments show the members who left them. While Rating Comments cannot be edited, they can be deleted by the writer [176].

Linking of Social Media Account

Users of Meetup.com also have the option of linking the platform to their social media account, such as Facebook. If a social media account is linked, users can be able to login through the social media account and also monitor the activities of their friends on the platform.

3.4 Vayable

Vayable is a type of business CMI which is quite similar to Airbnb; however, unlike Airbnb, Vayable doesn't offer any form of accommodation services, but solely provides experiences for people to participate in. For a fee, users on the site host various experiences which others can sign up to participate in. These experiences are tailored to help travellers better understand the culture of a city or country. The users involved in hosting the events are called insiders.

3.4.1 Mechanisms Used To Develop And Maintain Trust in Vayable

Verification

To verify potential insiders, Vayable gives the option of verification of the insider's email address and phone number. Potential insiders can also carry out video verification, which entails them uploading a video of themselves on their profile, explaining their services and what they offer.

Feedback and Rating

Vayable also allow users to write reviews and rate how insiders performed in the experiences hosted.

Review of insiders

Vayable assures users that they, "carefully vet all insiders for quality and safety" [267]. They specifically state in their guide [267]: "Every Insider on Vayable:

1. Commits to delivering a high-quality experience to every traveler.
2. Prioritizes safety and security above all else.

3. Is passionate, personable and trustworthy." [267]

This provides a huge sense of trust in users that the insiders on the platform have been carefully reviewed and vetted.

3.5 Couchsurfing

Couchsurfing is a personal CMI that involves hosts sharing their homes and experiences with guests for a specified duration of time, at no monetary cost. The platform serves as a form of hospitality service for travelers visiting different cities and countries. The hosts, who are usually locals of those cities, sign up for couchsurfing services and offer their 'couches' for free to guests called surfers. Though no monetary exchange occurs between host and guest, the platform encourages surfers to show their appreciation of their host's hospitality by doing something nice for them in return. They specifically state, "We do recommend that a guest show their appreciation by cooking a meal, taking the host out, bringing a small gift or offering some other gesture" [50].

The main purpose of bringing host and guests together offline is to create opportunities for people to make new friends with others around the world and have new experiences. Users are advised to interact and "share something" which could include stories, favorite dishes/meals. They are encouraged to "spend time with their host or surfer. Make new friends and help each other discover new things about the world" [51].

Guests can either search for hosts to house them, or they can make their trip plans public on the platform and hosts can contact them if they are interested in hosting. Apart from lodging with people for free, users can also view events organized by other couchsurfers that are taking place in any city and attend these events together with other surfers. This way, travelers and locals can meet up for events together in a new city. Couchsurfing also has crash events which is the largest couch crashing event. At this event, surfers from all over the world come to attend couch crashing events that have been planned by locals for a duration of time, sometimes for a long weekend or more. The platform ensures that all events organized by surfers are not businesses for the organizers. They encourage and approve free events or events where the cost of

gas or food is split among members as opposed to events where the surfers organizing the event gain a percentage of the amount surfers pay to attend the event [45].

Users also have the option of setting their couch status or host availability to "Accepting Guests, Maybe Accepting Guests, Not Accepting Guests or Wants to Meet Up" [48]. Users who make use of the couchsurfing application can also see other surfers who are interested in hanging out at any point in time, by setting their status to "Hangout Now" [49].

3.5.1 Similarity of Couchsurfing to Dating Sites

The services Couchsurfing provides have been said to be similar to some extent to what dating sites offer. Couchsurfing encourages their users to know their hosts, have conversations with them, and discuss how their experiences will be when they meet in person. Similar to dating sites, all this is done to make sure users find the perfect match they will be comfortable spending time with [270]. They encourage users to "review potential hosts' profiles and find out if they seem like a good match" [47]. While giving guidelines on how to write a good couch request, to help people better answer the question, "Why do I want to stay with a host?" the site states, *"If your answer is something along the lines of, 'I arrive in Cordoba tomorrow night and this person lives near the bus station,' you have some more thinking to do. Nobody likes to feel like a free hostel. If you're choosing hosts the way you'd choose a dorm then don't expect to be too popular. You're on the right track if your answer to this question is more like, 'They love cooking and so do I,' 'I bet they have some interesting thoughts about music theory,' or 'We could have a crazy night out together.' Know why you're interested in meeting this host, and let them know about it!"* [270]

They further give more guidelines, *"**Find common ground.** When sending a specific Couch Request, you should show your potential host that **you've read his or her profile and find it interesting.** There are reasons you've chosen him or her, so let them know! Tell them what you might have in common or what you think you can share with them. **Introduce yourself!** Don't send your resume and life history, just let your potential host know **why you think he'll enjoy getting to know you.** It could be as simple as a description of your trip and a mention of your hobbies"* [270]. Though the platform states that the site is not for dates but for friendship [45], using

the site to find dates is quite common [198, 209, 208, 207, 207, 250, 120, 23, 149, 246]. As a user commented, *"any time you put two people with similar interests in the same room overnight, feelings are bound to develop"* [198].

Below are some of the trust mechanisms employed by the site,

3.5.2 Mechanisms Used To Develop And Maintain Trust in Couchsurfing

Verification

After sign up, users must confirm their email address and add a profile picture to be allowed to use most services on the platform, including commenting on groups. For users to host a member or to request for another member to host them, their profile must have been fifty percent completed. Their profile is made up of the Account, Profile and References sections. As listed by Couchsurfing, the rubric for profile completion is itemized below [44]:

- Account
  - Confirm your email address 5%
  - Add your phone number 5%
  - Connect to Facebook 5%
  - Get Verified 25%
- Profile
  - Upload 2 profile photos 5%
  - Add your interests 5%
  - Describe yourself in "About Me" 15%
  - Complete 4 more Profile sections 20%
- References
  - Add a Friend on Couchsurfing 10%
  - Get a Reference 15%

- Get a 2nd Reference 15%

Once users engage in any of the activities above and obtain a sum of 50%, users can then host and be hosted.

For the Get Verified option listed above, Couchsurfing verifies users through their PayPal or credit card information for an annual fee. After payment of the fee, users get the verified icon and also have access to send unlimited messages to other users on the platform. Users also have 24/7 priority access to the couchsurfing trust and safety team once the fee is paid. Members can be further verified through their phone number, address or government ID. These additional verification steps are not necessary to host or be hosted. Once a profile has been 50% completed, users can freely host other surfers and vice versa.

Couchsurfing believes hosts should not have to pay to enjoy the site. Therefore, for every time a user hosts a guest, the host gets three months of free verified membership.

Safety Tips

Couchsurfing provides a set of safety tips for users to adhere to while meeting people. Tips include review of references and profiles, trust their gut feeling/instincts, make certain there is a backup plan, and acknowledging personal limits.

Messaging Platform

Couchsurfing encourages all forms of communication to be made solely through couchsurfing as their trust and safety team can be able to notice if something is off, "identify issues and react quickly" [44].

References

Users' reviews are referred to as references in Couchsurfing. Hosts and guests can leave references for the other after meeting offline. Like Airbnb, these references are not released until fourteen days after the meetup, or when both parties have left a reference for the other. People are unable to delete or change any reference left for them. However, references go away if an account is deleted [52]. The platform also doesn't take down negative references except if it violates their guidelines.

Couchsurfing also has a personal reference section. This section is made up of references acquired from friends, family members or from people that users have met through the platform but their meetup was not officially set up on the platform. Both sections collectively count towards the total number of references a user is said to have and can be used for verification purposes.

Feedback

Anonymous feedback can also be written for both guests and host after a trip has been completed [271]. This anonymous feedback can be done when there is a confirmed or accepted meetup request between guests and hosts. The feedback is filled out as tags. A user cannot fill out both negative and positive tags on a feedback; they can either be one or the other. After a tag has been given a tag number, the positive tags are displayed under a section called *'Praise'* on the person's profile, with a number assigned to each tag. For example, a person's *'Praise'* could read, "Wanted to hang out 4, Punctual 4, Good location 2" [75]. The negative feedbacks are not displayed but are "reviewed by the safety team" [271].

Report of Abuse and Blocking of Members

Couchsurfing also provides a means to confidentially report any bad or negative experiences, through sending emails [44]. Users can also make use of the "Report Abuse" button to report offensive messages.

Members are also able to block other members they are not comfortable interacting with. A blocked member will not be able to contact the user through couchsurfing and vice versa. Also, the blocked member will not be able to see some details about the user such as their About me, Photos and Description. The blocked member can however still write references for the user, read user's references, and still be able to find the user's name and general location.

While meeting with other surfers offline, Couchsurfing encourages users to report to the authorities should something go wrong in their hangout, event or meet up, after which they are also advised to report to the Couchsurfing safety team.

Privacy

Users can also update their location at any time; however, just their city, state and country will be made visible. Their street address is kept private.

3.6 Craigslist and Kijiji

Craiglist and Kijiji are both online advertising media that act as platforms for the introduction of goods and services to people. They are examples of CMIs that can be classified as both personal and business CMI as some goods and services exchanged involve monetary value, while others do not. They both act as a form of introduction for people seeking services such as ride share, accommodation, friendship, dating, sale of items, discussion forums, and nanny services.

While users can register for an account on the websites, registration is however not a requirement to use the site. Registration is also not needed to post an advertisement or to respond to one. If users want a verified account, Craigslist can carry out phone number verification; however both the verified and anonymous accounts have almost the same privileges.

To post ads on Kijiji and Craigslist, the user's postal code and email address is required. The postal code is needed for users to know what location the goods and services are in. For an ad to be successfully posted, users must login to their email address and click on the link sent in order to activate the ad. There is no captcha put in place to control spam advertisements.

All postings made are free except some specific postings. These exceptions have been listed on their site [55]. There is also a list of items that are prohibited, such as the advertisement of weapons, ammunition, and spamming activities. All postings are deleted once expired.

Profile pictures are not used on both platforms. It is also not a requirement to add a picture of the goods being put up for sale. Both platforms also do not employ a review, rating or reputation system.

The trust mechanisms used by the sites are listed below.

	AIRBNB	UBER	MEETUP.COM	VAYABLE	COUCHSURFING	CRAIGSLIST	KIJIJI
VERIFICATION STRATEGIES	Y	Y	Y	Y	Y	N	N
PRIVACY	Y	Y	Y	N	Y	N	N
BACKGROUND/SECURITY CHECKS	Y	Y	N	N	N	N	N
SECURED MESSAGING PLATFORM	Y	N/A	N	N	Y	N	N
REVIEWS/REFERENCES/FEEDBACKS	Y	Y	Y	Y	Y	N	N
RATING SYSTEM	Y	Y	Y	Y	Y	N	N
LINKING TO SOCIAL MEDIA	Y	N	Y	N	Y	N	N
SAFETY TIPS	Y	Y	Y	N	Y	Y	Y
FLAGGING/REPORT ABUSE	Y	Y	Y	N	Y	Y	Y
BLOCKING OF MEMBERS	N	N	Y	N	Y	N	N
24/7 CUSTOMER SUPPORT	Y	Y	N	N	Y	N	N

Figure 3.1: Table Showing Trust Mechanisms Used By The Evaluated CMIs

3.6.1 Mechanisms Used To Develop And Maintain Trust in Craigslist and Kijiji

Safety Tips

Both sites list safety tips users can adhere to when using the site and while meeting people offline. They also list authorities that users can contact in the event of a scam.

Flagging of Abusive Posts

Users can flag any abusive post or advertisement that they encounter.

The above sections give a detailed analysis of the various strategies CMIs have put in place in an attempt to build trust in users and safeguard them from dangerous others. However, some of the mechanisms mentioned have not been properly or successfully implemented by these platforms, thereby creating a false sense of trust and safety in users. In the next section, we analyze some of these mechanisms, and determine the credibility and usefulness of the approaches made in implementing them. In subsequent chapters, we will evaluate the trust mechanisms used by dating sites and determine if the successful approaches carried out here will also be useful when applied to dating sites.

It should also be noted that some of the issues highlighted in the section below are not limited to the CMI platform for which it was mentioned.

3.7 Alternative Methods Of Implementing Trust Mechanisms

1. **Linking of Account to Social Media**

   Making use of the existence of a person's social media account is a poor form of verification as such accounts can be easily forged or created solely for verification purposes. In some cases, users can also buy friends and contacts on such platforms, hence creating a fake social media presence [130, 100, 286, 73, 20, 235, 239].

   In the event that a valid social media account is linked to these platforms, if an interaction or transaction doesn't work as planned, communication between those parties will still exist. Hence, guest and host can easily resort to cyberbullying should a transaction not go in their favour [275].

2. **Verfication**

   Airbnb makes use of government ID as a form of verification for some of its users. However, there is no real guarantee that the ID being verified belongs to the person in question. Also Airbnb gives a verified icon to those fully verified but no 'unverified icon' is given to those who are unverified. As a result, new users may not be able to identify the difference between profiles or spot unverified profiles.

   Based on the conditions provided by Airbnb, it is possible for a person to be assigned as superhost by the platform without going through the Verified ID option or having the Verified ID symbol [6]. That is, a superhost could have just been verified using only their phone numbers and email addresses, which should not be the case.

   Vayable seem to create a false sense of safety for its users, when in reality users are left with the responsibility to verify those they choose to interact with. The site states in their guide that they ***"carefully vet all insiders for quality and safety"*** *and that every insider is,* ***"trustworthy****, prioritizes safety and security above all else"* [267]. But in their privacy policy, they specifically state that, *"Vayable does not endorse any Experiences. We* ***do not attempt to confirm, and do not confirm,*** *any user's purported identity.* ***You are responsible*** *for determining the identity and suitability of others who*

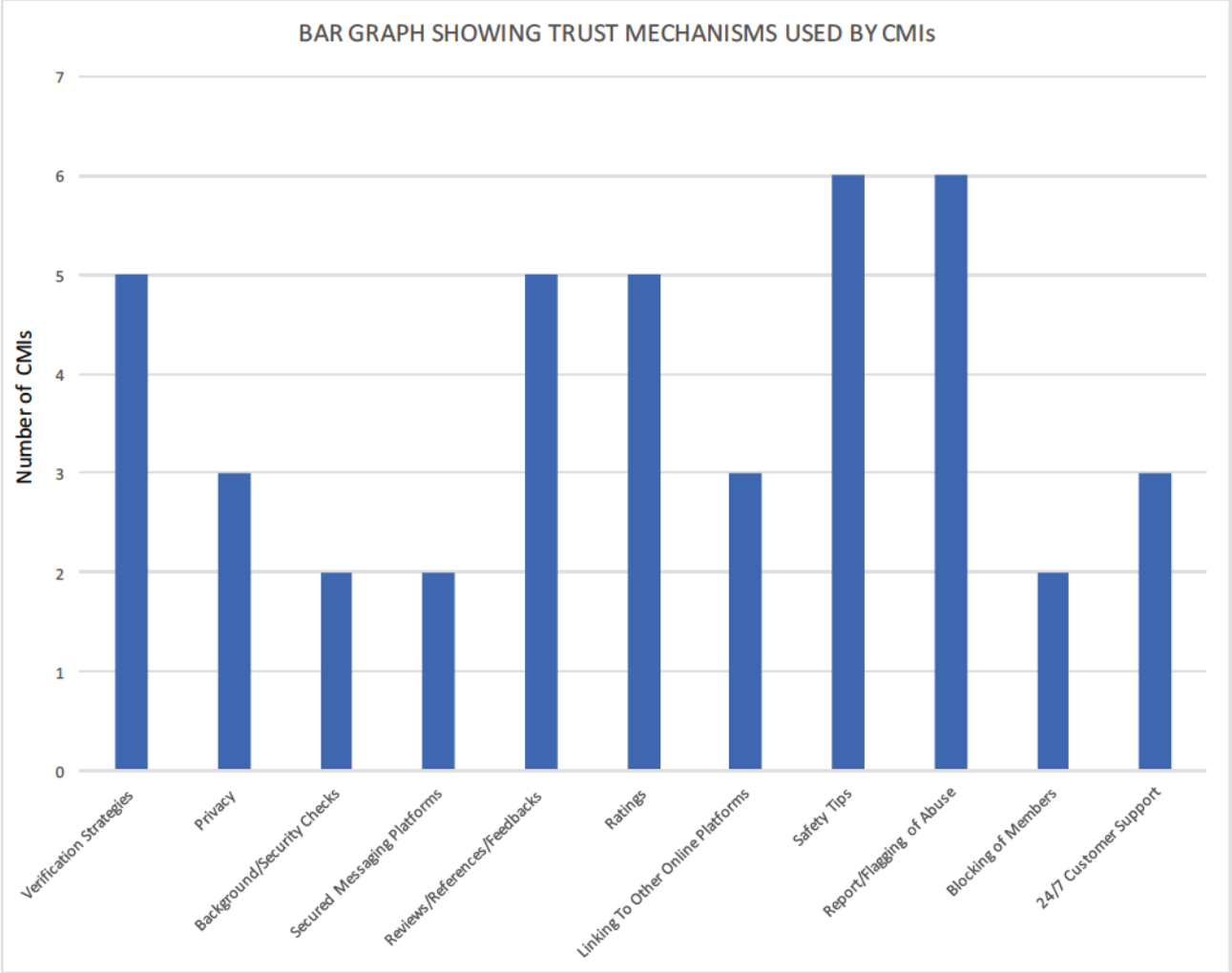

Figure 3.2: Bar Graph Showing The Number of CMIs Employing Specific Trust Mechanisms

you contact via the services." "Vayable cannot and does not control legality or suitability of any experiences. The planning or partaking of any experiences are at the provider's and/or traveler's own risk" [266].

This greatly contradicts their claims of carefully vetting all their insiders, when in reality, the site puts the entire responsibility of verification on users.

On Couchsurfing, for users to host they simply need to meet the fifty percent profile completion requirement. This fifty percent requirement can be met by getting references from friends, updating profile pictures, adding interests, confirming email address, and phone number, which may not be sufficient.

3. **24/7 Customer Service**

   Though some of the platforms assure users of 24/7 customer service, there have been repeated reports of people unable to reach the platforms when needed [76].

4. **Background Checks**

   For CMIs that carry out background checks, these checks are not carried out on all registered users on the sites, due to various limitations in accessing the required databases. According to Airbnb's privacy policy, though checks can be carried out in the US, this checks cannot be carried out on every state record. They are also limited in their capacity to run accurate checks on those living outside the US. To an extent, this defeats the purpose of carrying out the background check in the first place, as Airbnb does not specifically state which users' background checks have been carried out. Background checks are also not conducted on additional guests that accompany a user [13, 14].

   Uber also faces the same challenge in terms of carrying out background checks for their drivers as they engage in limited and less comprehensive checks [59]. This has resulted in a couple of issues in recent times [191, 242].

5. **References and Rating**

   On Vayable, new users that sign up on the platform automatically get assigned a five star rating, even before being verified by email. This could be very misleading to other users.

   On Couchsurfing, since references can significantly improve a user's verification status, the referencing system should therefore be better structured. At the moment, surfers who have never met or discussed with a user can mistakenly leave them references [46]. This could happen to newcomers who don't understand how the system works. For such comments to be taken down, users have to contact Couchsurfing to take them down, and the process may take a while to complete [46].

   Also Couchsurfing's referencing system works such that users can leave more than one reference for a single person at a time. Each of the references written will be counted as distinct individual references [113], as such a person can

get multiple references from the same user. These does not make the use of references a good verification option for the platform.

Craigslist does next to nothing to build trust in its users. The site states, "The overwhelming majority of craigslist users are trustworthy and well-meaning" [54]. They explain that billions of crimes occur, but most of them are not related to Craigslist [54].

In building trust, Craigslist advises their users to "take the same common sense precautions online as they would offline" [54]. They also offer an 'Avoiding Scams' page [53], where their number one rule is, "Deal locally, face-to-face: follow this one rule and avoid 99% of scam attempts" [53]. However such advice cannot be applied to their services where people are requesting to hangout or for hookups.

Kijiji is similar in terms of building trust. They specifically state, "While most individuals who use Kijiji have successful experiences, from time to time we do receive reports of people attempting to scam or defraud the community. We have found that one of the best ways to stay safe is to ensure that all transactions take place locally and in-person." [124]

3.8 Discussion

An examination of different categories of CMIs has provided insight into the specific strategies employed in an attempt to develop trust and keep users safe, both online and offline. While these mechanisms need to be applied on some of the CMI platforms studied, some of the mechanisms in use need to be properly implemented in order to improve users' security. The poor or total failure in the implementation of the trust mechanisms mentioned above, has resulted in a number of incidents on these platforms in recent times [275, 76, 13, 14, 191, 242]. While some of these strategies, if well executed, can be applied specifically to online dating sites, some will be ineffective as a result of the type of interaction that occurs on the platform. For better understanding, the next chapter presents the threat model of online dating sites.

Chapter 4

The Threat Model Of Online Dating Sites

In this chapter we evaluate and analyze the threat model of a typical dating site. Understanding the threats that dating site users face and how they occur, can help us better understand the current trust mechanisms that have been put in place, and define better ones to mitigate these threats, if need be.

The rest of this chapter is divided as follows: The first section defines the terms used, and the second to the forth sections examine the ideal roles of both the dating service and the users, before, during, and after a match respectively. The fifth section presents detailed scenarios of possible threats and itemizes where the dating service has failed to carry out their assigned roles. We conclude in the sixth section.

4.1 Definitions

Alice and Bob: People seeking matches.

Irene: The party carrying out the introduction of potential matches to Alice and Bob. (Irene could be a person or an online service.)

