ICEB 2010 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-1-2010

Intended Deception in the Virtual World

Lina Zhou

Dongsong Zhang

INTENDED DECEPTION IN THE VIRTUAL WORLD

Lina Zhou, University of Maryland Baltimore County, USA
Dongsong Zhang, University of Maryland Baltimore County, USA
E-mail: {zhoul, zhangd}@umbc.edu

Abstract

This study explores how people intend to deceive in the virtual world. Previous research has focused the intent and behavior of online deception, but has rarely looked into specific aspects of online deception including strategy, magnitude, and seriousness. We answered research questions about people's selection of deception strategies, perceived seriousness of deception, and magnitude of deception in the virtual world via a survey study. Additionally, we examined possible influence of age and gender on deception. The findings are interesting and offer implications for designing deception detection strategies.

Introduction

As an increasingly popular type of virtual community, the virtual world is an electronic artificial environment where users assume an identity as a made-up character and interact with other users in real time in a somewhat realistic manner. The virtual world offers a new platform and unprecedented opportunities for electronic business, with potential benefits ranging from increased productivity, enhanced engagement with customers or audience to reduced business costs [1]. The platform also takes online shopping experience to a higher level by providing rich and innovative means for navigation, community support, and multi-modal communication within its 3D marketplace [2, 3].

While cultivating new business opportunities and enabling new interaction experience, virtual world technologies may also provide easy and unique opportunities for deception [4]. Fraud is already a common problem that traditional 2D online businesses and consumers face [5]. The Web site of FBI Internet Crime Complaint Center received 336,655 Internet crime complaint submissions in 2009, which was a 22.3% increase as compared to 2008. Credit card fraud and auction fraud were among the top categories of offenses, accounting for 10.4% and 10.3% of all the referred cases respectively. Being an immersive virtual environment, the virtual world may foster new types of deception.

One of the major functions of the virtual world is social networking. A study of adults from 16 industrialized nations shows that, "on average, people belong to two social networking sites and have regular contact with 16 people who they have virtually met on the internet [6]". Deception can seriously harm a community and individuals because it damages trust, a necessary condition for the survival and growth of any communities [7]. Therefore, by improving our understanding of deception in the virtual world, we can help develop strategies and measures to counter against deception.

Deception is a part of daily life and the Internet is just a new and powerful tool for its practice [8]. Recent research efforts on deception in online communication such as emails and instant messaging have generated significant interests and findings. Some types of deception, such as gender switching, age deception, and enhancement of status, are easier to commit when communicating online than offline [9]. This is because people look for visual signs to identify the gender, age, personality traits, physical traits, and other features of a speaker, in addition to what he/she says. These types of features are filtered by electronic communication channels. Although in the virtual world, users can choose or create avatars to represent their self images, those avatars do not fully transfer non-verbal behavior of individuals such as body language, gestures, and even voice. This is partly because deceivers are more likely to choose avatars that are different from themselves [10]. The Internet offers an opportunity for users to experiment with their identity [11]. The ways for users to present their virtual selves are limited only by technology and imagination [10]. Virtual world technology is unique in that it provides support for communication and virtual world collaboration [4], compared with traditional online communication counterparts. Specifically, individuals do not have control over whom they interact with, and interactions are openly accessible by others. These two characteristics make virtual worlds especially prone to deception. However, we just start to understand deception in the virtual world.

Given the unique characteristics of the virtual world and potential impact of communication media on deception behavior [12-14], this study investigates deception in the virtual world. This study not only provides a preliminary understanding of deception in the virtual world in general but also looks into specific aspects of deception, including deception strategies, seriousness, and magnitude. Additionally, it investigates whether deception behavior varies with gender and age. The findings of this study enrich the deception literature and offer implications for designing deception detection strategies.

The rest of the paper is organized as the following. We introduce the theoretical background and research questions in the next section. Then, we describe the research methodology and present and discuss the results in the following two sections. Finally, we conclude the paper with contributions and future research.

Theoretical Background and Research Questions

Online Deception and Its Aspects

In response to the popularity of the Internet in interpersonal and business communication, there are emerging streams of research on online deception. Among them, some focus on online fraud in business communication such as credit card fraud and auction fraud [15, 16]. Others study deception in interpersonal communication (e.g., [12, 17]). The current study falls into the latter category.

Extant research on online deception can be grouped into several focused areas: classification of deception (e.g. [18]), identification of cues to deception [12], detection of moderating factors on cues to deception (e.g., [19]), and development of techniques for automatic deception detection [20]. These research foci are important because they provide strong initial evidence showing that: 1) some traditional deception theories developed based on face-to-face communication can be extended to explain some online deception behavior; and 2) online deception has some unique edges over face-to-face deception, calling for the development of new theories and models. The findings of this research are expected to contribute to this line of inquiry by investigating deception in the virtual world.

According to Interpersonal Deception Theory [21], deception involves both strategic and non-strategic behaviors within the context and relationship between the deceiver and targets of deception. Specifically, deceivers will display strategic modifications of behavior in response to a target's suspicion, but they may also display nonstrategic behavior, or leakage cues, that indicate the occurrence of deception. Much of the previous work on online deception has focused on nonstrategic behavior, the goal of which is to identify behavioral cues that signal an internal deception state. However, little research has examined the strategic behavior of online deception. Based on the underlying strategies, deception can be classified into three types: falsification (creating a fiction), concealment (hiding a secret), and equivocation (dodging the issue) [22]. For instance, many individual identity deceptions are acts of omission (e.g., concealment), rather than commission (e.g., falsification); they involve hiding one's identity [9]. Additionally, creating ambiguous statements is another strategy deceivers may use to leave targets with multiple possible interpretations [23]. Therefore, we propose the first research question as the following:

RQ1: What strategies do people use if they intend to deceive in the virtual world?

When online deception behavior is being studied, the focus is on whether deception would occur or not instead of how to measure deception qualitatively and quantitatively. There is a distinct difference between the seriousness and magnitude of deception [24-26]. Seriousness refers to severity of deception in terms of its potential negative consequence. For example, lying about one's marital status is viewed as more serious than lying about one's age in online dating [14, 24, 26]. Magnitude of deception refers to the degree of deviation from the fact. For example, the magnitude is greater if one lies about his income to be $100K than saying $80K when it is actually 60K. The two different aspects of deception can be characterized as qualitative versus quantitative differences.

Compared to the physical world, it is relatively easy to impersonate someone else online since there are relatively few identity cues to be used [9]. Galanxhi and Nah [10] suggest that "wearing a mask" in cyberspace may reduce anxiety in deceiving others. Crowell et al. [27] suggest that computer-mediated communication causes a form of altered ethical sensitivity wherein digital objects are not perceived as real objects and, at the moral level, people judge them differently. A study of lies in instant messaging (IM) [47] shows that the average magnitude of lies told in IM was close to the mid-point (2.62 in a 1 to 5 scale), suggesting that the lies researchers observed were relatively small in magnitude. So our next research question is:

RQ2: What is the magnitude of deception if people intend to deceive in the virtual world?

It is possible that despite of the similar magnitude of deception, a qualitative difference exists. For example, identity deception is considered harmless in many virtual communities [9]. In everyday life, people lie most often about their feelings, actions, plans, whereabouts, achievements, and knowledge. Most of these lies are not perceived to be serious [28]. In contrast, some deception involving exaggeration like enhancing one's resume for a job position could be relatively severe; some other deception involving serious consequences like death can be emotionally devastating [29]; financial frauds or outright lies that jeopardize national security are even more disastrous. Like the research on magnitude of deception, research that addresses the seriousness of online deception is hard to find. Do people view deception occurrences as little "white lies" [30] or more serious lies? To answer this question, we compared the perceived seriousness of deception on different issues. Small white lies should be rated less important than other lies. If lies are more damaging, they should be rated higher in seriousness. Our following research question is:

RQ3: How serious is deception perceived in the virtual world?

Deception could be attributed to privacy reasons. Several surveys confirm that Internet users generally feel differently about the disclosure of different types of information [31]. They are usually quite willing to disclose basic demographic and lifestyle information as well as personal tastes and hobbies, but less willing to disclose details about their Internet behavior and purchases, followed by extended demographic information. The disclosure of personal financial information, contact information, and specifically credit card and social security numbers raises the highest privacy concerns. Depending on the issues of deception, the seriousness and magnitude of deception could vary.