Before the Match: The time from when Alice and Bob sign up for Irene's services to when they get matched. During this period, Alice and Bob are expected to submit their information directly to Irene, complete Irene's profile template, or link their profiles from existing 3rd party services. Once this is completed, they can actively start searching for a potential match's profile or wait for Irene to suggest possible matches to them.

During the Match: The time during which Alice or Bob interacts online with a potential match found via Irene's services. The decision on whether to proceed to meeting a match offline is usually made within this time period.

After the Match: The time period where Alice and Bob meet offline after their introduction online.

Successful and Unsuccessful Introductions: The aim of dating sites is to introduce people online for the purpose of eventually dating and having a romantic relationship offline. Therefore, an introduction is successful only if Alice and Bob engage in a romantic relationship offline. Otherwise the introduction is unsuccessful.

4.2 Before The Match

4.2.1 Alice and Bob's Roles

1. **Sufficient Background Information:** Alice and Bob's role at this stage is to truthfully provide Irene with any requested current background information. It could range from telling Irene their hobbies, to likes and dislikes, to providing very personal information. The information can be verbally given to Irene or can be collected by filling out required fields in Irene's profile template. Depending on the type of services offered by Irene, Alice and Bob may have already given such information to other 3rd party services, such as Facebook, and are only required to link the information to Irene's services. Alice and Bob should always provide truthful, current and sufficient information to Irene to ensure they are properly matched. Alice and Bob are also required to update the information given to Irene as their requirements or other information change.

2. **Notification of Genuine Interest:** If Alice or Bob find profiles of other users that they are interested in, they should notify the potential match and/or Irene of their interest.

4.2.2 Irene's Role

1. **Detailed Information Requirements:** Irene should request information from both Alice and Bob that will help her choose appropriate matches for them. This information should also be able to assist Alice and Bob in determining whether a potential match is of interest.

2. **Verification of Information Collected:** Irene should verify that she has all the requested information or that all the required fields in Alice and Bob's profiles are complete.

3. **Authenticity of Identity and Collected Information:** Irene should verify the authenticity of Alice and Bob's identity as well as the information collected, ensuring that they are not malicious, untruthful or otherwise dangerous (towards potential matches, not just Irene).

4. **Secured Protection of Information and Identity of Users:** It is Irene's responsibility to employ security mechanisms that will ensure the protection and integrity of Alice and Bob's information as well as protect their identity, such that Alice and Bob's information and identity cannot be compromised in the event of a system's breach.

5. **Preserve Users' Privacy:** It is Irene's responsibility to ensure that only the information given to Irene by Alice for use in Irene's services is made available to Bob and vice versa. At Bob's request, Bob's information can be collected back from Alice without Alice having any online access or offline copy of Bob's information.

6. **Authentic Claims:** It is Irene's role to clearly explain the features she offers and to make authentic claims of the viability of her services. The claims made should not in any way misinform Alice or Bob.

7. **Availability of Potential Matches:** It is the role of Irene to make potential matches available to Alice and Bob. This could be done through search functions, suggestions from Irene or a combination of both.

4.3 During the Match

4.3.1 Alice and Bob's Roles

1. **Honest communication:** It is the role of both Alice and Bob to honestly communicate with each other and avoid deceit of any kind.

2. **React to Matches:** It is the role of both parties to react to matches during this time frame. Reaction could involve blocking of a match, reporting match, flagging match, ignoring match, cutting off all forms of communication with match, searching for other potential matches or move to the next stage with a match, which is meeting offline.

4.3.2 Irene's Role

1. **Effectively React to Users' Requests:** It is Irene's role to effectively act on Alice and Bob's requests made during matches.

   If Alice *flags* Bob as acting inappropriately, it is the responsibility of Irene to verify Alice's claim and, if true, take proper sanctions.

   If Alice requests that Irene *blocks* Bob from contacting her, Irene should carry out this request such that Alice and Bob will be unable to contact each other either through the platform or outside the platform.

   If Alice requests that her profile be *deleted* from Irene's pool of profiles, it is Irene's responsibility to ensure that Alice's profile is removed and made completely inaccessible to other profile owners. In other words, Bob should no longer be able to view Alice as a member making use of Irene's services.

2. **Preserve Users' Privacy:** It is Irene's responsibility to ensure that Alice and Bob's privacy is protected and only information provided to Irene is made available to Bob. At Alice's request, such information is retracted from Bob in such a way that Bob can no longer use the information provided either offline or online.

   Irene should also keep all past, present and future communications made by Alice to other members strictly private and confidential to Alice. In other words, Bob should have no knowledge of when or if Alice contacts other members using Irene's services.

   In addition, during the match, Irene should also ensure she carries out the following roles as previously explained:

3. **Secured Protection of Information and Identity of Users**

4. **Authentic Claims**

5. **Availability of Potential Matches**

4.4 After The Match

4.4.1 Alice and Bob's Roles

1. **Honest communications:** It is the role of both Alice and Bob to continue communicating honestly offline.

2. **React to Matches:** Reaction should be due to honest communications between both parties. Reaction could include blocking of match, reporting match, flagging match, cutting off communication with a match, seek out other potential matches or dating the match. The reactions at this stage essentially determine if the introduction was successful or unsuccessful.

4.4.2 Irene's Role

Irene's Role after the match is essentially the same as her role during the match. While Irene is mostly out of the picture after a successful introduction, if an introduction was unsuccessful, Irene may be required to carry out the following roles:

1. **Effectively React to Users' Requests**

2. **Preserve Users' Privacy**

3. **Secured Protection of Information and Identity of Users**

4. **Authentic Claims**

5. **Availability of Potential Matches**

4.5 Scenarios

Both malicious and non-malicious factors could lead to an introduction being unsuccessful. While we may not be able to control the roles that Alice and Bob assume, we

can however make efforts to control the role that Irene carries out so as to improve users' security. Here we give examples of scenarios that could vary the outcome of an introduction in dating sites and specify the roles Irene failed to carry out that could have changed the negative outcome of an introduction.

The scenarios below all assume the following. Alice is seeking love and companionship. She wants to meet more people beyond her everyday social interactions and improve her relationship life. Alice decides to engage the services of an introduction person called Irene, who specializes in introducing strangers with similar interests, in the hope that they find love. Irene offers both free and paid services, with the promise of offering better services should her users pay. Alice obtains a profile template from Irene and truthfully fills out personal and confidential information about herself, with the belief that the more Irene knows, the better the chances of her introducing someone Alice will like and vice versa. Alice hands back her profile to Irene, who includes it to her pool of profiles. Alice trusts that Irene is a credible introducer who only has valid profiles in her collection of profiles.

4.5.1 The Ideal

Bob is also in search of love. He had previously truthfully filled out his profile, and handed it to Irene. Both Bob and Alice believe that, like them, everyone is also sincere in filling out their profiles. Irene introduces many profiles to both Alice and Bob. These profiles were profiles Irene found similar to their submitted profiles. Engaging the services of Irene also meant Alice and Bob could go into the pool of profiles Irene has and look at other submitted profiles to decide for themselves if they would like to date the person with the profiles. Alice and Bob now have many profiles at their disposal. Of all the profiles Alice was introduced to, Bob's profile caught Alice's attention the most. Alice decides to contact Bob through the online space Irene provided and sends Bob a message. Bob sees Alice's message and gets Alice's profile from Irene to find out if he likes her profile. Bob decides he likes Alice's profile too and chats with her online for a while. Both Alice and Bob eventually meet in person and Bob finds out Alice was who she claimed to be in her profile and vice versa. They go on a couple more dates, fall in love and eventually get married. The introduction made by Irene in this case was successful.

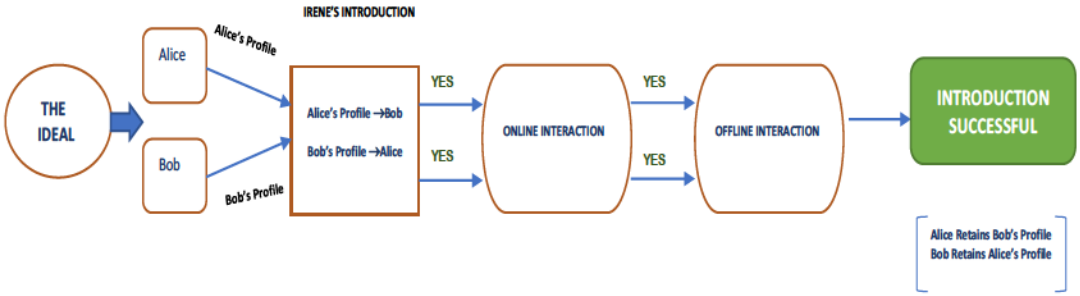

Figure 4.1: Diagram Showing The Ideal Scenario

4.5.2 The Graceful Ending

In this case Irene gives Alice, Charlie's truthfully completed profile and vice versa. Charlie, like Alice, is also looking for love. Both Charlie and Alice decide to chat in the online space Irene provided. After few online interactions, they find out they don't have as much in common as they thought they had and didn't really like each other. They decide to end things. Alice and Charlie both dispose of each other's profile and go back to Irene to get more profiles with similar interests. In this case the introduction was unsuccessful.

4.5.3 One-sided Interest

Cole, like Alice, is also in search of love. Cole truthfully completes his profile and gives it to Irene. Irene gives Alice, Cole's profile and vice versa. The both decide they like the other's profile and resolve to interact in Irene's online space. After chatting online for a while, Alice found out she didn't like Cole as much as she thought she did and decides to end all interactions between the two of them. Cole on the other hand thinks differently and feels he has found his soul mate in Alice. Alice disposes of Cole's profile and goes on to request for more profiles from Irene. Cole on the other hand holds on to Alice's profile and starts molesting her online consistently as a way to get Alice's attention. Alice decides to report the situation to Irene who blocks Cole from accessing Alice on the online space Irene had initially made for their

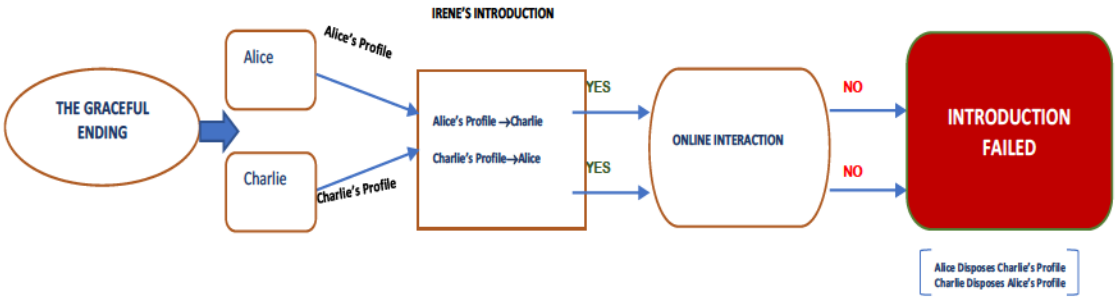

Figure 4.2: Diagram Showing The Graceful Ending Scenario

communication. However, Cole still has Alice's profile details and resorts to cyber bullying of Alice. Alice decides to collect her profile back from Irene and cut off all ties to Irene's introduction service, but Cole still has a copy of Alice's profile that cannot be returned. Even though Alice no longer uses Irene's service, Cole can still find Alice and bully her both online and offline whenever he pleases. In this case the introduction was unsuccessful.
Irene failed in the following roles:

1. Effectively reacting to user's request of having her match blocked and her profile deleted.

2. Preserve user's privacy

4.5.4 An Incomplete Profile

Irene gives Alice, Cody's profile and vice versa. However, Cody's profile is incomplete and omits a number of details about Cody. Alice decides the little Cody wrote about himself was interesting and resolves to interact with him online. Not long after, Alice found out Cody wasn't someone she wanted to keep talking to and decides to break off all communication with him. She disposes of his profile and blocks him from accessing her on the space Irene had provided. Cody on the other hand has major issues with anger and rejection, which was something Irene's profile template didn't account for. Cody uses Alice's profile to stalk her online and resorts to assaulting her constantly. Cody also found Alice's Facebook name and pictures and wrote a lot of demeaning comments on her Facebook wall. Through this means, Alice's coworkers found out

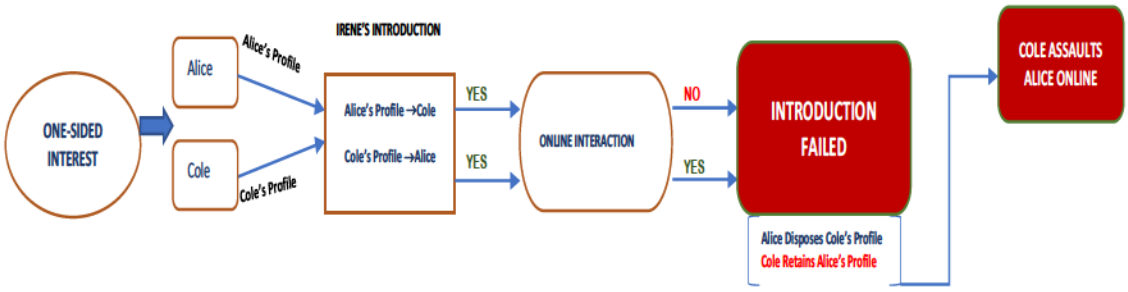

Figure 4.3: Diagram Showing The One-sided Interest Scenario

she was engaging the services of Irene. This further led to Alice being harassed in her workplace by her coworkers. In this case the introduction was unsuccessful.

Irene failed in the following roles:

1. Detailed Profile Requirements
2. Verification of Profile Completion
3. Effectively reacting to user's request of having her match blocked
4. Preserve user's privacy

4.5.5 A Killer

Alice was introduced to Cam through Irene's "Soul Mate Match" special feature. Irene claimed the feature only showcases people she was strongly confident Alice will date. Alice's understanding of the feature was that, of the possible matches Irene suggested, Cam had to be her soulmate and was therefore the best match for her. As such, Alice was confident she had found the one. Both Alice and Cam were looking for love. However, unknown to Irene and Alice, Cam had a bad criminal record and a violent past. Both Alice and Cam seemed to like each other a lot when they interacted online. They eventually decided to meet in person. Cam almost instantly became obsessed with Alice on meeting her in person for the first time. Alice on the other hand, didn't think she liked Cam as much as she thought she did. She decided to end their first date earlier than planned. Cam wasn't having any of that. He was very obsessed with Alice and wanted to spend every second of that day with her. Cam

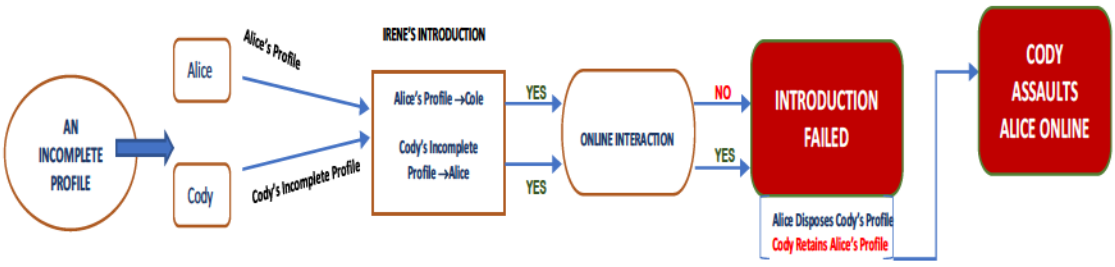

Figure 4.4: Diagram Showing An Incomplete Profile Scenario

ended up raping Alice. When Alice threatened to tell the police, Cam mistakenly kills Alice in a bid to shut her up. In this case, the introduction was unsuccessful.

Irene failed in the following roles:

1. Detailed Profile Requirements
2. Authenticity of Identity and Collected Information
3. Authentic claims

4.5.6 Blackmail

While Alice is seeking love, Dave is not. Dave deceitfully fills up the profile template he got from Irene and hands it back to her. Irene suggests Dave's profile to Alice as a profile that closely matches hers and Alice loved Dave's profile. Irene also gives Dave, Alice's profile and Dave sends Alice a message almost instantly. Dave chatted with Alice for a couple of weeks and then requests nude pictures. Alice sends him a few and Dave also sends Alice a couple of pictures without properly showing his face. Dave requests for more nudes and Alice sends him some more. Afterward, Dave started demanding money from Alice and threatened to release the nude pictures to her Facebook contacts if she refused to pay. Alice was scared because she knew Dave could easily find out her Facebook name and access her friends. Alice couldn't report to Irene as that would only make Dave carry out his threat. Alice decides to give Dave the money he requested. However, Dave could never get enough and he kept demanding for more. Alice kept giving him but she knew she couldn't keep up. Alice's reputation was paramount to her and she only sent the nude pictures to Dave

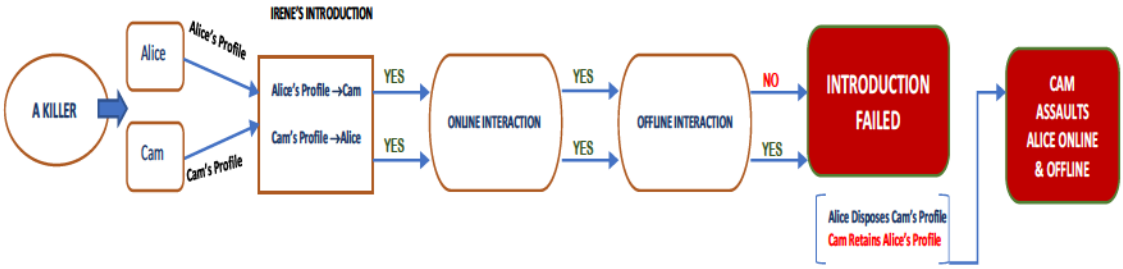

Figure 4.5: Diagram Showing A Killer Scenario

because she thought he truly cared about her. Alice slowly slid into depression and eventually committed suicide. In the case, the introduction was unsuccessful.

Irene failed in the following roles:

1. Authenticity of Identity and Collected Information

2. Preserve Users' Privacy

4.5.7 Trafficking

Devon has also deceitfully filled out the profile template he got from Irene. Devon's profile included pictures of places he claimed to have traveled to. He stated on his profile that he loved exploring new cities and he was looking for someone who would be willing to travel the world with him. Alice had listed traveling as one of her hobbies, so she was elated when Irene introduced Devon's profile to her. Devon and Alice chatted in the online space Irene provided and Alice was pleased at how much she seemed to have in common with Devon. After a while, Devon explained to Alice that he was out of the country exploring a new Island. He told Alice he would really love to see her in person but he didn't want to wait to travel back to where Alice was. Devon suggested Alice meets him on the Island where he was currently, so they could explore the place together, after which they could travel back. He offered to bear the cost of transportation and accommodation involved in carrying out the trip. Alice agreed to Devon's suggestion as it seemed like a dream come true for her. However, when Alice got to the Island, she realized it was all a scam and Devon was a sex trafficker. Alice was stripped of all her belongings and was denied access to

the Internet. Alice tried to run away and alert the Island authorities, but all efforts proved futile as she was a foreigner in the Island. In this case, the introduction was unsuccessful.

Irene failed in the following role:

1. Authenticity of Identity and Collected Information

4.5.8 Fraud

Alice was introduced by Irene to Dan's profile, and after talking online with Dan, Alice felt like she had found true love. Dan on the other hand had a very deceptive profile with a fake Facebook account. Dan insisted they meet in person and Alice obliged. While on their date, Dan sedated Alice and stole all her credit cards, money and jewelry. After Alice woke up and discovered what had happened, she decided to report the incident to Irene and the police. However, when Alice went to Irene's pool to get more information about Dan from his profile, she discovered that Dan had collected his profile from Irene and discontinued the service. Dan's fake Facebook profile had also been deleted. Dan went on to fill out another profile and handed it back to Irene with a new fake identity. In this case, the introduction was unsuccessful.

Irene failed in the following roles:

1. Authenticity of Identity and Collected Information
2. Preserve Users' Privacy
3. Effectively reacting to users' report

4.5.9 Hacking

Henry has been surveying Irene's pool of profiles for a while now and analyzing the mechanism she uses to operate and deliver her services. After a couple of trials, Henry was successfully able to hack into Irene's large pool of profiles and released the personal details of many of Irene's users to the internet. Henry went on to blackmail other users with the threat of releasing their confidential profile details as well as their identity. Henry was also able to get some credit card details of users who paid for Irene's service.

Irene failed in the following roles:

1. Secured Protection of Profiles and Identity of Users
2. Preserve Users' Privacy

4.6 Discussion

In this chapter, we examined the threat model of online dating sites and used various scenarios to showcase the possible threats that occur on this platform. We also identified roles the dating site model failed to perform that would have prevented negative outcomes. In the next chapter, we present the results of a user study carried out to find out how dating sites users determine who to trust, in order to mitigate the various threats identified above. We also determine if these trust strategies are adequate or if better ones need to be defined.

Chapter 5

Users' Trust and Security Strategies for Online Dating

In this chapter we present a user study carried out to determine the strategies users employ in trusting people they are introduced to online, and how they ensure safety. Through semi-structured interviews with ten subjects and qualitative data analysis, we explored how users of online dating sites address their privacy and security concerns. The goals of this study were as follows:

1. Understand the security and privacy precautions taken by users in online dating sites.

2. Understand how users balance the need for sharing information with the need to protect themselves.

3. Explore situations where users discover others were untruthful in their representations and how this might endanger them.

4. Explore how users gauge the accuracy of information revealed by others on dating sites, to determine who to trust.

This chapter is divided into three sections. In the first section, we describe the methodology of the user study. In the second section, we present the results of the user study. We analyze and discuss the results in the third and fourth sections respectively.

5.1 Methodology

After receiving clearance from our University's Research Ethics Board, we recruited 10 participants, primarily through a university-wide email announcement and subsequent snowballing. We had difficulty recruiting more participants, due to the stigma attached to using dating sites; however the number of participants was sufficient to carry out in-depth qualitative analysis of data. We also did not opt for a simple

mechanical turk survey as this would have not been a suitable means for producing substantial data for qualitative analysis. The participants included six females and four males with ages ranging from 18-50 years old. Six participants were students while the rest were university staff. All participants had used a dating site at some point for at least a month. The participant demographics are summarized in Table 5.1.

We conducted individual semi-structured interviews with participants. While the interview was structured around a question guide, digressions were allowed so participants could expand upon their experiences where appropriate. We chose this approach because it offers participants the freedom to express their view in their own terms, providing more reliable, comparable, qualitative data.

Participants completed a demographic questionnaire before their interviews. Interview sessions were audio-recorded. Participants were asked to discuss the various activities they have carried out on dating sites and the end results of those activities. Participants could skip any question they were not comfortable answering. Participants were further encouraged to share additional dating site experiences they may have that could be of benefit to the research. Each session lasted approximately 20 minutes.

The questions covered:

1. The sites they use, whether they pay for these services, whether their online interactions have resulted in real life meetings or relationships.

2. The completeness and accuracy of their profile information, and how this affected their experiences.

3. The precautions taken to avoid scammers.

4. Any situations where they have dealt with scammers, untruthful others, or dangerous situations.

We conducted thematic analysis on the interview data. This form of data analysis is suitable for qualitative data analysis and involves a small number of participants. From the users' responses, we extracted relevant incidents and common themes, paying particular attention to issues of trust, security, privacy, and safety. We also

ID	Gender	Age	Occupation
P1	Female	22	Masters Student
P2	Female	18	Undergraduate Student
P3	Male	21	Undergraduate Student
P4	Male	19	Undergraduate Student
P5	Female	24	Research Assistant
P6	Female	20	Undergraduate Student
P7	Female	49	Administrator/Advisor
P8	Male	20	Undergraduate Student
P9	Male	23	Trainer
P10	Female	50	Staff

Table 5.1: Demographics summary of participants

tabulated common responses as an indication of their frequency. We note that these numbers represent a lower bound since some participants may also have similar behavior or opinions but not have explicitly mentioned it since responses were open-ended.

5.2 Results

Using thematic analysis, participants' responses have been grouped into themes, focusing on security, privacy, trust, and personal safety issues.

5.2.1 Security And Privacy Precautions

Participants generally felt a need to protect themselves while on dating sites or on dates. They reported several strategies and precautions, as summarized in Figure 5.1. We observe that females reported more protective strategies than males. Next, we describe these strategies and offer exemplar quotes from participants describing their approaches.

Providing Limited or Incorrect Information

9 participants (5 females and 4 males) reported omitting information when filling out their profiles on dating sites. No one felt that this had negatively affected their dating site experiences.

Not all participants omitted information solely for security or privacy reasons. Two participants (1 male and 1 female), said they omitted information in order to

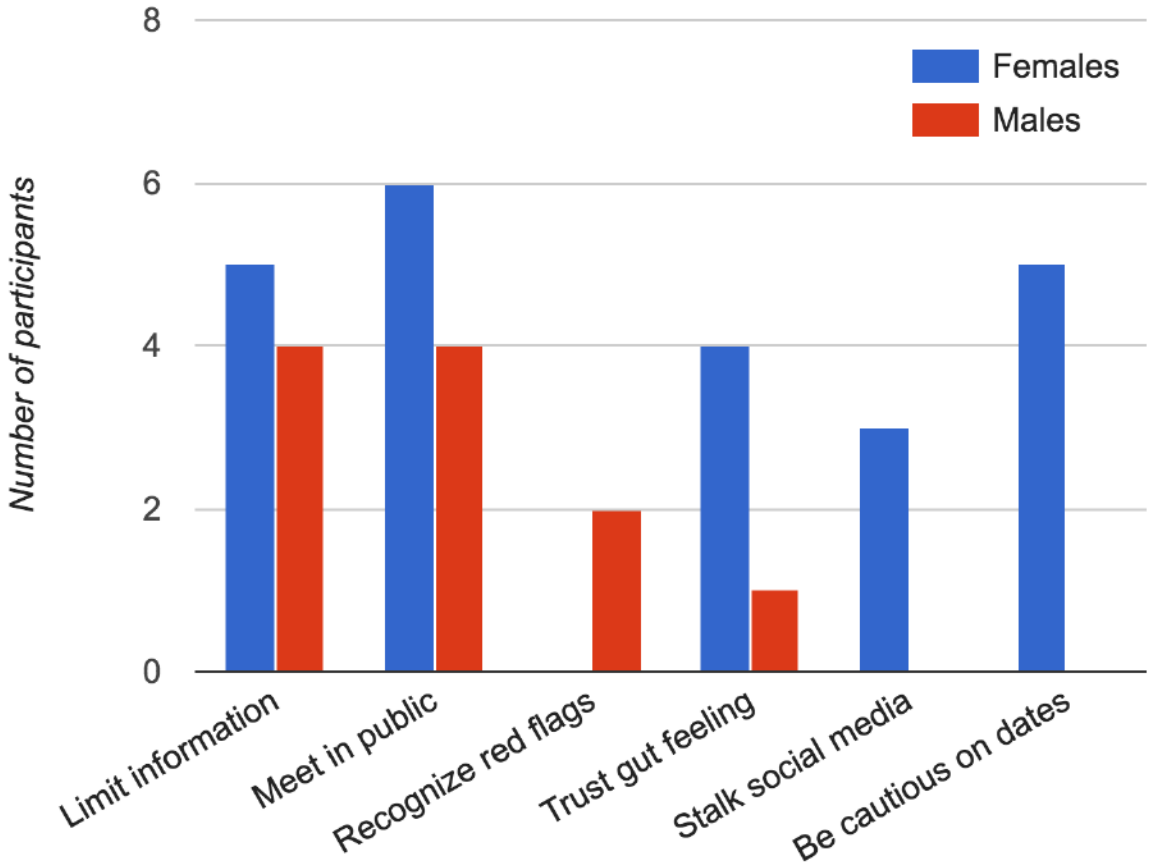

Figure 5.1: The number of participants reporting each precautionary measure

invoke some form of mystery. P2 explains, *"If you put out all of the information at once, what are you going to say when you meet the person?"*. Therefore 7 participants omitted information as a precautionary security and privacy measure. Participants claimed they left out information that was too readily identifiable or revealing, such as their home address, occupation, date of birth and income. P3 commented, *"If you call your bank at anytime, the first thing they would ask you is your date of birth, hence I never put up my correct date of birth when filling out profiles"*. One participant, P5, explained that in addition to omitting information about herself, she also gave misinformation to stay safe, saying, *"I always fill out a wrong digit or two in my mobile number whenever I need to put it up"*.

The remaining participant, on the other hand, said she truthfully fills out all fields and uploads her most recent pictures when filling out profiles. She explains, *"I am always 100% true... there is nothing you can do if people recognize your picture from a dating site, it's the price you have to pay."*

Interestingly, all 10 participants uploaded their pictures. When asked whether they considered photos personally identifiable, none of the participants could defend this practice, acknowledging that it was a concern but believing it was a necessary risk. P5 explained *"Yeah, they can trace me... but no one's going to talk to you if you don't have your picture up, that's how dating sites work."*

Sharing Further Information

As a security measure, participants delayed sharing some information until they felt they could trust their matches better. Participants, however, had varying ideas on how long the waiting period should last before exchanging more personal information or agreeing to meet in person. P5 explained that she would talk to a match for at least a week before exchanging phone numbers. P2, on the other hand, said she would never exchange phone numbers or further personal details until she met the match in person. P10 was of the opinion that it was best to collect the match's phone number but to never give hers and hide her caller ID whenever making calls to the match.

Setting Up First Dates

All 10 participants believed that a first date should be set up in a public location, for example, at a coffee shop. However, strategies for when to meet potential matches varied. Two female participants said that for security reasons, it was better to meet sooner rather than later. P5 narrated an experience of how a dating site user she was starting to like, kept postponing their date. She soon discovered the user was a scammer. She explained that scammers would rather not meet and that if a match repeatedly postponed the meeting time then you should be suspicious. However, three other participants were of the opinion that to be safe, it was better to meet only after talking for an extended period of time. P2 thought three weeks was sufficient to know a person, after which she would set up a date. P1 insisted that two months was the best time frame.

Recognizing Weird Requests As Red Flags

Two female participants stated that as a security measure, they stayed away from guys who made 'weird' requests such as asking for nude pictures or monetary assistance. They believed those type of guys were mostly scammers. To further illustrate her point, P10 said, *"One guy I was chatting with online claimed he was staying at Sussex Drive [in Ottawa]... only the Prime Minister [of Canada] stays there! It was then I discovered he was a scammer... and soon enough he started requesting money."* She further explained other cues that she utilizes to identify potential red flags in her conversations with other dating site users, such as location or time differences. In staying safe online, half of the participants (4 males and 1 female) mentioned that going with their gut feeling was critical as it was almost never wrong.

Stalking Social Media

Three female participants admitted to carrying out social media stalking as a precautionary measure to uncover details about potential matches. P2 explained, *"[before agreeing to meet up] I'm good at stalking, I look up people on Facebook, Twitter, Instagram... everywhere!"* P10 further asked questions to verify if potential matches can back up what they shared online; she explains, *"I always do my research online,*

then I ask them direct questions to confirm if what they wrote is true."

Being Cautious While On Dates

Five female participants took additional precautions while on dates, such as making sure a third party was present. P1 commented *"... (my match) came to my apartment for the first date, but I made sure my roommate was in."* P2 agreed, saying she always went on dates with a friend, *"Whenever I go to Starbucks for the dates, I always went along with my friend... he [the date] would never know my friend and I know each other... my friend sat out of sight watching us all through the date."*

Others made sure that someone knew the details of the date and sometimes made it clear to their dates that this was the case. P6 explained, *"I would give my friends his picture and they will always know where we are meeting... like when I wanted to go with a guy on a first date, I took a picture of his license plate number. He didn't know. I then texted my friends the make of the car. During the date, I kept telling him I'm updating my Facebook status. It was like making a subtle threat to him".* P5 also explained *"My roommates always knew where we were headed."*

5.2.2 Balancing Privacy and Sociability

Participants struggled with how to fulfill their desire for privacy with the purpose of the dating site, which is to meet people, socialize, and get to know each other. In many cases, they sacrifice their privacy when faced with a choice between the two. This is clearly a situation where the security and privacy are hindering the user's primary task [276].

Three participants (2 males, 1 female) agreed that there is such a thing as "too much information" when using dating sites. But none could give a definite answer on where they draw the line on how much information is considered "too much." Those who considered omitting information from their profiles were asked how they decided what should be included and what should be left out, but no consensus emerged. P3 noted, *"There's nothing you can really do to keep safe online cause it's online... they could always hack into it anyway... so... ".* He further explained, *"When using dating sites, sometimes I would put up sensitive information... in my head I'm like you shouldn't be doing that, but there's not much you can do."* P5 went

on to say, *"I just assume that people at the other end are also as sincere as I am and are looking to just date too"*. P10 and P5 explained that it was only when they were *"less protective and loosened up"* that they found suitable matches. P10 explained, *"I was very careful not to give out too much information, but then it could restrict you... so I loosened up... you just have to be wise."* P5 commented, *"I started to have lots of success when I started joking about it and let down my guard."*

Participants thus compromised between the need to share information and the need to stay private and secure. In these circumstances, participants clearly believed that one had to be sacrificed for the other since they saw positive results when they revealed more information than they initially wanted.

5.2.3 Detecting Scammers and Gauging Trustworthiness

Participants had developed several strategies for identifying potential scammers and determining who to trust, mostly based on social cues from the potential match. Figure 5.2 summarizes these strategies.

Trusting A Gut Feeling

Four participants (all male) claimed they relied on their gut feeling to know if the information provided online is true or whether a scammer is at play. They recognized, however, that this was not a foolproof strategy. P3 commented, *"it's tough... I mean if you are a good judge of character that may help, but really you never know."*

Relying On Social Norms

Participants relied on characteristics of the conversation and interaction to identify potential threats. When these varied from the expected social norms, this was a cause for concern.

Three participants (2 females, 1 male) claimed that the topic and pace of conversation could sometimes help them determine if a potential match is a scammer. P1 commented, *"Creepy ones always start the conversation way off the line."* P4 explained, *"if a first conversation starts with 'Hey baby, how you doing?'... I'm like 'really'?"* Two females were alarmed if matches consistently requested nude pictures. One male participant (P4) strongly believed that if the conversation speed was too

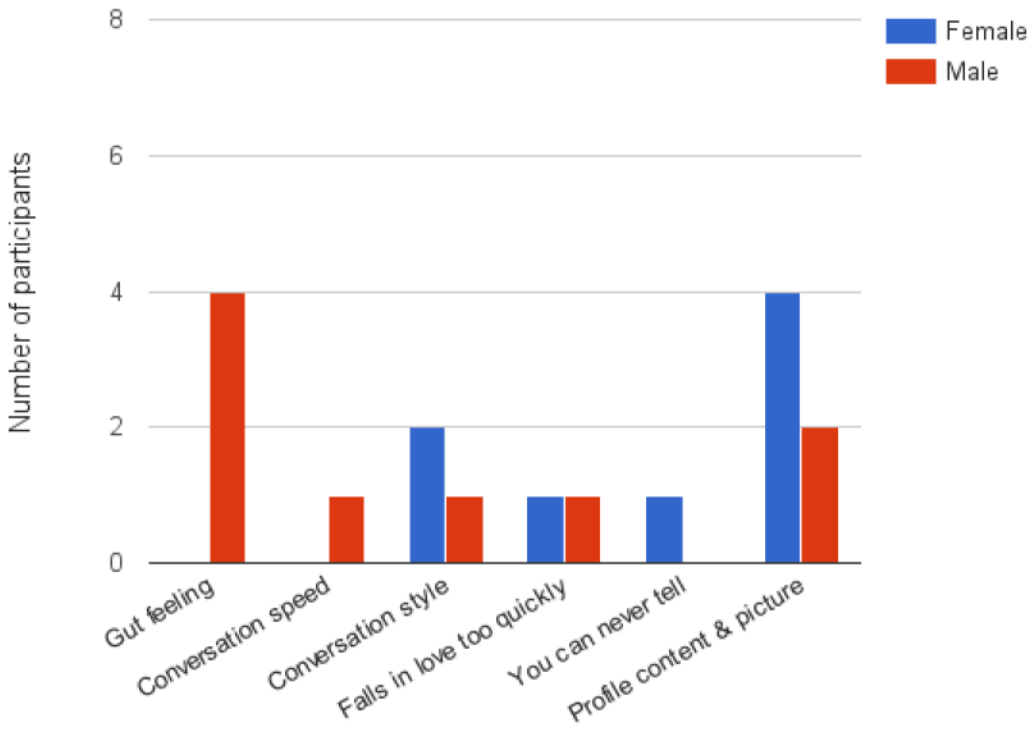

Figure 5.2: Shows the male and female ratio of how participants gauged the accuracy of information shared online

fast, then the person was most likely a scammer. He explained, *"People who reply way too fast or way too often are definitely scammers"*. P2 elaborated, *"If they ask to hang out too soon, they are scammers!"*

Others thought that displays of emotion that seemed out of sync with the stage of the relationship were suspicious. Two participants (1 male, 1 female) strongly believed that if a match professed falling in love very fast, it was another sign of a scam was underway. P7 comments, *"All of a sudden they are in love with you... they want to meet you right away, those are fake people."*

Noticing Inconsistencies in Profiles

Six participants (4 females and 2 males) believed that inconsistencies in normal profile content and picture could signal a scammer. Participants attributed weight to the profile pictures, expecting them to depict 'average' people and expected profile descriptions to provide sufficient detail about the person. Two females felt that if a profile picture is too cute then the profile is suspicious. Three participants (2 males, 1 female) said weird pictures accompanying weird profile descriptions were a cause for concern. To illustrate this, P4 explained *"Some people have like a dog as profile picture... and write as description 'I'm a dog'... those are completely fake..."* P6 claimed sighting multiple profiles for the same person was also a red flag, *"I found same person (the same profile picture) multiple times, but I can tell it's a different person because of the way they speak and respond."*

Requesting Proof

In some circumstances, participants who were already suspicious took extra steps to determine whether they were interacting with a scammer. Two participants (1 male, 1 female) believed that asking for proof of identity was one of the major ways to detect whether a person was a scammer. They did not expand on how they determined the authenticity of the provided proof. P8 explains, *"It's hard to do [detect scammers]... I ask them to prove it [their identity] by sending maybe a picture or something specific."* P10 shared her experience with a scammer, *"So the Nigerian scammer that claims he stays at Sussex Drive started asking me for money that he was stuck somewhere, I told him to scan his passport and send to me... I never heard from him again."* It

is unclear what her next steps would have been had the scammer provided a photo of a passport.

You Can Never Tell

One female participant held on to the thought that there was no way you could tell if a potential match was a scammer solely through online interactions. P6 explained, *"It's really hard to do. It's only if you are going to meet someone, you would know if the person is scammer or not. You just have to meet in a public place."*

5.2.4 General Dating Site Experiences and Feedback

Looking at outcomes, participants seemed to have had reasonable success with dating sites despite their concerns about trust, privacy and security. Overall, eight participants (6 females, 2 males) had set up dates with people they met on dating sites. The most dates set up by a participant was 30 dates within a space of six months. Six participants (5 females, 1 male) were currently in a relationship with someone they met on a dating site. Two participants said they met people online, who, even though it did not result in a romantic relationship, were still very close friends. P3 explained that even though he had never gone on a date personally, he knew a lot of his friends had been successful at using dating sites.

Interestingly, their opinions seemed to contradict this apparent success. When asked what advice participants would give a friend who was considering using a dating site, half of the participants (4 males, 1 female) advised that people stay away completely from using dating sites. Two claimed that there was a social stigma attached to using dating sites and that people were better off without them. P2 explained further, *"Don't use it [dating site], it's a waste of time... imagine my parents asks me where we met? I would then say dating site?... it makes one look irresponsible."* P4 also remarked, *"Don't go do it [dating sites]... don't go there... it gets you down. It's also easy to waste your time and very emotionally draining"*. P3 cautioned, *"Try as hard as you can not to use it... stay off completely from it, it's not worth it... try and meet someone in real life"*. P6, who was in support of using dating sites, advised, *"Also don't go into it thinking you would have a long term thing, go with the mindset that you want to have fun and if it works that long term way good... else good."*

P5 also recommended that dating sites should adopt additional verification of users at registration to reduce the number of scammers and hence improve trust. She explained that she would like users to scan their passport or driver's license as a way of verifying their identity. She also worried about her past interactions on dating sites. She worried that her previous dating site may be hacked and all her sensitive sexual information would be made available to the public. She continues, *"I didn't think hard about that until when I was done with it [the dating site]. I was like, I shouldn't have been so truthful with these questions, what if they come back to haunt me in future?"* As dating sites become more popular, these types of regrets and anxiety about potential attacks are likely to increase.

5.2.5 Awareness of Security and Privacy Risks

Participants were sufficiently aware of security and privacy issues arising from online dating to correctly identify the major traits exhibited by dating sites scammers and their scams as identified in the threat model.

Huang et al. [115] discussed how dating site scammers make use of multiple profiles with the same fake content. Six participants correctly identified this scam. They noted that unusual profile content and multiple profiles with the same content could belong to scammers. Huang et al. further explained how scammers use very attractive profile pictures to attract unsuspecting users; our participants also noted this as suspicious. 30% of participants also correctly identified that unusual requests from dating site users such as request to share nude pictures or money could be a red flag that something is fishy, a characteristic previously noted in the literature [115]. Also, 10% of participants identified that the speed at which dating sites' users respond to conversations could also verify if the user is a scammer (see [115, 201]). Whitty et al. [277] noted that a dating site user who falls in love too fast or almost immediately, could be a sign that the user is a scammer. 20% of participants correctly recognized this trait.

On how users gauge the accuracy of information shared online and how they protect themselves from scammers, Gibbs et al. [93] identified using basic instinct as one of the methods. This was correctly identified by 40% of participants. However, gut feeling may not be sufficient to judge the accuracy of information put online or

to determine another user's sincerity.

Whitty et al. [277] noted that dating site users should take precautions before meeting new people, including taking time to get to know individuals and letting others know they are going on a date. 60% of participants let someone know their plans when going on a date. All participants (100%) were of the opinion that meeting someone from a dating site should be done in a public place. Also 90% of participants correctly identified that sharing limited information could help protect oneself from scammers.

Like McRae et al.[169], our participants were unable to come to a conclusion on how much information sharing was too much.

5.3 Analysis of User Study

Based on the results of the user study, Figure 5.3 presents a model showing the relationship between the problems faced by dating sites users and the methods that users used to protect themselves. The model is structured in three categories,

1. **Online Dating Realities:** This showcases the realties involved in making use of online dating sites as identified by users in the study.

2. **Risks Arising From Realties:** This describes the possible risks users can face as a result of the facts and realities identified.

3. **Mitigation Strategies:** This refers to the various methods implemented by users in the user study, to protect themselves from the risk associated with the corresponding reality.

5.4 Discussion of Results

As seen in the results, the problem of balancing security and privacy is a prominent issue faced by dating sites users. Users sometimes provide limited or false information in their profiles, but hope their potential matches' profile is truthfully filled out. Some users also create profiles that can't be directly linked to them, but they hope to be able to link other users' profiles in other to get the best possible match. This creates a paradox as seen in social psychology.

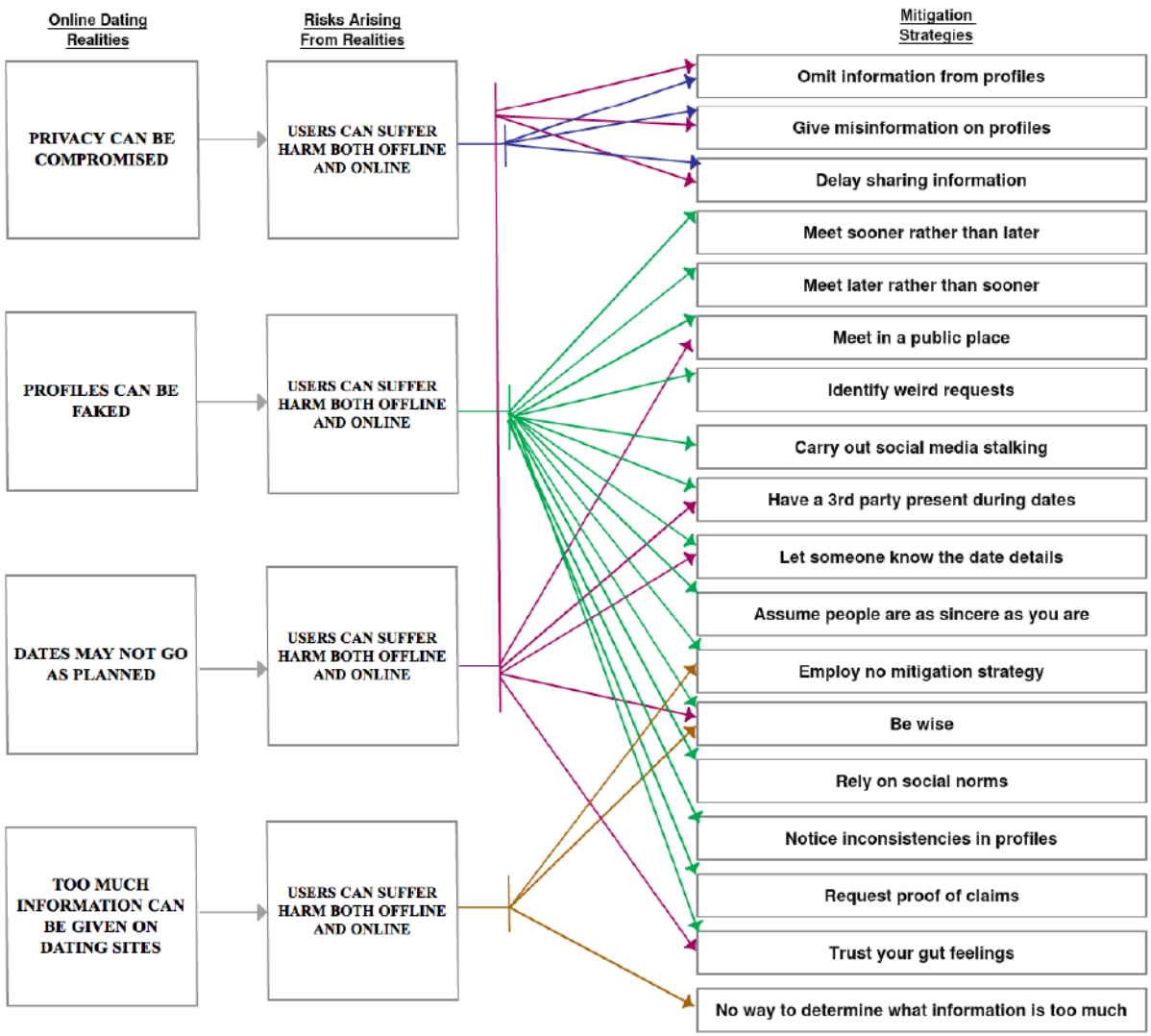

Figure 5.3: Model showing online dating realities, risks and mitigation strategies

On the collective trust strategies users employed, Bonabeau et al. [25] noted that though intuition plays an important role in decision making, it can be dangerously unreliable in complicated situations. Using intuition to judge the accuracy of information shared on a dating site may be even more dangerous because, as previously stated, scammers tend to exploit the vulnerable emotional state of users [115], leaving their gut feelings clouded. Our results indicate however that intuition, directly or indirectly, is key to how users of online dating sites determine who to trust and how they ensure their safety.

They look for "weird" requests and deceptive profiles based on heuristics derived from regular profiles. They observe whether correspondents reply too quickly. They determine what to share, and what not to share, on an ad-hoc basis depending on how safe they feel in a given interaction. These methods can all lower the risks of normal threats, i.e. avoiding the "creeps" and the "crazies." Con artists, however, are adept at taking advantage of such emotionally-driven decision making, and the relative anonymity and data analysis opportunities of online dating gives purveyors of scams plenty of opportunities in which to operate.

While none of our participants was deceived by an outright scam in their online dating experiences, this may be a result of our relatively small sample size. Even so, virtually all of our participants encountered some level of deception in online dating at a sufficient level that a common refrain was *"you can never know."* Mechanisms that can reduce the ability of individuals to deceive each other in online dating thus have significant potential for improving the quality of the entire experience. More practical approaches are needed to help dating sites' users better gauge the accuracy of information shared and determine who to trust, as the available ones are not sufficient to protect users and to prevent them from falling prey to scamming attacks. They also need help in sharing information about themselves in a way that protects their privacy and safety while also helping them find potential partners. Since users do not possess sufficient strategies to keep themselves safe while using dating sites, in the next chapter, we survey the trust strategies employed by dating sites in securing users, even as they introduce them to others online. We compare these strategies with Irene's ideal roles discussed in Chapter 4, to determine the viability of these trust mechanisms. We finally compare them with the trust mechanisms employed by

other CMIs.

Chapter 6

Trust Strategies Used By Dating Sites

All dating sites provide mechanisms to help individuals establish trust with potential matches. In this chapter, we evaluate and analyze the various mechanisms used to develop trust and improve the security of users on three popular dating platforms, Match.com, Plenty of Fish and Tinder. We compare these mechanisms with the roles described in the model dating service, Irene, in Chapter 4. We also compare the trust strategies employed by dating sites with those implemented by other CMIs. We finally discuss why some of the trust mechanisms employed on other CMCs may be ineffective when applied to online dating sites.

The rest of the chapter is divided as follows. We evaluate the trust mechanisms used by Match.com, Plenty of Fish and Tinder in the first three sections respectively. In the fourth section, we compare our findings with the ideal role of the introduction service discussed in Chapter 4. In the fifth section, we compare the dating sites' trust mechanisms with those of other CMIs and discuss their differences. We analyze and discuss the results of the evaluation in the sixth and seven sections, respectively.

6.1 Match.com

When new users signup to Match.com, a welcome message and registration confirmation notification is sent to the email address used to register. Match.com sends another email with an optional verification link, which if left unclicked, does not in any way stop the user from making use of the service. Users are also made to fill up their profiles during signup where they give information about themselves, both personal and otherwise, that could assist them in being matched. Match takes a few minutes to approve a profile and picture before it can be displayed. Users can also signup on Match.com using their Facebook account.

Match has both free and paid versions. With the free version, users receive notifications when prospective matches have shown interest in them or send them messages.

However, users are not allowed to see the pictures/profiles of these people or the messages sent, until they have fully subscribed for the service. Subscription is done by paying a renewable subscription fee. If users fail to subscribe, Match.com will continue to send regular updates of events happening on their account which the user can only see after subscription. This is usually done to prompt users to subscribe to their services.

We now describe the various mechanisms Match.com employs to establish trust between potential matches.

- Match.com provides users the ability to be able to block and unblock other users from contacting them. Users can block no more than 2000 members, after which users will have to unblock old users, for them to be able to block new ones. Users can also report people they do not feel comfortable interacting with. The options are displayed as, *"Block from contact, Block from search and Report a concern"* [162]. The blocked members are usually unaware that they have been blocked, and can still view the user's profile and send messages. However, the user who blocked the member will be unable to receive any messages sent from them [156] . Cobb et al. explains that dating sites users feel "empowered" by the ability to be able to block other users they would rather not communicate with [41]. They tend to feel a sense of safety knowing they can control those they communicate with and vice versa, which in turn helps users better trust the platform [29, 263].

- The site also gives the option of viewing only users with profile pictures. Previous research has shown that users who have more photos are generally more trusted than those who don't, whereby users are more likely to contact those with profile pictures than those without [81, 278, 117, 110]. Also, while profile pictures are being reviewed by Match.com's customer service team, the pictures are usually not displayed [155]. Therefore profile pictures give users more confidence that the profiles as well as the pictures have been approved by the site.

- Match.com uses the frequency of users' logins as a way of building trust in users. Users generally trust profiles with more recent logins, as this is viewed as an

indicator of a person's reliability, seriousness and availability [74].

- Match.com always indicates that a more completed profile gets more attention [154], which in turn suggests to users that complete profiles are more trustworthy.

- Match.com also offers *Mutual Match, Daily Match* and *Singled Out* features. These features present potential matches to users as selected by Match.com. The site explains that the matches have been chosen from their large pool of users, based on compatibility, and have been found to best suit the user as potential matches [159, 161]. Of their Singled Out feature, Match.com explains that they have high confidence that the selected few singled out, will be potential dates for users [161]. This helps users trust that they will most likely be interested in dating members acquired via these features.

- Subscribed members generally have much more benefits than non paying users, such as being able to receive and send messages to other users, even if a profile is yet to be approved by the site [160]. While explaining the benefits of paid subscription, the site states that subscription "creates a more secure environment and helps ensure that those you're communicating with are as serious in their search as you are." [158] This encourages users to trust paid subscribers more than non paying users.

- Users have the option of filling up their profiles at signup or at their own convenience. After the profile section has been filled up, Match.com's customer care team takes some minutes to approve the profile before it is displayed. During this period, free users cannot send messages, though paid subscribers are free to communicate even if their profiles are yet to be vetted. This process helps users trust that everyone's profile on the site is being vetted by Match.com's team, and can be trusted. It also creates a sense of trust in the service provided, with users feeling that someone, somewhere is watching out for them, when in reality this is not necessarily the case [163, 213].

- Match.com advertises upcoming events for singles to participate in. This helps create a sense of community feel for those that attend the event and aids in

Feature	Match.com	POF	Tinder
Block/Unmatch users	Yes	Yes	Yes
View only users with pictures	Yes	Yes	No
Warning about fraudsters	Yes	No	No
Report users	Yes	Yes	Yes
Frequency of users' login	Yes	Yes	No
Completed profiles	Yes	Yes	No
Subscription to paid versions	Yes	Yes	Yes
Delayed approval of profiles and pictures	Yes	No	No
Events	Yes	Yes	Yes
Special Features	Yes	Yes	Yes
Facebook verification	No	No	Yes
Instagram verification	No	No	Yes

Table 6.1: Mechanisms used in online dating platforms that helps build trust in other users.

building trust in the availability of potential singles on the site.

6.2 Plenty of Fish

Plenty of Fish (POF) is one of the largest free dating sites available [196]. The site however has an upgraded version which users have to pay for in order to put their pictures in major searches and be seen by more people. However, the basic services offered by dating sites such as viewing pictures, receiving and sending messages, and finding matches, are offered for free. During signup, users fill out their profile which includes personal details and basic interest questions. Like Match.com, POF does not verify your account through your email address. After signing up, new users receive a welcome message from the CEO, after which the users can go on to the site and find people of similar interests.

Like Match.com, POF uses several mechanisms to establish trust between potential matches.

- POF does not allow users to change their birthdays or gender after two weeks of signing up for the service. We believe this is a safety and precautionary measure taken by site, which helps to build trust in the profiles of the users, whereby users are certain their potential match is unable to change their age in order to fit the user's criteria.

- Users who present a variety of pictures on the site are viewed as more trustworthy, with the site encouraging users to upload a minimum of 3 photos, explaining that the more pictures users put up the more people will be able to know how they truly look [98]. These multiple pictures help build confidence in people, making them believe that they are interacting with the same person and not fake individuals. The site further states, "POF users with at least 10 images on their profile receive 8 times more messages!" [194, 70]

- POF claims to delete accounts with sexual language; they explicitly state, "If your profile contains sexual language of any kind your account will be deleted." The site also explains that once a user is deleted, they will be prevented from signing up again. This helps users better trust the services offered on the platform. However, users signing up again for their service can simply be done by changing the email address used to signup initially.

- POF also has a feature called *"Rate Images"* where they display a series of profile pictures that are mostly inappropriate and ask users to make POF better by rating these pictures. They also present instructions on how these pictures should be rated. By enabling users to enforce community guidelines, POF implicitly builds trust in the community of potential matches on the site.

- POF also provides login updates of users, showing users that are consistently logged in. This helps users identify active members and trust that those they are interacting with are actively involved in the platform.

- POF gives users the option of receiving messages from only upgraded users. The site states that, "The best way to be successful on POF is to become an Upgraded Member." [193]. This creates a form of trust in users, making them believe that those "upgraded" profiles are sincere users and not scammers.

- POF also has a section that displays mutual matches for users, tagged *"My matches"*, which states, "None of the users who have messaged others for sex/intimate encounters show up in your matches. If you want to prevent people who have messaged others for sex or intimate encounters from contacting you, you can block them entirely here". This filter helps users trust that those

they are interacting with through this feature, have never committed those acts, which is not always the case [213].

6.3 Tinder

Tinder is a dating platform that currently only works on mobile devices. Unlike other dating sites and applications, Tinder forces all users to signup with a Facebook account. Tinder makes use of users' Facebook profile to set up a profile on their account. After signup, users can see pictures of other users that are within close range. As series of these pictures is displayed and users swipe to verify their interest in the picture of a particular person. If that person also shows mutual interest, then a match is formed and both parties can begin chatting.

Tinder's strategies for establishing trust between potential matches is a bit different from those of Match.com and POF.

- A major way Tinder builds trust and develops a sense of security in its users is by allowing users to signup on the platform only through their Facebook account. This is Tinder's method of verifying users are who they claim to be and to check for people's identity. While this seems like a better strategy employed than other conventional dating sites, this however does not stop creeps and scammers from creating fake Facebook accounts with the sole purpose of using them on Tinder [185].

- On Tinder, while users can adjust the distance within which a match can be searched for, users cannot change the location from where the search is made. Tinder applies a user's Facebook location or the current GPS location of the user's phone, depending on the chosen setting. This helps build trust in users that people are actually where they claim to be. For users to change location to a specific place, get their profile boosted to the top searches once a month, turn off ads, control who sees them, make their distance invisible and other features, users have to pay a fee.

- Tinder has *Tinder social*, where users' friends can invite them to go out on a social. This builds a form of community feel to the site for those people that

choose to engage in the social. Tinder also allows the creation of groups on Tinder social.

- Though not everyone uses Instagram as an additional feature, Tinder allows people to also connect their Instagram account to the site to help build trust in users.

- Users cannot change their ages from their profiles on Tinder, whereby for that to be done, users have to delete the Tinder account, which also automatically deletes all previous messages and previous matches, change their age on Facebook, and then create a new account. To also change a username on Tinder, the user has to update their Facebook name. If their Tinder name doesn't change after few days, then they have to delete their account and start over. This process also applies when a user wants to change their interests.

- Tinder also has "verified" badges to confirm the authenticity of profiles; however, it offers this feature to only celebrities, brands and public figures. For those people to get the verified badge they have to send an email to an authorized email address. The key question though is, why would a public figure want to be verified on a dating application or site?

- Tinder users also have the option of reporting users. When a user is reported, Tinder bans the user for a couple of days, during which they review the account [264]. If reported users want to clarify their stand to Tinder, they have to send an email to Tinder. Users can also block or unmatch with someone if they please. However once a user is blocked, it is permanent, and they cannot be unblocked. Blocking means you completely disappear from the other person's search, such that you will be unable to message them and vice versa.

6.4 Comparison With Irene's Introduction Service Roles

Based on experiments and the findings in the case study listed above, we now compare the roles carried out by the introduction services Match.com, Plenty of Fish (POF) and Tinder, with those carried out by Irene in an ideal situation, as described in Chapter 4. Table 6.2 shows a summary of the comparison.

1. **Detailed Information Requirements:** While Match.com and POF require users to answer some personal questions in order to be matched, there is currently no profile requirement question that will enable users to know about their matches' personal and social vices or habits. Though such information may not readily be given, the presence or obvious absence of such information can help users better decide on who they would rather be matched with. Tinder on the other hand does not ask for personal user preferences to aid matchmaking, but simply makes use of the users' Facebook profile.

2. **Verification of Information Collected:** In Match.com and POF, users' profiles do not need to be completed in order for users to interact with potential matches or for the dating service to suggest potential matches to them. This also applies to Tinder whose users' Facebook profiles do not need to be completed for a match to occur.

   In the case of Match.com, profiles are checked to ensure the absence of offensive words [163], however users are sent matches almost as soon as they signup, even before profiles are checked and approved.

   When signing up on POF, while all profile fields are marked "required", they do not need to be filled up for users to make use of their services. Users' profile are also not vetted for content. The site also states that they delete pictures which do not meet their requirement [192, 195], however they give the responsibility back to users through their *"Rate Images"* feature.

3. **Authenticity of Identity and Collected Information:** Our definition of authenticity of identity and collected information specifies that users are checked to ensure they do not have previous traits or a record that could jeopardize the safety others. Match.com and POF do not authenticate the identity of their users. Tinder attempts to use Facebook as a means of authenticating its users; however, Facebook does not carry out any background checks or prevent users with a past criminal record from signing up for their services [78].

4. **Secured Protection of information and Identity of Users:** Instances of security breaches, where users' information was leaked, have been reported on all three dating services [84, 101, 139, 95, 186, 128].

Irene's Ideal Roles	Match.com	POF	Tinder
Detailed Information Requirements	No	No	No
Verification of Information Collected	No	No	No
Authenticity of Identity	No	No	No
Secured Protection of Information and Identity of Users	No	No	No
Preserve User's Privacy	No	No	No
Authentic Claims	No	No	Yes
Availability of Potential Matches	Yes	Yes	Yes
Effectively React to User's Requests	No	No	No

Table 6.2: Comparison of Irene's ideal introduction roles with those offered by Match.com, POF and Tinder

5. **Preserve Users' Privacy:** On Tinder, users' Facebook information is used as their profile information. Users can also subscribe to Match.com through Facebook, and have the option of uploading their Facebook pictures to the platform. In Match.com, non-active members' profiles can be seen [163, 153]. The site also retains users' profiles in their database after deletion [157, 11, 285, 83]. In POF, users can still view deleted profiles.

6. **Authentic Claims:** As seen in their special features and their website statements, Match.com and POF make claims that are not necessarily true and cannot be backed up or verified [206].

7. **Effectively React to User Requests:** Blocking of users on Match.com, POF and Tinder does not prevent the user from being contacted through other linked social media platforms. Users' profiles are also never completely removed from the dating service.

6.5 Comparison With Trust Strategies Implemented By Other CMCs

Figure 6.1 shows the comparison of the trust strategies used by dating sites with those employed by some CMIs, as listed in Chapter 3. Dating sites currently do not make use of most of these trust mechanisms. An important trust mechanism implemented on every other form of computer mediated communications, but which will be ineffective in dating sites, is the use of reputation systems. As explained in Chapter 2, reputation systems are used in CMCs as a major way to build trust in

online users about the viability of a communication, based on past successes. It helps online users decide if to purchase a particular good or engage in a service. Reputation systems are implemented in the form of feedback, ratings or reviews; however, it will be difficult to make use of reputation systems in improving trust in online dating platforms. This is because, to use reputation systems in online dating services, a series of questions arises, such as, Should reputation be built on how good a date a person is? How romantic a dating experience was? How long the person has been on the site? Mostly, if an individual gets positively rated based on these, then ideally such persons will no longer be using the dating service and their profiles should be unavailable. As such, the reputation built has no benefit to potential daters. For instance, if an individual has a high reputation based on high amount of dates had, the inherent question then is, "why is the individual still on the dating site?"; if otherwise, the question becomes, "why is no one going on date with the individual?" Also, there is currently no way to know if a date occurs between dating sites users, as is seen in other CMIs such as Uber and Airbnb. This is because dating sites have no record of when or if users go on dates as well as the location of the dates.

In other computer mediated communications also, reputation is usually built based on the quality of the service an individual provides. In online dating, the service provided is the 'dating' itself, and if the service is well provided, the chances of the person still being on the dating site is low. Dating site users also cannot rate their dating experiences with another individual, as an ideal dating experience for one person varies for another, and if a date is good the individual ideally should no longer be on the platform and as such cannot be rated. It will also be difficult to build reputation without bias on dating sites in the event that a potential date does not go as planned.

Dating sites attempt to employ stories of successfully matched couples as a form of feedback reputation mechanism, but usually there is no incentive to come back to the site to leave a story. Also, unlike conventional computer mediated interaction, leaving a review on goods bought or services offered is done so that others can purchase those same goods from the individual. In dating sites, those services cannot be acquired from that individual at that point in time. The ultimate problem then in using reputation systems on dating sites is that the services dating sites offer are distinct

	MATCH.COM	PLENTY OF FISH	TINDER
VERIFICATION STRATEGIES	N	N	Y
PRIVACY	N	N	N
BACKGROUND/SECURITY CHECKS	N	N	N
SECURED MESSAGING PLATFORM	Y	Y	Y
REVIEWS/REFERENCES/FEEDBACKS	N	N	N
RATING SYSTEM	N	N	N
LINKING TO SOCIAL MEDIA	Y	Y	Y
SAFETY TIPS	Y	Y	Y
FLAGGING/REPORT ABUSE	N	N	N
BLOCKING OF MEMBERS	Y	Y	Y
24/7 CUSTOMER SUPPORT	N	Y	Y

Figure 6.1: Table Showing Comparison of Trust Mechanisms Used By Other CMIs With Dating Sites

and specific to individuals, whereby once successfully given to an individual from one user, they cannot be offered to another by that same user.

Also, the use of pictures, as a form of multimedia-based trust, may be of help in some CMCs, however it becomes a tricker means of establishing trust in CMIs as a whole, and more so in dating sites. As seen in the user study results presented in Chapter 5, pictures tend to confuse dating sites users, with some users identifying attractive pictures as a sign of deception; in other contexts, more attractive pictures increases trust [168]. Other dating site research shows that men frowning and women smiling were cited as trustworthy signs [24].

6.6 Analysis of Results

Based on the above evaluation, the model in Figure 6.2 shows the relationship among the reality of dating sites, the risks involved and mitigation strategies used to address those risks.

The model is structured in three categories similar to the model developed from the user study in Chapter 6.

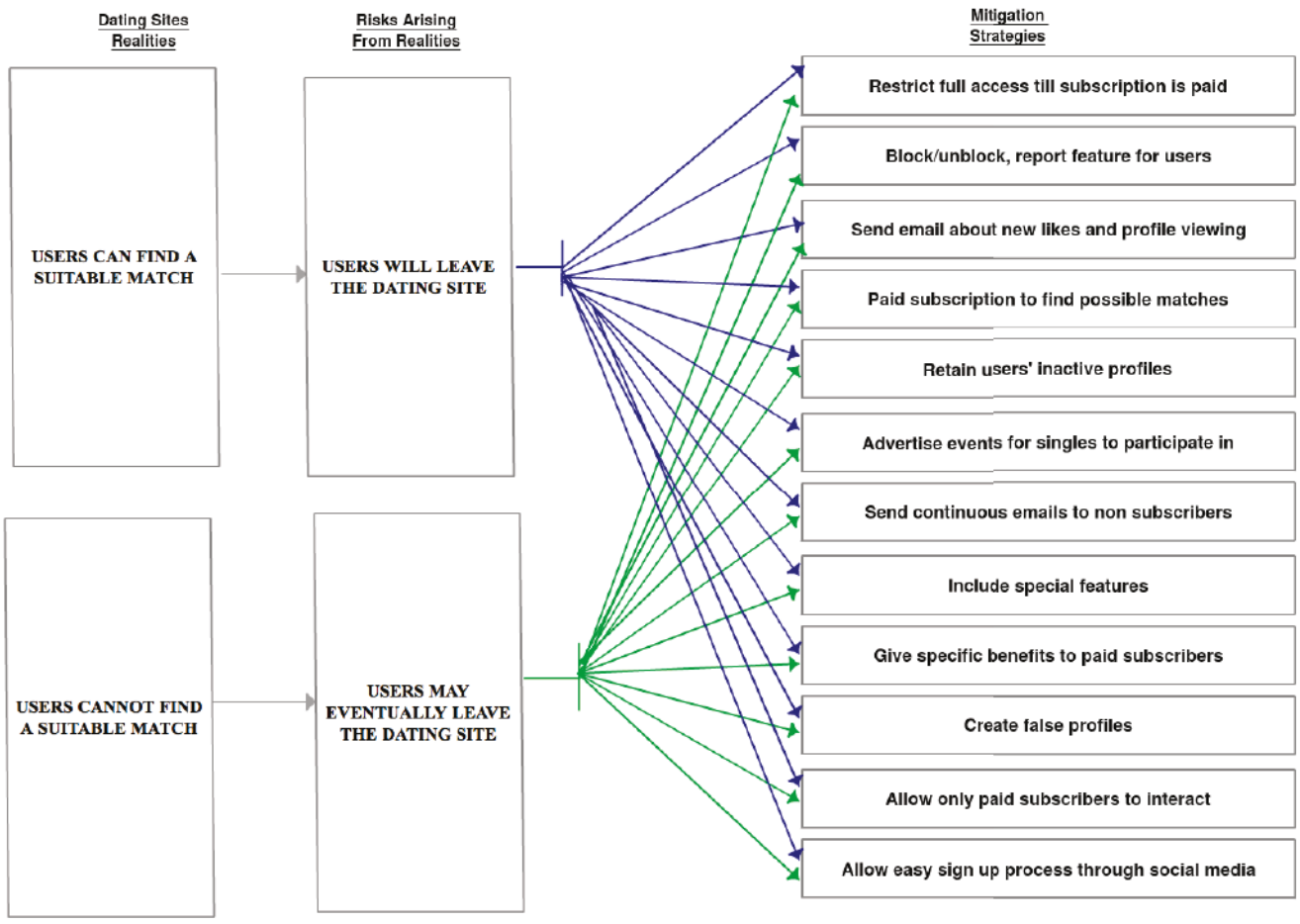

Figure 6.2: Model showing dating sites realities, risks and mitigation strategies

1. **Dating Sites Realities:** This showcases the realities faced by dating sites.
2. **Risks Arising From Realties:** This describes the possible risks dating sites are susceptible to as a result of the facts and realities identified.
3. **Mitigation Strategies:** This refers to the various methods dating sites have implemented to protect themselves from the risk associated with the corresponding reality.

6.7 Discussion

In comparing the models developed in Figure 5.3 and Figure 6.2, it should be noted that the focus of online dating sites may be said to differ significantly from those of their users. Some dating sites users make use of the platform to flirt and do not have plans to meet up with those they interact with on the platform. Other dating site users focus on getting potential matches they could interact with offline. However as seen in Chapter 5, no matter the users' reasons for making use of dating sites, users continuously seek ways to balance their privacy and security while using the platforms. Dating sites on the other hand are faced with the risks of losing users and therefore employ strategies to retain current users and acquire new ones. For example, the use of false profiles to retain users can be seen in the Ashley Madison dating platform. The Ashley Madison dating site was hacked in 2015 [114], which led to the release of information on members of the sites as well as false profiles [151, 216]. The difference in focus may be a major issue in dating sites establishing trust and ensuring the security of users.

Table 6.2 summarizes the comparisons between Irene's ideal roles specified in Chapter 4 and the roles currently played by the dating sites surveyed, while Table 6.1 summarizes the key mechanisms the surveyed dating sites use to establish trust between potential matches. What is remarkable about Table 6.1 is that *none* of the mechanisms are robust against a malicious adversary. Anyone reading a dating profile asks themselves, "Is this really who they are? Are they leaving out important details? Are they outright lying? Are those pictures even real?" These are basic questions that we constantly ask when we meet someone new. In person we can look a person in the eye in order to assess their intentions. While con artists and actors

can imitate sincerity, in-person cues are generally solid mechanisms for establishing trust.

In contrast, every trust signal presented by dating sites can be easily manufactured. Social media accounts can be faked. Time of login can be faked. A complete profile can be faked. A blocked user can create a new account and attempt contact again. None of these signals represent a significant impediment to parties who wish to misrepresent themselves. Today, then, it is unwise for individuals to go into a first in-person meeting with a significant level of trust if their only previous interaction has been through an online dating site. Having a friend sitting at the bar watching the progress of your date may in fact be a good idea.

But can we do better?

Chapter 7

Developing Security Mechanisms for Online Dating

Trust matters in online dating in part because of the high stakes involved in meeting a stranger in person one on one for such an intimate purpose. However, trust is also a vital issue because people generally prefer to be somewhat anonymous when meeting strangers. When interacting in public spaces, strangers will generally not exchange names or contact information until they both feel comfortable with each other. Similarly, users of online dating sites use pseudonyms and conceal contact information until they sense some degree of trust has been established.

Unfortunately, the protection provided by anonymity is also a danger because it allows malicious actors to conceal themselves as well. Various instances have been recorded of users' privacy being violated as well as users experiencing violence, sexual assault, cyberbullying, physical stalking, workplace harassment, monetary fraud, sex trafficking and, even worse, death, as a result of using online dating services [103, 245, 127, 96, 8, 40, 231]. Most of these incidents go unreported or unknown due to the stigma attached to such disclosure [233, 134, 123, 165, 22]. Data breaches also occur in dating sites, with previous incidents leading to the disclosure of those with HIV or sexually transmitted infections [269, 21, 212]. Sensitive past messages as well as the accurate geolocation of dating sites users have also been released [79, 205]. While safety concerns could in principle cause individuals to obfuscate or outright lie in their online profiles and interactions, in practice this is often not the case. Online daters are relatively truthful about their physical attributes [106], and they tend to reveal a significant amount of personal information—enough to potentially make them susceptible to scammers [169]. Indeed, people are sometimes traumatized by their experiences with online dating. Sometimes the trauma comes from going on "bad dates," or from ending up in abusive relationships. However, individuals are also traumatized by being outright scammed [277]. Online dating scams can result in financial losses for victims and forms of blackmail such as sextortion [69].

Sometimes these scams aren't even conducted directly by humans. Instead, chatbots can deceive individuals into disclosing enough sensitive information that an attack can be mounted [115]. As stated by Norcie et al., "because of the inherent need to engage with and reveal potentially sensitive information to unknown others, dating sites amplify many of the traditional social-networking security and privacy issues" [190].

The results of the user study in Chapter 5 show that users essentially do not know how to protect themselves, whereby online daters go often into initial meetings with significant amounts of distrust. To compensate, they engage in a variety of risk mitigation strategies such as online searches, staying in contact with friends electronically during a date, and having third parties quietly observe the date from a distance so they can step in if anything goes wrong. Dating sites also do not provide alternatives to the subtle interaction of verbal and body language cues that can help people detect deception and aggression in face-to-face interactions. As seen in the model presented in Chapters 5 and 6, while users aim at balancing security and privacy, this is not necessarily the goal of dating sites. Dating sites themselves do not employ sufficient strategies to safeguard users. While standard trust mechanisms exist for other computer mediated communications, some of these mechanisms cannot be effectively applied in online dating sites. There are however a number of ways dating sites can improve the level of trust potential matches have in each other. We discuss these below in terms of what can be done in three phases: before the match, during the match, and afterwards.

The rest of the chapter is divided into three parts. We first discuss alternative trust mechanisms that can be employed by online dating sites, before, during and after a match has been formed. In the second part we discuss the evaluation of the suggested trust mechanisms and summarize in the third part.

7.1 Alternative Trust Mechanims

7.1.1 Before the Match

Dating sites could take steps to not just recommend users, but actually verify the users they recommend. The use of general email addresses as a single identifier of

a person, should be discouraged. Making use of other forms of verification of the identity of people should be looked into. Couchsurfing [44] verifies their users by verification of their payment method, phone number, address and government ID. These steps could be taken by dating sites to ensure people are better identified. The users do not need to know the true identity of who they are interacting with, unless the person chooses to reveal themselves. However, the dating site should be able to adequately vouch for the person's identity.

The dating sites can also be structured such that to further verify people, they request them to take selfies with a mobile version of the dating site. These selfies can then be compared with the uploaded pictures on the site. The selfies do not have to be placed as profile pictures; they only need to be seen by dating sites administrators (or their automated proxies) for verification purposes. By requiring the capturing of a live image, it makes it much harder for an adversary to misrepresent their appearance.

While Tinder employs Facebook as a verification method, it does not absolutely protect users as fake Facebook profiles can be easily created. Dating site users will most times prefer to remain anonymous, so using Facebook accounts to get a profile picture and profile defeats the whole purpose of anonymity on dating sites. If a user decides to block another on a dating site, the blocked user can find the user on Facebook, which could have the same picture used on Twitter, LinkedIn, and other social media accounts. Therefore, making users sign up with their Facebook name and profile may cause people to create fake Facebook accounts instead for perfectly legitimate reasons. However, having the site anonymously properly verify these accounts would go a long way in solving the problem of fake accounts and reduce the ease at which people can commit crimes and change their identity.

On the issue of fake profiles, Ambler in an article addressed the problem by listing possible steps that could easily weed out fake profiles on dating sites; however, he suspected that these profiles are instead left on the sites for profit making purposes [9]. We implore dating sites to improve the filtering of fake profiles, by using readily available algorithms and monitoring of users' activities, in order to improve trust on these platforms [9].

If verification features cannot be applied to the free version of dating sites, then they should be applied to the paid or upgraded versions. At the moment, paid

versions of dating sites put the paid users at the top of searches, thereby increasing their exposure to fraudsters. Paid versions of dating sites could instead ensure users interact with only verified members while also being verified by the means outlined above. Though this may not completely eliminate the creeps or con artists, it will go a long way in reducing their activities on dating sites.

People on dating sites should also be clearly able to differentiate between verified and non-verified members. Match.com writes about a verified badge, but it is unknown what it looks like or which members have been verified. Verified badges should also be for everyone who requests and possibly pays for it, not just for celebrities as in the case of Tinder.

Tinder also tries to build reputation by putting a number next to a Facebook friend. The first number means "you and your match are both friends with this person." The second number to the Facebook friends' picture means that your friend knows someone who knows your last match [251]. While this is a great idea, it should be applied specifically on dating sites, if possible, and not through Facebook, because, as previously discussed, the use of Facebook as a means of verification on dating sites should be discouraged.

A "Rate the Interaction" field could be introduced on dating sites whereby early on in a conversation with someone, a user is presented with the option to rate an interaction, based on the speed at which the person replies messages, the tone of conversations, use of words, and the overall quality of the interaction. To avoid biased rating, the rating should be gathered during the early stages of a matched pair's interactions so the rating is of the initial interaction rather than the quality of an ongoing relationship. Such ratings would help users filter out those who are rude or otherwise obviously antisocial.

7.1.2 During the Match

Dating sites should make use of more user friendly messaging interfaces that encourage users to remain on the platform and continue their conversations on-site. As in the case of Match.com and POF, while their mobile versions do a reasonable job, it is harder to have a conversation with a match using the web interface. Any such difficulties assist con artists when they encourage targets to move their conversations

to other messaging platforms.

"Safety" links with tips on dating site guidelines and safety measures should be made more visible to users. If users do not know such links exist they would not be able to read them and better protect themselves.

In the event that dating sites users are open to the idea of having selected friends know that they are making use of dating sites, potentially peer-group evaluation of profiles could be implemented. The dating site could be structured such that at users' request, their selected friends can be able to access part of their conversations with a match and the match's profile. Since dating sites users can be emotionally vulnerable, their friends can help them decide if they think they should meet offline with a match or not.

Also, as text-based chatting has been identified as having major issues in developing trust in humans [28], other methods of communication should therefore be supported. The dating sites could offer 3 communication steps to users as a way to better verify their dates before meet up. Step 1 could involve text based chats, Step 2 could involve voice based communication with the match for a duration of time, and Step 3 could involve a limited-time video conversation.

7.1.3 After the Match

This step is the core of CMI that differentiates it from other CMC. If proper precautionary measures are taken before and during the period a match is formed, then making use of this step may not be necessary.

One method that could be looked into by dating sites to ensure the security of users on dates is to employ the use of something like the Uber panic button mechanism. Uber panic button option exists for Uber users in India. Once this button is pressed on the app, an incident response team is triggered and the police are alerted immediately. Details about the trip are also immediately sent to those being contacted [204]. Although this may raise some privacy concerns, a similar feature could potentially be applied on dating sites to further protect their users.

7.1.4 Evaluating Security Mechanisms for Online Dating

As with other security mechanisms, it will be important to evaluate whether any new mechanism actually improves the security of online dating. The most straightforward evaluation strategy would be to gather feedback from users after they meet with a match offline. However, as previously stated, getting feedback from dating sites users can be difficult because of the type of interaction that occurs on the platform.

In other CMI interactions, such as Airbnb, guests and hosts give feedback because they have incentives to do so: hosts want to attract more guests, and guests want to be appealing to hosts so they can stay where they want for a reasonable price. These same incentives do not hold on dating sites. Indeed, the goal of most users of dating sites is to stop using them—once they've found someone to date!

Ideally, dating sites would need feedback from users once they meet in person so that patterns of misrepresentation or fraud can be addressed. We are yet to identify effective means through which adequate feedback can be acquired from users as soon as an offline interaction occurs. Periodically, dating sites could engage researchers to carry out user studies in order to find out the effectiveness of the suggested trust mechanisms. The cost, challenge of scale, and invasiveness of any such study, however, make such research extremely challenging. To make more secure platforms for CMI, however, we will need to address these challenges.

7.2 Summary

In this chapter, we reviewed strategies that can be applied on dating sites to improve trust and security in their services. We itemized mechanisms that could be employed, before, during and after a match. We also discussed the evaluation of the suggested strategies.

Chapter 8

Discussion

This chapter is divided into four parts. In the first part we discuss the main contributions of this research to computer security. We discuss the limitations and future work in the second and third parts respectively. We give some concluding remarks in the fourth part.

8.1 Contributions

Our main contribution is the identification of Computer Mediated Introductions (CMI) as an area of potential study in computer security. We grouped CMI into business and personal CMIs, based on the presence or absence of monetary exchange. CMI identifies a separate niche of online communications that has not been previously identified in computer mediated communications. We place our focus on the importance of trust on these platforms because these online CMI interactions eventually lead to offline communications. To that aim, in Section 3, we present an in-depth analysis of the trust mechanisms implemented by seven CMIs. We critically analyzed these mechanisms and suggest alternative methods of implementation that will safeguard users. While recognizing the unique type of interactions that occur on a specific type of personal CMI, online dating sites, we designed and evaluated the threat model of dating sites in Section 4. We identified the possible threats that could occur, throwing more light on the importance of the development of effective trust mechanisms in this type of communications.

In Section 5, we presented results from a user study to find out if users are aware of the possible threats and to identify the mechanisms they implement to protect their safety when using dating sites. We did a qualitative analysis of the results and carried out an evaluation in Section 5.2. Results showed that users had insufficient strategies to protect themselves from the identified threats and were quite vulnerable to attacks by dangerous others. We discussed this in Section 5.3, acknowledging that

the emotional vulnerability of dating sites users can be easily exploited, making them susceptible to attacks. We concluded that dating sites are therefore tasked with the responsibility of protecting users as users are not doing a good job of it.

In Section 6, we carried out a study of the current mechanisms implemented by dating sites to protect their users. We compared these strategies to the ideal roles discussed in the threat model in Section 6.4. We discovered that dating sites do next to nothing to effectively protect their users. In Section 6.5, we compared the current trust mechanisms with those being applied in other CMCs, and established that the nature of the interactions that occur on dating sites makes it difficult for conventional trust mechanisms to be applied to this type of CMI; thereby, we established it as an independent research area.

We suggested possible mechanisms that could be implemented to dating sites in Section 7 and encouraged the research community to carry out more research into how trust can further be developed and maintained in CMIs that are heavily dependent on humans' emotional exchange.

8.2 Limitations

In evaluating the problem of trust in CMI, we studied the trust mechanisms implemented by CMI platforms and the users of the platforms. The trust mechanisms used by the platforms refer to various techniques, methods, and features that are implemented by the sites in order to build trust in their users and improve safety both offline and online. The mechanisms implemented by users refer to the strategies employed by users in determining who to trust online, and eventually meet up with offline. There are however limitations in the approaches used in our study. In the next section, we identify these limitations and we also comment on problems we feel are inevitable when carrying out research such as this.

8.2.1 Limitations In Our Approach

Research Methods

The research methods used to identify trust mechanisms applied by CMIs may have limited the authenticity, scope, and depth of the findings made. The trust mechanisms

discussed in the thesis were identified primarily through evaluation of the various CMIs. This involved the researcher creating an account on the CMI platform and surveying the sites' services and features. Thus, the trust strategies identified were largely dependent on the researcher's point of view. This may have led to some false claims and false conclusions, as there was no study conducted to find out if these were the actual mechanisms that built trust for users. Also, experiments were not performed to discover if these were the trust mechanisms users used in deciding who to interact with. As such, there is need to verify the trust strategies identified in the thesis.

An alternative method which could potentially have improved the results would involve carrying out user studies. The user studies would aim to identify specific features and techniques implemented by the CMIs that act as positive cues which help users trust in the credibility of those they choose to interact with, both online and offline. This may further assist in better identifying mechanisms that have been implemented by the platform which breed confidence, trust, and a sense of safety in users. It could also aid in determining if there are other online cues we failed to observe. This type of user study can be structured such that the researcher studies participants in a one-on-one or group setting, to observe how they choose who to communicate with on the CMI platforms. Discussions on the choices made can be carried out with users afterward. However, it should be noted that this type of study may not necessarily produce better results, as participants are aware of being watched. As such, participants may opt for choices they will not necessarily consider in real life. Also in comparison with real CMI interactions, the duration used to carry out such a study may not be sufficient for users to decide who they will normally trust. In CMI communications, users search for those to interact with and in some cases, establish a significant relationship with such people, before deciding to trust them and eventually take the conversation offline. Therefore, determining who to trust online, may take much more time than the user study can accommodate. Hence carrying out such research in this setting may not produce better results.

Optionally, researchers could ask past and current users of those platforms to recall features on the sites that helped them trust that they are being introduced to credible people. Such information could be gathered offline or online through

surveys. In the surveys, participants can be asked to identify ways they choose those to trust based on the site's features. Carrying out the research online could involve conducting surveys using web services such as Amazon's Mechanical Turk. However, online surveys have been known to produce false results. Having the research done offline could involve conducting interviews with such users. This may produce better results than the online research, however there may be the problem of users identifying specific features on the platform that helped them better trust those they interacted with. Also, there are typically far fewer participants in offline interviews, and so results could be limited or skewed.

Alternatively, the researcher could decide to recruit people to use the CMI services for at least a month. Such participants will be given incentives to use the platform. This form of study may also help determine the viability of the trust mechanisms used by the CMI platforms. Ideally, participants will document their experiences, highlighting features of the site that motivated them to trust individuals they communicated with. However, there is the problem of finding the right incentives to encourage participants to use the services for the specified duration of time, in which they will be expected to interact and make use of the site's features. It may also be difficult to verify if users are being sincere in their choices, or if the choices are being made in a bid to finish up with the research. This approach may also act as a form of deceit to legitimate users, as participants will be interacting on the platform not because they are interested in making use of the services being offered, but for research purposes. For example, in an Airbnb listing, participants may engage in interactions with a host, not necessarily because they have any intent of booking the host's services, but to gain information from the host that will help them determine if to trust the host or not. Ultimately, CMI communications are successful only after interactions occur offline. Therefore, further research could involve participants meeting up with people they feel they trust online on these platforms, in order to determine the credibility of the trust mechanisms used. Such meet ups may be endangering participants' safety.

Another approach that could be considered is contacting the CMI platforms to discuss mechanisms they have implemented in other to build trust in users, and ensure users are protected both offline and online. Enquiring from these platforms directly,

possibly through interviews, could have improved the accuracy of the results obtained in the thesis. These communications may lead to clarifications that could aid better understanding of the problems CMIs face in effectively building trust in users. It may also help in effective analysis of current trust mechanisms being implemented by the platforms, as well as in discussing strategies that may have been previously employed, but were unsuccessful in building trust and keeping users safe. The platforms may also be able to help identify reasons for failure and discuss future work being put in place to safeguard users. It will also help understand why some suggested trust strategies are yet to be implemented on the platform. Also, better statistics on the number of failed and successful introductions carried out by the platforms may have been obtained through direct contact with the CMIs. This will aid the assessment of the functionality of the trust mechanisms employed.

A major limitation to this approach however is getting in touch with the platforms to discuss the methods they have implemented. Such interviews may inevitably lead to the platforms having to admit a certain level of users' privacy breach as well as safety and trust issues on the sites, which the platforms may not be willing to admit.

User Study of Dating Sites

On the issue of trust in dating sites, while we analyzed the trust mechanisms dating sites employed to keep users safe, we also studied the mechanisms users employed in trusting others on the platform. Ten participants were involved in the user study done to evaluate users' trust strategies. Though the user study accounted for a wide age range (18-50 years), an increase in the number of participants may have resulted in a more extensive user study. Also, participants were recruited solely from the university. Having participants from other segments of the society could have potentially improved the results. Better results may have also been obtained if participants had been grouped based on their computer literacy skills. Essentially, all these may have assisted in finding out if dating sites' users carry out other approaches at establishing trust and serve as means for better evaluation and analysis of the trust strategies.

Reputation Systems in Online Dating Sites

As discussed in Section 6.5, the inability to effectively make use of reputation systems in dating sites is a major limitation. Though user studies can be attempted to evaluate the success of current trust mechanisms, for better results, an evaluation of the interaction, both offline and online, needs to be done. Ideally, after dates occur, the success of the trust mechanisms implemented by dating sites should be evaluated through reviews, ratings, and feedback, as seen in other CMI platforms. This is however difficult to implement because of the nature of the services provided by dating sites. Dating sites users move off the platform once an introduction is successful and biased feedback may be obtained from users once an introduction is unsuccessful (see Section 6.5 for a detailed explanation of the problem of trust evaluation in dating sites). Hence, it will also be difficult to evaluate the trust mechanisms suggested in the thesis, on dating sites' users.

8.3 Future Work

We believe our approach in helping to formalize and study the problem of trust is a starting point in improving trust and ultimately security in CMI. We discuss below, future work that can be done to help improve trust in this type of interactions.

8.3.1 Suggestions For Future Work

Contacting CMI Platforms

We suggest that CMI platforms be contacted directly for interviews, in a bid to better understand the trust mechanisms currently being implemented on the platforms. Though this may be difficult to do, it may be required to understand and properly address the problems CMIs face in developing trust. In carrying out such research, work has to be done in finding out ways in which CMIs will avoid compromising their integrity, but at the same time provide adequate information that will help improve trust and security on the platforms.

In dating sites particularly, we realize that the sites typically engage in trust strategies that will be economically feasible even though they are being implemented at the risk of users' safety. Human matchmakers, who also provide services similar

to dating sites, provide better secured and private services for their users, however they are not scalable in terms of cost. We hope to be able to discuss this problem with dating sites and assist in finding a balance so as to ensure user's security is not sacrificed in any way.

Implementing Alternative Trust Mechanisms

We hope to work with CMI platforms to implement the alternative trust mechanisms suggested in the thesis. We realize that evaluating the potency of these trust mechanisms may be difficult to do in dating sites; however, the mechanisms can be evaluated by other CMI platforms to determine if they better improve trust and security on those sites.

Developing an Alternative Reputation System

Research needs to be done to find out how adequate evaluation and feedback can be acquired in computer mediated interactions that involve human emotional exchange, as seen in dating sites. Since standard reputation systems do not work on dating sites, alternative methods on how reviews can effectively be obtained from dating sites' users should be looked into. Such a reputation system will be built differently from conventional reputation systems seen in other CMIs. The ultimate goal of the reputation system will be to determine if the trust mechanisms used by the site is sufficient or if better ones need to be developed. The reputation system should be able to effectively get feedback from users as online interactions take place and immediately after offline dates or interaction occurs. The reputation system should be developed such that there is no avenue for any form of biased feedback, review or rating from the users of the systems. Users should also have some form of incentives to make use of the reputation system. Incentives could include things like restaurant coupons that users can use on their next dates with their current successful match, or their next match from the site.

Tracking of CMI Users

As seen in Uber, other CMI platforms could have a means of tracking meetups involving people that have been introduced on their site. This will involve the CMI

platforms being aware of when users agree to meet offline, as well as when and where the meeting will be taking place. The CMI platforms should also have an effective means of determining if the meetup actually does take place. This will involve the site having some form of schedules that are regularly being updated. For example, in dating sites, when dates occur between users that have been introduced by the platforms, the dating site should know the exact location of the dates and the time when the dates happen. The dating site platform should be able to track in real time where both individuals are at any point in time during the meet up. If there is any variation from the original schedule, the CMI platform should be very aware of this. However, such tracking should only occur when both individuals meet up and should be turned off once the meet up is completed.

Implementing 'Danger Alert' Icon on CMIs

All CMI platforms could look into implementing a *Danger Alert* icon that could be used by people during offline meetings. This icon could work similar to the panic buttons being used by Uber users in India [204]. The icons could be some form of software or application that should be able to work offline. They should function such that, once people sense any form of danger, the icon can be pressed and the local authorities are contacted immediately. This could potentially improve the trust and security of users on CMI platforms.

Analyzing Conversations

Future work could also involve identifying means by which CMIs can be able to determine when users are in danger online and act accordingly, by effectively analyzing the conversations the users have on the platform. These conversations should be analyzed in real time. If the CMI platform notices a conversation is not going as should be, they could ask the users if they are comfortable with the conversation or if they would prefer to end communications with the user. If users opt for ending communications, the platform should carry this out with immediate effect, such that no form of contact is possible between both users, except if requested.

Using Cryptography For Verification

CMI platforms could consider using cryptographic methods to verify the identity of people using the sites. This could involve the use of some form of token key between users to verify the identity of people engaged in interactions carried out on the platform. This could lead to having unique individuals on these platforms, and may solve the problem of having multiple profiles for the same individuals. When people know that the users they are interacting with are real people with a real identity, this may ultimately increase trust in the sites.

Balance Security and Privacy in CMIs

We recognize that while the suggested mechanisms above may be able to improve trust and security in CMIs, they may however result in the privacy of users being compromised. Future work therefore will include developing methods of improving trust on these platforms, but at the same time effectively balancing users' security and privacy.

8.4 Conclusion

Rheingold rightly stated that, "computer mediated communications provide new ways to fool people" [219]. Computer mediated introductions (CMI) introduce strangers online and bring them together offline. In this thesis, we identified CMI as an understudied area of computer security. We evaluated the trust mechanisms implemented by CMIs, and further identified that Personal CMIs, specifically dating sites, are not adequately served by standard security practices such as cryptographic authentication and ratings-based reputation systems. We explain why current trust mechanisms are not sufficient in improving the safety and security of users. We also suggest alternative mechanisms that could be employed to improve trust in CMIs. We hope this work will encourage others to further study this problem through user studies and the development of technical mechanisms specialized to the CMI problem.

Bibliography

[1] Airbnb. Airbnb about us. https://www.airbnb.ca/about/about-us/, 2017. Online; Accessed: 2017-07-25.

[2] Airbnb. Airbnb home page. https://www.airbnb.ca/, 2017. Online; Accessed: 2017-07-25.

[3] Airbnb. Airbnb levels. https://community.withairbnb.com/t5/Hosting/quot-Levels-quot/m-p/942#M92/, 2017. Online; Accessed: 2017-07-25.

[4] Airbnb. Airbnb privacy policy. https://www.airbnb.ca/terms/privacy_policy?locale=en/, 2017. Online; Accessed: 2017-07-25.

[5] Airbnb. Airbnb superhost. https://www.airbnb.ca/superhost/, 2017. Online; Accessed: 2017-07-25.

[6] Airbnb. Apartment booking. https://www.airbnb.ca/rooms/8629737?s=fRfyD4Tf#host-profile/, 2017. Online; Accessed: 2017-07-25.

[7] Airbnb. How does airbnb help build trust between hosts and guests? https://www.airbnb.ca/help/article/4/how-does-airbnb-help-build-trust-between-hosts-and-guests/, 2017. Online; Accessed: 2017-07-25.

[8] Richard Alleyne. Personal trainer raped, beat and robbed secretary he met on dating website. http://abcnews.go.com/US/woman-sues-match-date-attacks/story?id=18314916/, 2012. Online; Accessed: 2017-07-25.

[9] Christopher Ambler. Match.com's fake problem. https://www.linkedin.com/pulse/matchcoms-fake-problem-christopher-ambler/, 2016. Online; Accessed: 2017-07-25.

[10] Traci Anderson and Tara Emmers-Sommer. Predictors of relationship satisfaction in online romantic relationships. *Communication Studies*, 57(2):153–172, 2006.

[11] Erin Anderssen. You deleted your dating profile. is it really gone? https://www.theglobeandmail.com/life/the-hot-button/you-deleted-your-dating-profile-is-it-really-gone/article615323/, 2011. Online; Accessed: 2017-07-11.

[12] Joanne Arciuli, David Mallard, and Gina Villar. "Um, i can tell you're lying": Linguistic markers of deception versus truth-telling in speech. *Applied Psycholinguistics*, 31(3):397–411, 2010.

[13] Michael Arrington. Airbnb victim speaks again: Homeless, scared and angry. https://techcrunch.com/2011/07/29/airbnb-victim-speaks-again-homeless-scared-and-angry/, 2011. Online; Accessed: 2017-07-25.

[14] Michael Arrington. Another airbnb victim tells his story: "there were meth pipes everywhere". https://techcrunch.com/2011/07/31/another-airbnb-victim-tells-his-story-there-were-meth-pipes-everywhere/, 2011. Online; Accessed: 2017-07-25.

[15] Ira Asherman, John W Bing, and Lionel Laroche. Building trust across cultural boundaries. *Regulatory Affairs Focus*, 5:6–16, 2000.

[16] Michael Bacharach and Diego Gambetta. Trust as type detection. In *:Castelfranchi C., Tan YH. (eds) Trust and Deception in Virtual Societies. Springer, Dordrecht*, pages 1–26. Springer, 2001.

[17] Joan C Bachenko and Michael J Schonwetter. Method and system for the automatic recognition of deceptive language. *Google Patents*, (EP Patent App. EP 20,050,858,583, US Patent 7,853,445), 2010.

[18] Annette Baier. Trust and antitrust. *Ethics, University of Chicago Press*, 96(2):231–260, 1986.

[19] Preet Banerjee. Why i won't be using airbnb's online verification system. https://www.theglobeandmail.com/globe-investor/personal-finance/household-finances/why-i-wont-be-using-airbnbs-new-online-verification-system/article19290229/, 2017. Online; Accessed: 2017-07-25.

[20] Abigail Barthel and Courtney Aydt. The effects of sexualized facebook profile pictures on ratings of physical attractiveness and task competence. *Undergraduate Journal of Psychology, The University of Minnesota*, 2016.

[21] BBC. Positivesingle's STD dating site faces $16.5m penalty. http://www.bbc.com/news/technology-29912279/, 2014. Online; Accessed: 2017-07-25.

[22] Martin Beckford. 80% of women don't report rape or sexual assault, survey claims. http://www.telegraph.co.uk/news/uknews/crime/9134799/Sexual-assault-survey-80-of-women-dont-report-rape-or-sexual-assault-survey-claims.html/, 2012. Online; Accessed: 2017-07-25.

[23] Sharyn Beech. Why sleeping with my couch surfing host was a huge mistake. http://www.nerve.com/love-sex/true-stories/why-sleeping-with-my-couch-surfing-host-was-a-huge-mistake/, 2014. Online; Accessed: 2017-07-25.

[24] Katharine Blodget. Why you shouldn't smile in your match.com profile, and other online dating tips for execs. `http://www.businessinsider.com/data-driven-online-dating-tips-for-execs-2011-4/`, 2011. Online; Accessed: 2017-07-25.

[25] Eric Bonabeau. Don't trust your gut. *Harvard Business Review*, 81(5):116–23, 2003.

[26] Gary D Bond and Adrienne Y Lee. Language of lies in prison: Linguistic classification of prisoners' truthful and deceptive natural language. *Applied Cognitive Psychology*, 19(3):313–329, 2005.

[27] Prashant Bordia. Face-to-face versus computer-mediated communication: A synthesis of the experimental literature. *The Journal of Business Communication (1973)*, 34(1):99–118, 1997.

[28] Nathan Bos, Judy Olson, Darren Gergle, Gary Olson, and Zach Wright. Effects of four computer-mediated communications channels on trust development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '02, pages 135–140, New York, NY, USA, 2002. ACM.

[29] Megan Bostic. 18 honest lessons about online dating from someone who has been there. `http://thoughtcatalog.com/megan-bostic/2015/12/18-honest-lessons-about-online-dating-from-someone-who-has-been-there/`, 2015. Online; Accessed: 2017-06-30.

[30] Josh Boyd. In community we trust: Online security communication at ebay. *Journal of Computer-Mediated Communication*, 7(3):0–0, 2002.

[31] Robert J Brym and Rhonda L Lenton. Love online: A report on digital dating in canada. *MSN.ca*, 6, 2001.

[32] David B Buller, Judee K Burgoon, JA Daly, and JM Wiemann. Deception: Strategic and nonstrategic communication. *Strategic Interpersonal Communication*, pages 191–223, 1994.

[33] Judee Burgoon and David Buller. Interpersonal deception theory: Purposive and interdependent behavior during deceptive interpersonal interactions. *Engaging theories in interpersonal communication, Sage Publications Los Angeles, CA*, pages 349–362, 2015.

[34] John K Butler Jr. Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. *Journal of management, Sage Publications Sage CA: Thousand Oaks, CA*, 17(3):643–663, 1991.

[35] Billie E Cali, Jill M Coleman, and Catherine Campbell. Stranger danger? Women's self-protection intent and the continuing stigma of online dating. *Cyberpsychology, Behavior, and Social Networking*, 16(12):853–857, 2013.

[36] GW Carpenter. *Imagine me and you: A mixed methods investigation of imagined interactions in online dating.* PhD thesis, The University of Alabama, 2016.

[37] Elisabetta Carrara and Giles Hogben. Reputation-based systems: A security analysis. *European Union Agency for Network and Information Security (ENISA) Position Paper*, 424, 2007.

[38] Cristiano Castelfranchi and Rino Falcone. Trust and control: A dialectic link. *Applied Artificial Intelligence*, 14(8):799–823, 2000.

[39] Bessie Chong, Zhilin Yang, and Michael Wong. Asymmetrical impact of trustworthiness attributes on trust, perceived value and purchase intention: A conceptual framework for cross-cultural study on consumer perception of online auction. In *Proceedings of the 5th International Conference on Electronic commerce*, pages 213–219. ACM, 2003.

[40] Susan Clairmont. Clairmont: Is this rapist trolling for women online? `https://www.thespec.com/news-story/4391497-clairmont-is-this-rapist-trolling-for-women-online-/`, 2014. Online; Accessed: 2017-07-25.

[41] Camille Cobb and Tadayoshi Kohno. How public is my private life?: Privacy in online dating. In *Proceedings of the 26th International Conference on World Wide Web*, pages 1231–1240. International World Wide Web Conferences Steering Committee, 2017.

[42] Cynthia L Corritore, Beverly Kracher, and Susan Wiedenbeck. On-line trust: concepts, evolving themes, a model. *International journal of human-computer studies*, 58(6):737–758, 2003.

[43] Danielle Couch, Pranee Liamputtong, and Marian Pitts. What are the real and perceived risks and dangers of online dating? perspectives from online daters: Health risks in the media. *Health, Risk & Society*, 14(7-8):697–714, 2012.

[44] Couchsurfing. Couchsurfing homepage. `https://www.couchsurfing.com/`, 2017. Online; Accessed: 2017-07-25.

[45] Couchsurfing. Couchsurfing policies. `http://www.couchsurfing.com/about/policies/`, 2017. Online; Accessed: 2017-07-25.

[46] Couchsurfing. Couchsurfing safety faq. `http://www.couchsurfing.com/about/faq/`, 2017. Online; Accessed: 2017-07-25.

[47] Couchsurfing. Getting started for new members. `https://support.couchsurfing.org/hc/en-us/articles/214891777-Getting-Started-for-New-Members/`, 2017. Online; Accessed: 2017-07-25.

[48] Couchsurfing. How do i update my hosting availability? https://support.couchsurfing.org/hc/en-us/articles/203844030-How-do-I-update-my-Hosting-Availability-/, 2017. Online; Accessed: 2017-07-25.

[49] Couchsurfing. How to use couchsurfing hangouts. https://support.couchsurfing.org/hc/en-us/articles/221750007-How-to-Use-Couchsurfing-Hangouts/, 2017. Online; Accessed: 2017-07-25.

[50] Couchsurfing. I heard of someone charging for a couch. is that ok? https://support.couchsurfing.org/hc/en-us/articles/200639420-I-heard-of-someone-charging-for-a-couch-Is-that-OK-/, 2017. Online; Accessed: 2017-07-25.

[51] Couchsurfing. Tips to be a great couchsurfer! https://support.couchsurfing.org/hc/en-us/articles/200717684-Tips-to-be-a-Great-Couchsurfer-/, 2017. Online; Accessed: 2017-07-25.

[52] Couchsurfing. Updates to the reference system. https://support.couchsurfing.org/hc/en-us/articles/212679127-Updates-to-the-Reference-System/, 2017. Online; Accessed: 2017-07-25.

[53] Craiglist. Avoiding scams. https://www.craigslist.ca/about/scams/, 2017. Online; Accessed: 2017-07-25.

[54] Craiglist. Craigslist personal safety. https://www.craigslist.ca/about/safety/, 2017. Online; Accessed: 2017-07-25.

[55] Craigslist. All craigslist postings are free, except for:. https://www.craigslist.ca/about/help/posting_fees/, 2017. Online; Accessed: 2017-07-25.

[56] Yao-Hua Tan Cristiano Castelfranchi. The role of trust and deception in virtual societies. *International Journal of Electronic Commerce*, 6(3):55–70, 2002.

[57] B Dambrine, J Jerome, and B Ambrose. User reputation: Building trust and addressing privacy issues in the sharing economy. In *Future of privacy forum*, 2015.

[58] Partha Dasgupta. Trust as a commodity. *Trust: Making and breaking cooperative relations*, 4:49–72, 2000.

[59] Carmel DeAmicis. Here's the problem with the way Uber vets drivers. https://gigaom.com/2014/12/10/heres-the-problem-with-the-way-uber-vets-drivers/, 2017. Online; Accessed: 2017-07-25.

[60] Morton Deutsch. Trust and suspicion. *Journal of conflict resolution*, 2(4):265–279, 1958.

[61] Morton Deutsch. Cooperation and trust: Some theoretical notes. *M. R. Jones (Ed.), Nebraska Symposium on Motivation*, pages 275–319, 1962.

[62] Morton Deutschi. The effect of motivational orientation upon trust and suspicion. *Human relations*, 13(2):123–139, 1960.

[63] Andreas Dieberger, Paul Dourish, Kristina Höök, Paul Resnick, and Alan Wexelblat. Social navigation: Techniques for building more usable systems. *Interactions*, 7(6):36–45, 2000.

[64] Judith S Donath et al. Identity and deception in the virtual community. *Communities in cyberspace*, 1996:29–59, 1999.

[65] Patricia M Doney and Joseph P Cannon. An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing*, pages 35–51, 1997.

[66] Jessica E Donn and Richard C Sherman. Attitudes and practices regarding the formation of romantic relationships on the internet. *CyberPsychology & Behavior*, 5(2):107–123, 2002.

[67] Samuel Dukhovni, Ja Kob Weisblat, and Istvan Chung. Solving the dating problem with the senpai protocol. `http://sigtbd.csail.mit.edu/pubs/veryconference-paper10.pdf/?utm_term=.dc0917fe6ff7/`, 2016. Online; Accessed: 2017-04-14.

[68] Catherine C Eckel and Ragan Petrie. Face value. *The American Economic Review*, 101(4):1497–1513, 2011.

[69] Simon Edmunds. Scammers & online dating fraud: 2015 trends and tactics. `https://scamalytics.com/wp-content/uploads/2015/02/GDI-Scammers-Online-Dating-Fraud-Scamalytics.pdf/`, 2015. Online; Accessed: 2017-04-14.

[70] eHarmony. The most successful online dating profile photos revealed. `http://www.eharmony.com/dating-advice/using-eharmony/the-most-popular-online-dating-profile-photos-revealed/\#.WW0c88YZNbU/`, 2013. Online; Accessed: 2017-06-30.

[71] Paul Ekman and Wallace V Friesen. Nonverbal leakage and clues to deception. *Psychiatry*, 32(1):88–106, 1969.

[72] Paul Ekman, Maureen O'Sullivan, Wallace V Friesen, and Klaus R Scherer. Invited article: Face, voice, and body in detecting deceit. *Journal of nonverbal behavior*, 15(2):125–135, 1991.

[73] Hany Mohamed Hassan El Hoby and Akram M Zeki. Impersonate affecting users' attitude toward facebook in egypt. In *Advanced Computer Science Applications and Technologies (ACSAT), 2015 4th International Conference on*, pages 45–49. IEEE, 2015.

[74] Nicole Ellison, Rebecca Heino, and Jennifer Gibbs. Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication*, 11(2):415–441, 2006.

[75] Emma. What does the "experience" section on my couchsurfing profile show? `https://support.couchsurfing.org/hc/en-us/articles/216359187-What-does-the-Experience-section-on-my-Couchsurfing-Profile-Show-/`, 2017. Online; Accessed: 2017-07-25.

[76] Ernie. Deplorable customer service from airbnb. slow, unresponsive and unprofessional. `https://community.withairbnb.com/t5/Hosting/Deplorable-customer-service-from-Airbnb-Slow-unresponsive-and/m-p/191665/`, 2015. Online; Accessed: 2017-07-25.

[77] Eyal Ert, Aliza Fleischer, and Nathan Magen. Trust and reputation in the sharing economy: The role of personal photos in airbnb. *Tourism Management*, 55:62–73, 2016.

[78] Facebook. Facebook terms of use. `https://www.facebook.com/terms/`, 2017. Online; Accessed: 2017-07-11.

[79] Jody Farnden, Ben Martini, and Kim-Kwang Raymond Choo. Privacy risks in mobile dating apps. In *Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015)*. arXiv preprint arXiv:1505.02906, 2015.

[80] Eli J Finkel, Paul W Eastwick, Benjamin R Karney, Harry T Reis, and Susan Sprecher. Online dating: A critical analysis from the perspective of psychological science. *Psychological Science in the Public Interest*, 13(1):3–66, 2012.

[81] Andrew T Fiore, Lindsay Shaw Taylor, Gerald A Mendelsohn, and Marti Hearst. Assessing attractiveness in online dating profiles. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 797–806. ACM, 2008.

[82] Andrew T Fiore, Lindsay Shaw Taylor, Gerald A Mendelsohn, and Marti Hearst. Assessing attractiveness in online dating profiles. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 797–806. ACM, 2008.

[83] Atlantic Data Forensics. Why you shouldn't use your facebook picture on a dating website. `https://www.atlanticdf.com/news/2016/03/shouldnt-use-facebook-picture-dating-website/`, 2016. Online; Accessed: 2017-07-11.

[84] Emily Fox. Here's how to check if your partner is cheating on tinder. `http://www.vanityfair.com/news/2016/04/check-tinder-cheater-swipe-buster/`, 2016. Online; Accessed: 2017-07-11.

[85] Batya Friedman, Peter H Khan Jr, and Daniel C Howe. Trust online. *Communications of the ACM*, 43(12):34–40, 2000.

[86] Francis Fukuyama. Trust: The social virtues and the creation of prosperity. *Free Press Paperbacks*, (D10 301 c. 1/c. 2), 1995.

[87] Diego Gambetta et al. Can we trust trust. *Trust: Making and breaking cooperative relations*, 13:213–237, 2000.

[88] Liz Gannes. Airbnb now wants to check your government id. `http://allthingsd.com/20130430/airbnb-now-wants-to-check-your-government-id/`, 2017. Online; Accessed: 2017-07-25.

[89] Karoline Gatter and Kathleen Hodkinson. On the differences between tinder™ versus online dating agencies: Questioning a myth. an exploratory study. *Cogent Psychology*, 3(1):1162414, 2016.

[90] David Gefen. Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM Sigmis Database*, 33(3):38–53, 2002.

[91] David Gefen, Elena Karahanna, and Detmar W Straub. Trust and tam in online shopping: an integrated model. *MIS quarterly, Society for Information Management and The Management Information Systems Research Center*, 27(1):51–90, 2003.

[92] Jennifer L Gibbs, Nicole B Ellison, and Rebecca D Heino. Self-presentation in online personals: The role of anticipated future interaction, self-disclosure, and perceived success in internet dating. *Communication Research, Sage Publications Sage CA: Thousand Oaks, CA*, 33(2):152–177, 2006.

[93] Jennifer L Gibbs, Nicole B Ellison, and Chih-Hui Lai. First comes love, then comes google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, 38(1):70–100, 2011.

[94] Anthony Giddens. The consequences of modernity. *Stanford University Press, Stanford, CA*, (9780804718912), 1990.

[95] Mof Gimmers. Match.com is latest dating site to be hacked. `https://www.bitterwallet.com/privacy/match-com-is-latest-dating-site-to-be-hacked-87645/`, 2017. Online; Accessed: 2017-07-11.

[96] Russell Goldman. Woman sues match.com after date attacks her. `http://abcnews.go.com/US/woman-sues-match-date-attacks/story?id=18314916/`, 2013. Online; Accessed: 2017-07-25.

[97] David Good. Individuals, interpersonal relations, and trust. *Trust: Making and breaking cooperative relations*, pages 31–48, 2000.

[98] Sarah Gooding. The most important tips to online dating success. `http://blog.pof.com/2013/06/the-10-most-important-tips-to-online-dating-success/`, 2013. Online; Accessed: 2017-06-30.

[99] Stefano Grazioli, Paul E Johnson, and Karim Jamal. A cognitive approach to fraud detection. *Journal of Forensic Accounting, SSRN Electronic Journal, University of Alberta School of Business Research Paper*, VII, Issue 1:65–88, 2006.

[100] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80. ACM, 2005.

[101] The Guardian. New website lets anyone spy on tinder users. `https://www.theguardian.com/technology/2016/apr/05/tinder-swipebuster-spy-on-users-privacy-dating-app/`, 2016. Online; Accessed: 2017-07-11.

[102] Gregory T Gundlach and Joseph P Cannon. "trust but verify"? the performance implications of verification strategies in trusting relationships. *Journal of the Academy of Marketing Science, Springer*, 38(4):399–417, 2010.

[103] Robert Hackett. Researchers caused an uproar by publishing data from 70,000 okcupid users. `http://fortune.com/2016/05/18/okcupid-data-research/`, 2016. Online; Accessed: 2017-07-25.

[104] Keith Hampton, Lauren Sessions Goulet, Lee Rainie, and Kristen Purcell. Social networking sites and our lives. *Pew Internet & American Life Project*, 16, 2011.

[105] Jeffrey T Hancock, Lauren E Curry, Saurabh Goorha, and Michael Woodworth. On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes, Taylor & Francis*, 45(1):1–23, 2007.

[106] Jeffrey T Hancock, Catalina Toma, and Nicole Ellison. The truth about lying in online dating profiles. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 449–452. ACM, 2007.

[107] Charles Handy. Trust and the virtual organization. *Harvard business review*, 73(3):40–51, 1995.

[108] Michael Hardey. Mediated relationships. *Information, Communication & Society*, 7(2):207–222, 2004.

[109] Valerie Hauch, Iris Blandón-Gitlin, Jaume Masip, and Siegfried L Sporer. Are computers effective lie detectors? a meta-analysis of linguistic cues to deception. *Personality and Social Psychology Review*, 19(4):307–342, 2015.

[110] Rebecca D Heino, Nicole B Ellison, and Jennifer L Gibbs. Relationshopping: Investigating the market metaphor in online dating. *Journal of Social and Personal Relationships, Sage Publications Sage UK: London, England*, 27(4):427–447, 2010.

[111] Millsom Henry-Waring and Jo Barraket. Dating & intimacy in the 21 st century: The use of online dating sites in australia. *International Journal of Emerging Technologies & Society*, 6(1), 2008.

[112] Edward S Hinchman. Assertion, sincerity, and knowledge. *Noûs, Wiley Online Library*, 47(4):613–646, 2013.

[113] Eric Ho. Eric ho's couchsurfing references. `https://www.couchsurfing.com/people/eric-ho-10/references/`, 2017. Online; Accessed: 2017-07-25.

[114] Rachel Hosie. Ashley madison hacking: What happened when married man was exposed. `http://www.independent.co.uk/life-style/love-sex/ashley-madison-hacking-accounts-married-man-exposes-cheating-website-infidelity-rick-thomas-a7529356.html/`, 2017. Online; Accessed: 2017-08-22.

[115] JingMin Huang, Gianluca Stringhini, and Peng Yong. Quit playing games with my heart: Understanding online dating scams. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 216–236. Springer, 2015.

[116] Nick Janetos and Jan Tilly. Reputation dynamics in a market for illicit drugs. *arXiv preprint arXiv:1703.01937*, 2017.

[117] Annukka Jänkälä et al. Dating expectations in social media: From profile pictures to a date and beyond. Master's thesis, Aalto University, 2017.

[118] Sirkka L Jarvenpaa and Dorothy E Leidner. Communication and trust in global virtual teams. *Journal of Computer-Mediated Communication*, 3(4):0–0, 1998.

[119] Jimmy. Government id vs personal info. `https://community.withairbnb.com/t5/Help/Government-ID-vs-Personal-info/td-p/294119/`, 2017. Online; Accessed: 2017-07-25.

[120] Jo. 7 couchsurfing stories from across the globe. `https://www.wanderwithjo.com/couchsurfing-stories/`, 2016. Online; Accessed: 2017-07-25.

[121] Patrik N Juslin and Klaus R Scherer. Vocal expression of affect. *The new handbook of methods in nonverbal behavior research*, pages 65–135, 2005.

[122] KM Kambara. The social construction of online dating: Towards an understanding of technological use and consumption. In *Philadelphia, PA: Paper presented at the Annual Meeting of the American Sociological Association*, 2005.

[123] Stacey Katz-Schiavone, Jill S Levenson, and Alissa R Ackerman. Myths and facts about sexual violence: Public perceptions and implications for prevention. *Journal of Criminal Justice and Popular Culture*, 15(3):291–311, 2008.

[124] Kijiji. Safety at kijiji. `https://help.kijiji.ca/helpdesk/basics/safety-at-kijiji/`, 2017. Online; Accessed: 2017-07-25.

[125] Dan J Kim, Donald L Ferrin, and H Raghav Rao. A study of the effect of consumer trust on consumer expectations and satisfaction: The korean experience. In *Proceedings of the 5th international conference on Electronic commerce*, pages 310–315. ACM, 2003.

[126] Sherrie Xiao Komiak and Izak Benbasat. Understanding customer trust in agent-mediated electronic commerce, web-mediated electronic commerce, and traditional commerce. *Information Technology and Management*, 5(1-2):181–207, 2004.

[127] Andrew Koubaridis. Tourist sexually assaulted in sydney by several men after meeting on tinder. `http://www.news.com.au/national/tourist-sexually-assaulted-in-sydney-by-several-men-after-meeting-on-tinder/news-story/f30af6eb552e5d2a201514b112faa14b/`, 2014. Online; Accessed: 2017-07-25.

[128] KrebsOnSecurity. Plentyoffish.com hacked, blames messenger. `https://krebsonsecurity.com/2011/01/plentyoffish-com-hacked-blames-messenger/`, 2011. Online; Accessed: 2017-07-11.

[129] Jody Kreiman and Diana Sidtis. Introduction. In *Foundations of voice studies: An interdisciplinary approach to voice production and perception*. John Wiley & Sons, Wiley-Blackwell, Oxford, UK., 2011.

[130] Katharina Krombholz, Dieter Merkl, and Edgar Weippl. Fake identities in social media: A case study on the sustainability of the facebook business model. *Journal of Service Science Research*, 4(2):175, 2012.

[131] Laney and Brent. Airbnb host's homepage. `https://www.airbnb.ca/users/show/764443/`, 2017. Online; Accessed: 2017-07-25.

[132] Robert LaRose, Nora J Rifon, and Richard Enbody. Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3):71–76, 2008.

[133] Chih-Chen Lee, Robert B Welker, and Marcus D Odom. Features of computer-mediated, text-based messages that support automatable, linguistics-based indicators for deception detection. *Journal of Information Systems*, 23(1):5–24, 2009.

[134] William Lee. Match.com assault victim: I wasn't going to let it destroy my life. `http://www.chicagotribune.com/news/ct-match-com-victim-settlement-met-20160606-story.html/`, 2016. Online; Accessed: 2017-07-25.

[135] Amanda Lenhart, Rich Ling, Scott Campbell, and Kristen Purcell. Teens and mobile phones: Text messaging explodes as teens embrace it as the centerpiece of their communication strategies with friends. *Pew Internet & American Life Project*, 2010.

[136] Roy J Lewicki and Barbara B Bunker. Developing and maintaining trust in work relationships. *Trust in organizations: Frontiers of theory and research*, 114:139, 1996.

[137] Roy J Lewicki and Barbara Benedict Bunker. Trust in relationships. *Administrative Science Quarterly*, 5:583–601, 1995.

[138] Tracey Lien. Kalamazoo shooting: Here's how Uber does its background checks. `http://www.latimes.com/business/technology/la-fi-tn-uber-background-check-20160222-story.html/`, 2017. Online; Accessed: 2017-07-25.

[139] Natasha Lomas. Someone scraped 40,000 tinder selfies to make a facial dataset for ai experiments. `https://techcrunch.com/2017/04/28/someone-scraped-40000-tinder-selfies-to-make-a-facial-dataset-for-ai-experiments/`, 2017. Online; Accessed: 2017-07-11.

[140] Bridget L Long. *Scripts for online dating: A model and theory of online romantic relationship initiation.* PhD thesis, Bowling Green State University, 2010.

[141] Michael Luca. Reviews, reputation, and revenue: The case of yelp. com. *Harvard Business School Working Paper,2011 (Revised March 2016. Revise and resubmit at the American Economic Journal - Applied Economics)*, 12-016, 2016.

[142] Niklas Luhmann. Trust and power. *Studies in Soviet Thought, Springer*, 23(3):266–270, 1982.

[143] Niklas Luhmann. Familiarity, confidence, trust: Problems and perspectives. i gambetta, diego (red.). In Diego Gambetta, editor, *Trust: Making and Breaking Cooperative Relations.* Blackwell, 1988.

[144] Wenhong Luo and Mohammad Najdawi. Trust-building measures: a review of consumer health portals. *Communications of the ACM*, 47(1):108–113, 2004.

[145] Anna Lysyanskaya. Cryptography: How to keep your secrets safe. *Scientific American*, pages 89–94, 2008.

[146] Michael W Macy and John Skvoretz. The evolution of trust and cooperation between strangers: A computational model. *American Sociological Review*, pages 638–660, 1998.

[147] Mary Madden and Amanda Lenhart. Online dating. `http://www.pewinternet.org/2006/03/05/online-dating/`, 2006. Pew Internet and American Life Project Online; Accessed: 2017-07-25.

[148] Adriana M Manago, Michael B Graham, Patricia M Greenfield, and Goldie Salimkhan. Self-presentation and gender on myspace. *Journal of Applied Developmental Psychology*, 29(6):446–458, 2008.

[149] Charlie Marchant. Best and worst couchsurfing stories from around the world. `http://charlieontravel.com/best-worst-couchsurfing-stories/`, 2014. Online; Accessed: 2017-07-25.

[150] Stephen Paul Marsh. *Formalising trust as a computational concept*. PhD thesis, University of Stirling, 1994.

[151] Robinson Martin and Zolfagharifard Ellie. Names of 37 million cheating spouses are leaked online: Hackers dump huge data file revealing clients of adultery website ashley madison - including bankers, un and vatican staff. `http://www.dailymail.co.uk/sciencetech/article-3202851/Ashley-Madison-customers-exposed-Hackers-finally-posted-details-cheating-spouses-use-adultery-site.html/`, 2015. Online; Accessed: 2017-08-22.

[152] Christopher M Mascaro, Rachel M Magee, and Sean P Goggins. Not just a wink and smile: an analysis of user-defined success in online dating. In *Proceedings of the 2012 iConference*, pages 200–206. ACM, 2012.

[153] Match.com. Match.com, l.l.c. privacy policy. `http://www.match.com/registration/privacystatement.aspx/`, 2016. Online; Accessed: 2017-07-11.

[154] Match.com. Match help page. `http://www.match.com/help/faq/7/145/`, 2017. Online; Accessed: 2017-04-14.

[155] Match.com. Match.com faq adding photos. `http://www.match.com/help/faq/7/128/\#holder/`, 2017. Online; Accessed: 2017-06-30.

[156] Match.com. Match.com faq blocking and unblocking. `http://www.match.com/help/faq/3/50/\#holder/`, 2017. Online; Accessed: 2017-04-14.

[157] Match.com. Match.com faq canceling a membership. `http://www.match.com/help/faq/1/2/\#holder/`, 2017. Online; Accessed: 2017-07-11.

[158] Match.com. Match.com faq messaging free members. `http://www.match.com/help/faq/3/63/\#holder/`, 2017. Online; Accessed: 2017-06-30.

[159] Match.com. Match.com faq mutual matches-explained. http://www.match.com/help/faq/8/164/\#holder/, 2017. Online; Accessed: 2017-06-30.

[160] Match.com. Match.com faq profile completion requirements. http://www.match.com/help/faq/7/143/\#holder/, 2017. Online; Accessed: 2017-06-30.

[161] Match.com. Match.com faq singled out - explained. http://www.match.com/help/faq/8/178/\#holder/, 2017. Online; Accessed: 2017-06-30.

[162] Match.com. Match.com homepage. https://www.match.ca/, 2017. Online; Accessed: 2017-04-14.

[163] Match.com. Match.com terms of use agreement. http://www.match.com/registration/membagr.aspx/, 2017. Online; Accessed: 2017-06-30.

[164] Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of management review*, 20(3):709–734, 1995.

[165] MCASA. Reporting sexual assault: Why survivors often don't. https://ocrsm.umd.edu/files/Why-Is-Sexual-Assault-Under-Reported.pdf/, 2017. Online; Accessed: 2017-07-25.

[166] Steven A McCornack. Information manipulation theory. *Communications Monographs*, 59(1):1–16, 1992.

[167] Steven A McCornack, Kelly Morrison, Jihyun Esther Paik, Amy M Wisner, and Xun Zhu. Information manipulation theory 2: a propositional theory of deceptive discourse production. *Journal of Language and Social Psychology*, 33(4):348–377, 2014.

[168] Rory McGloin and Amanda Denes. Too hot to trust: Examining the relationship between attractiveness, trustworthiness, and desire to date in online dating. *New Media & Society, SAGE Publications*, pages 1461–4448, 2016.

[169] Brent McRae and Jessica McKnight. Privacy and online dating. *Convenient or Invasive: The Information Age, Boulder, CO: Ethica*, 2007.

[170] Meetup. Does meetup cost money? https://www.meetup.com/help/article/902250/, 2017. Online; Accessed: 2017-07-25.

[171] Meetup. Event fees. https://www.meetup.com/help/article/902189/, 2017. Online; Accessed: 2017-07-25.

[172] Meetup. Get feedback from my members. https://www.meetup.com/help/article/868868/, 2017. Online; Accessed: 2017-07-25.

[173] Meetup. Meetup homepage. https://www.meetup.com/, 2017. Online; Accessed: 2017-07-25.

[174] Meetup. Member dues. https://www.meetup.com/help/article/1064652/, 2017. Online; Accessed: 2017-07-25.

[175] Meetup. Organizer subscription pricing. https://www.meetup.com/pricing/, 2017. Online; Accessed: 2017-07-25.

[176] Meetup. Rate a meetup event. https://www.meetup.com/help/article/875294/, 2017. Online; Accessed: 2017-07-25.

[177] Albert Mehrabian. Nonverbal communication. In *Nebraska symposium on motivation*. University of Nebraska Press, 1971.

[178] Gustavo S Mesch and Ilan Talmud. Online friendship formation, communication channels, and social closeness. *International Journal of Internet Science*, 1(1):29–44, 2006.

[179] Ian Miers, Matthew Green, Christoph U Lehmann, and Aviel D Rubin. Vis-à-vis cryptography: Private and trustworthy in-person certifications. In *Presented as part of the 3rd USENIX Workshop on Health Security and Privacy*, Bellevue, WA, 2012. USENIX.

[180] Rada Mihalcea and Carlo Strapparava. The lie detector: Explorations in the automatic recognition of deceptive language. In *Proceedings of the ACL-IJCNLP 2009 Conference Short Papers*, pages 309–312. Association for Computational Linguistics, 2009.

[181] John Mikhail, Emad Farag, and Minasyan. Cryptographic dating. https://courses.csail.mit.edu/6.857/2016/files/35.pdf/, 2016. Online; Accessed: 2017-06-30.

[182] Ananda Mitra. Trust, authenticity, and discursive power in cyberspace. *Communications of the ACM*, 45(3):27–29, 2002.

[183] KC Moffitt, JS Giboney, E Ehrhardt, JK Burgoon, and JF Nunamaker. Structured programming for linguistic cue extraction (splice). In *Proceedings of the HICSS-45 Rapid Screening Technologies, Deception Detection and Credibility Assessment Symposium*, pages 103–108, 2012.

[184] Robert M Morgan and Shelby D Hunt. The commitment-trust theory of relationship marketing. *The journal of marketing*, pages 20–38, 1994.

[185] V Narendhiran. Tinder without facebook. https://www.allinfopark.net/tinder-without-facebook-working-methods, 2016. Online; Accessed: 2017-06-30.

[186] Dave Neal. Match.com claims that members have been untouched by malvertising attack. https://www.theinquirer.net/inquirer/news/2424475/matchcom-malvertising-hack-suggests-that-digital-daters-are-doomed/, 2015. Online; Accessed: 2017-07-11.

[187] Matthew L Newman, James W Pennebaker, Diane S Berry, and Jane M Richards. Lying words: Predicting deception from linguistic styles. *Personality and social psychology bulletin*, 29(5):665–675, 2003.

[188] Riley Newman and Judd Antin. Building for trust; insights from our efforts to distill the fuel for the sharing economy. `https://medium.com/airbnb-engineering/building-for-trust-503e9872bbbb/`, 2017. Online; Accessed: 2017-07-25.

[189] Uber Nigeria. Lagos, cash payments are arriving now! `https://www.uber.com/en-NG/blog/lagos-cash-payments-are-arriving-now/`, 2017. Online; Accessed: 2017-07-25.

[190] Gregory Norcie, Emiliano De Cristofaro, and Victoria Bellotti. Bootstrapping trust in online dating: Social verification of online dating profiles. In *International Conference on Financial Cryptography and Data Security*, pages 149–163. Springer, 2013.

[191] Olivia Nuzzi. The definitive list of Uber horror stories. `http://www.thedailybeast.com/the-definitive-list-of-uber-horror-stories/`, 2014. Online; Accessed: 2017-07-25.

[192] Plenty of Fish. Plenty of fish help center: Pof faq. `http://www.pof.com/helpcenter/helpcenter_faq.aspx/`, 2017. Online; Accessed: 2017-07-11.

[193] Plenty of Fish. Plenty of fish help center: Upgraded memberships. `http://www.pof.com/HelpCenter/helpcenter_upgradedMemberships.aspx/`, 2017. Online; Accessed: 2017-06-30.

[194] Plenty of Fish. Plenty of fish help center: Upload image. `http://www.pof.com/HelpCenter/helpCenter_uploadImage.aspx/`, 2017. Online; Accessed: 2017-06-30.

[195] Plenty of Fish. Plenty of fish image upload. `http://www.pof.com/userimages.aspx/`, 2017. Online; Accessed: 2017-07-11.

[196] Plenty of Fish. Pof homepage. `http://www.pof.com/`, 2017. Online; Accessed: 2017-04-14.

[197] Plenty of Fish. Pof statistics. `http://www.datingsitesreviews.com/staticpages/index.php?page=Plenty-of-Fish-Statistics-Facts-History/`, 2017. Online; Accessed: 2017-04-14.

[198] OnceATraveller. Couchsurfing love story. `http://www.onceatraveler.com/couchsurfing-love-story/`, 2012. Online; Accessed: 2017-07-25.

[199] Jenny Onyx and Paul Bullen. Measuring social capital in five communities. *The journal of applied behavioral science*, 36(1):23–42, 2000.

[200] Koray Özpolat and Wolfgang Jank. Getting the most out of third party trust seals: An empirical analysis. *Decision Support Systems*, 73:47–56, 2015.

[201] Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, and Markus Jakobsson. Scambaiter: Understanding targeted nigerian scams on craigslist. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*. NDSS, 2014.

[202] Paul Pavlou. Integrating trust in electronic commerce with the technology acceptance model: model development and validation. In *Proceedings of Americas Conference on Information Systems (AMCIS)*, page 159, 2001.

[203] Bridgette Peteet, Caravella McCuistian, and Quiera Lige. Something new: A scholarly review and clinical perspective of black online dating. *Journal of Black Sexuality and Relationships, University of Nebraska Press*, 1(2):81–96, 2014.

[204] Andrea Peterson and William Wan. Uber panic button. `https://www.washingtonpost.com/news/the-switch/wp/2016/02/22/uber-has-a-panic-button-in-india-but-dont-expect-it-to-come-to-the-u-s/?utm_term=.dc0917fe6ff7/`, 2017. Online; Accessed: 2017-04-14.

[205] Iasonas Polakis, George Argyros, Theofilos Petsios, Suphannee Sivakorn, and Angelos D Keromytis. Where's wally?: Precise user discovery attacks in location proximity services. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 817–828. ACM, 2015.

[206] Huffington Post. Mary kay beckman sues match.com after wade ridley tried to murder her. `http://www.huffingtonpost.com/2013/01/24/mary-kay-beckman_n_2544390.html/`, 2016. Online; Accessed: 2017-07-11.

[207] User Post. Couch bangs. `https://couchbangs.wordpress.com/page/2/`, 2013. Online; Accessed: 2017-07-25.

[208] User Post. Couchsurfing is a substitute for a dating site. `https://www.reddit.com/r/couchsurfing/comments/1vbr1u/couchsurfing_is_a_substitute_for_a_dating_site/?st=j4fk2w88&sh=4ca0c310`, 2014. Online; Accessed: 2017-07-25.

[209] User Post. Couchsurfing is a dating site, get over it. `https://www.reddit.com/r/couchsurfing/comments/3a2ao7/couchsurfing_is_a_dating_site_get_over_it/?st=j4fk1ow0&sh=c45f9d31/`, 2015. Online; Accessed: 2017-07-25.

[210] PowerReviews. The power of reviews. `http://www.powerreviews.com/wp-content/uploads/2015/08/13185402/ThePowerofReviews-Report.pdf3/`, 2014. Online; Accessed: 2017-07-25.

[211] Michael K Rabby. Relational maintenance and the influence of commitment in online and offline relationships. *Communication Studies*, 58(3):315–337, 2007.

[212] Steve Ragan. HIV dating app leaks sensitive information, company threatens infection over disclosure. `http://www.csoonline.com/article/3014580/security/hiv-dating-app-leaks-sensitive-information-company-threatens-infection-over-disclosure.html/`, 2015. Online; Accessed: 2017-07-25.

[213] Anita Ramasastry. Does match.com have to make sure its member profiles are real and accurate? Why a federal judge correctly ruled no. `https://verdict.justia.com/2012/09/11/does-match-com-have-to-make-sure-its-member-profiles-are-real-and-accurate/`, 2012. Online; Accessed: 2017-06-30.

[214] Pauline Ratnasingham and Kuldeep Kumar. Trading partner trust in electronic commerce participation. In *Proceedings of the twenty first international conference on Information systems*, pages 544–552. Association for Information Systems, 2000.

[215] Aunshul Rege. What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, 3(2):494, 2009.

[216] Telegraph Reporters. Ashley madison admits tricking men with fake fembots. `http://www.telegraph.co.uk/women/life/ashley-madison-admits-tricking-men-with-fake-fembots/`, 2016. Online; Accessed: 2017-08-22.

[217] Paul Resnick, Ko Kuwabara, Richard Zeckhauser, and Eric Friedman. Reputation systems. *Communications of the ACM*, 43(12):45–48, 2000.

[218] Paul Resnick and Hal R Varian. Recommender systems. *Communications of the ACM*, 40(3):56–58, 1997.

[219] Howard Rheingold. A slice of my life in my virtual community. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, MIT Press*, pages 413–36, 1996.

[220] Jens Riegelsberger, M Angela Sasse, and John D McCarthy. The researcher's dilemma: evaluating trust in computer-mediated communication. *International Journal of Human-Computer Studies, Elsevier*, 58(6):759–781, 2003.

[221] Jens Riegelsberger, M Angela Sasse, and John D McCarthy. Shiny happy people building trust?: Photos on e-commerce websites and consumer trust. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 121–128. ACM, 2003.

[222] Nora J Rifon, Robert LaRose, and Sejung Choi. Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, 39(2):339–362, 2005.

[223] Peter Smith Ring and Andrew H Van de Ven. Structuring cooperative relationships between organizations. *Strategic Management Journal, Wiley Online Library*, 13(7):483–498, 1992.

[224] Elena Rocco. Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 496–502. ACM Press/Addison-Wesley Publishing Co., 1998.

[225] Michael J Rosenfeld and Reuben J Thomas. Searching for a mate the rise of the internet as a social intermediary. *American Sociological Review*, 77(4):523–547, 2012.

[226] Julian B Rotter. A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35(4):651–665, 1967.

[227] Julian B Rotter. Generalized expectancies for interpersonal trust. *American Psychologist*, 26(5):443, 1971.

[228] Julian B Rotter. Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, 35(1):1, 1980.

[229] Denise M Rousseau, Sim B Sitkin, Ronald S Burt, and Colin Camerer. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3):393–404, 1998.

[230] Jörn PW Scharlemann, Catherine C Eckel, Alex Kacelnik, and Rick K Wilson. The value of a smile: Game theory with a human face. *Journal of Economic Psychology*, 22(5):617–640, 2001.

[231] Steve Schmadeke. Public relations exec is convicted of raping woman he met on an online dating site. `http://www.chicagotribune.com/news/ct-executive-rape-trial-met-20141211-story.html/`, 2014. Online; Accessed: 2017-07-25.

[232] Björn W Schuller, Stefan Steidl, Anton Batliner, Julia Hirschberg, Judee K Burgoon, Alice Baird, Aaron C Elkins, Yue Zhang, Eduardo Coutinho, and Keelan Evanini. The INTERSPEECH 2016 computational paralinguistics challenge: Deception, sincerity & native language. *Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH*, pages 2001–2005, 2016.

[233] SFSU. Myths and facts about sexual violence. `http://titleix.sfsu.edu/sites/default/files/MythsAndFactsAboutSexualViolence.pdf/`, 2017. Online; Accessed: 2017-07-25.

[234] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, 48:199–207, 2015.

[235] Husna Siddiqui, Callum Brill, Zachary Davis, and Aspen Olmsted. Friend or faux? engineering your social network to detect fraudulent profiles. In *Information Society (i-Society), 2016 International Conference on*, pages 169–170. IEEE, 2016.

[236] Aaron Smith and Monica Anderson. 5 facts about online dating. `http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/`, 2016. Online; Accessed: 2017-07-25.

[237] Aaron Whitman Smith and Maeve Duggan. Online dating & relationship. `http://www.pewinternet.org/2013/10/21/online-dating-relationships/`, 2013. Online; Accessed: 2017-07-25.

[238] Adam Smith. The theory of moral sentiments. *Cambridge Texts in the History of Philosophy, Cambridge University Press, Haakonssen, KnudEditor*, 2002.

[239] Lauren Reichart Smith, Kenny D Smith, and Matthew Blazka. Follow me, what's the harm? considerations of catfishing and utilizing fake online personas on social media. *Journal of Legal Aspects of Sport*, 27(1):32–45, 2017.

[240] Chris Snijders and Gideon Keren. Determinants of trust. In *Games and human behavior : essays in honor of Amnon Rapoport / Ed. D. van Budescu, I. Erev, R. Zwick. - Hillsdale, New Jersey : Lawrence Erlbaum*, pages 355–385, 1999.

[241] Siegfried Ludwig Sporer and Barbara Schwandt. Paraverbal indicators of deception: A meta-analytic synthesis. *Applied Cognitive Psychology*, 20(4):421–446, 2006.

[242] Astoria Starr. The 15 most shocking Uber horror stories ever. `http://www.therichest.com/rich-list/most-shocking/the-15-most-shocking-uber-horror-stories-ever/`, 2016. Online; Accessed: 2017-07-25.

[243] Ulrike Steinbrück, Heike Schaumburg, Sabrina Duda, and Thomas Krüger. A picture says more than a thousand words: Photographs as trust builders in e-commerce websites. In *CHI'02 extended abstracts on Human factors in computing systems*, pages 748–749. ACM, 2002.

[244] R Todd Stephens. A framework for the identification of electronic commerce design elements that enable trust within the small hotel industry. In *Proceedings of the 42nd annual Southeast regional conference*, pages 309–314. ACM, 2004.

[245] The Sun. Olympics and chill, 'a sexually charged time': Inside rio olympic's tinder game where athletes are getting their swipe on. `https://www.thesun.co.uk/living/1588637/a-sexually-charged-time-inside-rio-olympics-tinder-game-where-athletes-are-getting-their-swipe-on/`, 2016. Online; Accessed: 2017-07-25.

[246] Sya. Couchsurfing to love. `http://www.patheos.com/blogs/loveinshallah/2013/01/23/couchsurfing-to-love/`, 2013. Online; Accessed: 2017-07-25.

[247] Yla R Tausczik and James W Pennebaker. The psychological meaning of words: Liwc and computerized text analysis methods. *Journal of Language and Social Psychology, Sage Publications Sage CA: Los Angeles, CA*, 29(1):24–54, 2010.

[248] Michael Tegos. Uber launches cash payments in Singapore. `https://www.techinasia.com/uber-cash-payments-singapore/`, 2017. Online; Accessed: 2017-07-25.

[249] Lisa Collins Tidwell and Joseph B Walther. Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human communication research*, 28(3):317–348, 2002.

[250] Tiffany. The romantic side of couchsurfing. `http://www.hejorama.com/articles/the-romantic-side-of-couchsurfing-1417/`, 2011. Online; Accessed: 2017-07-25.

[251] Tinder. Tinder homepage. `https://www.tinder.com/`, 2017. Online; Accessed: 2017-04-14.

[252] Catalina Toma. An examination of deceptive self-presentation in online dating profiles. Master's thesis, Cornell University, 2006.

[253] Hannes Tschofenig, Melanie Volkamer, Nicola Jentzsch, Simone Fischer-Hübner, Stefan Schiffner, and Rodica Tirtea. On the security, privacy and usability of online seals: An overview. *European Union Agency for Network and Information Security (ENISA)*, 2013.

[254] Douglas Twitchell, Jay Nunamaker, and Judee Burgoon. Using speech act profiling for deception detection. *Intelligence and Security Informatics*, pages 403–410, 2004.

[255] Uber. Drive with uber Ottawa. `https://www.uber.com/en-CA/drive/ottawa/`, 2017. Online; Accessed: 2017-07-25.

[256] Uber. How uber helps keep riders safe. https://www.uber.com/en-CA/ride/safety/, 2017. Online; Accessed: 2017-07-25.

[257] Uber. I want to use Uber without a smartphone. https://help.uber.com/h/b9dc6681-b346-4774-9ab1-ecaa3f22cabe/, 2017. Online; Accessed: 2017-07-25.

[258] Uber. Uber cash faq. https://www.uber.com/en-SG/drive/resources/cash-faq/, 2017. Online; Accessed: 2017-07-25.

[259] Uber. Uber community guidelines. https://www.uber.com/legal/community-guidelines/us-en/, 2017. Online; Accessed: 2017-07-25.

[260] Uber. Uber homepage. https://www.uber.com/en-CA/, 2017. Online; Accessed: 2017-07-25.

[261] Uber. Uber Nigeria faq. https://www.ubernigeria.com/faq/, 2017. Online; Accessed: 2017-07-25.

[262] Uber. Uber safety tips. https://www.uber.com/info/rider-safety-tips/, 2017. Online; Accessed: 2017-07-25.

[263] Angela Upex. How to protect yourself when using online dating services. http://www.chroniclelive.co.uk/special-features/how-protect-yourself-using-online-13047420/, 2017. Online; Accessed: 2017-06-30.

[264] Reddit User. Reddit tinder comment. https://www.reddit.com/r/Tinder/comments/3lymz1/reported_too_many_times_cant_even_delete_my, 2016. Online; Accessed: 2017-06-30.

[265] Lyn M Van Swol, Michael T Braun, and Deepak Malhotra. Evidence for the pinocchio effect: Linguistic differences between lies, deception by omissions, and truths. *Discourse Processes*, 49(2):79–106, 2012.

[266] Vayable. Vayable's terms of service. https://www.vayable.com/terms/, 2013. Online; Accessed: 2017-07-25.

[267] Vayable. Vayable guides. https://www.vayable.com/guides/, 2017. Online; Accessed: 2017-07-25.

[268] Iris Vessey. Cognitive fit: A theory-based analysis of the graphs versus tables literature. *Decision Sciences*, 22(2):219–240, 1991.

[269] Daniel Victor. The ashley madison data dump, explained. https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html/, 2015. Online; Accessed: 2017-07-25.

[270] Vince. How do i write a good couch request? `https://support.couchsurfing.org/hc/en-us/articles/200640010-How-do-I-write-a-good-couch-request-/`, 2017. Online; Accessed: 2017-07-25.

[271] Vince. What is the difference between surf, host and personal references and feedback? `https://support.couchsurfing.org/hc/en-us/articles/212281057-What-is-the-difference-between-Surf-Host-and-Personal-references-and-Feedback-/`, 2017. Online; Accessed: 2017-07-25.

[272] Aldert Vrij, Ronald Fisher, Samantha Mann, and Sharon Leal. Detecting deception by manipulating cognitive load. *Trends in Cognitive Sciences*, 10(4):141–142, 2006.

[273] Aldert Vrij, Pär Anders Granhag, and Stephen Porter. Pitfalls and opportunities in nonverbal and verbal lie detection. *Psychological Science in the Public Interest*, 11(3):89–121, 2010.

[274] Joseph B Walther. Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research, Sage Publications London*, 23(1):3–43, 1996.

[275] Wei and Ting. Block people. `https://community.withairbnb.com/t5/Hosting/Block-People/td-p/90073/`, 2016. Online; Accessed: 2017-07-25.

[276] Alma Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 14–14, Berkeley, CA, USA, 1999. USENIX Association.

[277] Monica Whitty and Tom Buchanan. The psychology of the online dating romance scam. *A report for Economic and Social Research Council (ESRC)*, page 23, 2012.

[278] Monica Whitty and Adrian Carr. Cyberspace romance: The psychology of online relationships. *Palgrave Macmillan New York*, pages xvi, 218 p. ;, 2006.

[279] Jeanne Wilson, Susan Straus, and Bill McEvily. All in due time: The development of trust in electronic and face-to-face groups. *Organizational Behavior and Human Decision Processes, Elsevier*, 99:16–33, 2000.

[280] Rick K Wilson and Catherine C Eckel. Judging a book by its cover: Beauty and expectations in the trust game. *Political Research Quarterly*, 59(2):189–202, 2006.

[281] Peng Xia, Bruno Ribeiro, Cindy Chen, Benyuan Liu, and Don Towsley. A study of user behavior on an online dating site. In *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on*, pages 243–247. IEEE, 2013.

[282] Sherrie Xiao and Izak Benbasat. The formation of trust and distrust in recommendation agents in repeated interactions: a process-tracing analysis. In *Proceedings of the 5th international conference on Electronic commerce*, pages 287–293. ACM, 2003.

[283] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering*, 16(7):843–857, 2004.

[284] Yutaka Yamamoto. A morality based on trust: Some reflections on Japanese morality. *Philosophy East and West, University of Hawaii Press*, 40(4):451–469, 1990.

[285] Artem Yankov. How to find facebook users on match.com by using face recognition tools. `http://artemyankov.com/how-to-find-facebook-users-on-match-dot-com-by-using-face-recognition-tools/`, 2015. Online; Accessed: 2017-07-11.

[286] Alyson L Young and Anabel Quan-Haase. Information revelation and internet privacy concerns on social network sites: a case study of facebook. In *Proceedings of the fourth international conference on Communities and technologies*, pages 265–274. ACM, 2009.

[287] Giorgos Zacharia and Pattie Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(9):881–907, 2000.

[288] Paul J Zak and Brad Winn. The neuroscience of trust. *People and Strategy, New York, Human Resource Planning Society*, 37(2):14–17, 2014.

[289] Lina Zhou, Judee K Burgoon, Jay F Nunamaker, and Doug Twitchell. Automating linguistics-based cues for detecting deception in text-based asynchronous computer-mediated communications. *Group decision and negotiation*, 13(1):81–106, 2004.

[290] John Zimmerman and Kaushal Kurapati. Exposing profiles to build trust in a recommender. In *CHI'02 Extended Abstracts on Human Factors in Computing Systems*, pages 608–609. ACM, 2002.

[291] Miron Zuckerman, Bella M DePaulo, and Robert Rosenthal. Verbal and nonverbal communication of deception. *Advances in experimental social psychology*, 14:1–59, 1981.

[292] Martin Zwilling. How many more online dating sites do we need? `https://www.forbes.com/sites/martinzwilling/2013/03/01/how-many-more-online-dating-sites-do-we-need/#3cbdcaf17882/`, 2013. Online; Accessed: 2017-07-25.

[293] Douglas Zytko, Sukeshini A Grandhi, and Quentin Jones. Impression management struggles in online dating. In *Proceedings of the 18th international conference on supporting group work*, pages 53–62. ACM, 2014.

[294] Douglas Zytko, Sukeshini A Grandhi, and Quentin Jones. Frustrations with pursuing casual encounters through online dating. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1935–1940. ACM, 2015.