RQ4: On which kind of issues do people intend to deceive in the virtual world?

Gender and Age Effects

Research has shown that females are often perceived to be more cooperative and less exploitative than males [32]. Compared with males, females are more non-verbal oriented. Non-verbal communication conveys information outside spoken language in the form of facial expressions, gestures, body language, and eye contact [33]. However, these features have mostly been filtered out by electronic communication channels. Thus, when females choose to deceive, they may adopt different deception strategies from males.

Females also have higher expectations regarding ethics than males [34, 35]. Further, females tend to feel bad about damaging social relationships, the goal of their online participation. It has been found that females are likely to become victims to social phishing attack overall (77% versus 65% for males) [36]. Thus, females are expected to perceive deception more seriously than their male counterparts.

Compared with interacting via traditional computer-based tools, users' interaction in the virtual world requires more technical skills. There is a gender difference in technology use with males being more technical savvy [37]. Competent users deceive more than non-competent [38]. It can be inferred that males are more likely to deceive in the virtual world due to a higher level of technical expertise. Several studies have found that the overall deception rate of males could be twice as high as that of females [39, 40]. Men are also found to be more likely than women to explore and experiment with identity boundaries online [18, 41]. Therefore, we propose our fifth research question as the following:

RQ5: Do females intend to deceive differently from males in the virtual world?

It has been found that there are systematic changes, with age, in the kinds of messages that subjects perceive as deceptive [42]. Specifically, for five teenager groups ranging from the sixth grader to college students, subjects at the younger age levels judged expressions of negative affect as more deceptive than expressions of positive affect; however, this trend is reversed for the older subjects, who judged expressions of positive affect to be relatively more deceptive than expressions of negative affect. A correlation between age and the success rate of phishing attack has also been reported, with younger targets (freshman to senior) being slightly more vulnerable [36]. Thus, people's perception of deception may change with age.

Old users are less competent in computer and Internet technologies. They tend to be more responsible and more aware of the influence of deception in real-world life. Conversely, younger people feel less inhibited when interacting through a computer network because of the reduction in social cues that provide information regarding one's status in the group. Young users are found to deceive more than old users in online environments in one study [38]. Although the above findings predated the popularity of the virtual world, it motivates us to ask the last research question:

RQ6: Does age have any influence on intended deception in the virtual world?

Research Method

The target virtual world in this study was Second Life (SL) [1], which is a virtual world equipped with an advanced 3D interface and avatar system. Approximately one million people around the world log-in to Second Life every month. Those users spend a total of about 40 million hours inworld, and participate in SL's virtual economy that involved transactions worth over USD500 million in 2009. Immersed into a visually constructed environment, SL users can customize their personal avatar's appearance and put it into clothing. Also, users can initiate or join synchronous chatting via controlling a personal avatar. Further, a user can create 3D objects and sell them to other users for real profit. Aside from personal use, corporate use of Second Life has evolved from the pure marketing experiments popular in 2006 and 2007 to today's business collaboration, product demonstration and training, promoting sales, and holding virtual meetings and events. More than 1,400 organizations around the world, including universities, non-profit organizations, and large business companies are using Second Life [43].

We conducted surveys to answer the research questions. Participants were undergraduate and graduate students recruited from a mid-sized university on the east coast of the U.S. They all contributed to the study on a voluntary basis and were compensated with course credits. Participants signed an informed consent approved by IRB before responding to the survey. A total of 69 participants successfully completed the survey. Among them, 36% were males.

Before receiving the survey questionnaire, respondents were provided with a one-page description of the virtual world in general and Second Life in specific, which was followed with a short introductory video about Second Life. There are three major sections of the questionnaire. In first section, respondents were asked about their general perception of deception and deception in the virtual world. In second section, participants were asked about their attitude, perception, and intention with regard to deception in virtual worlds. Finally, respondents were asked to express their Internet experiences and computer skills, and some basic demographic information. Three constructs, including deception strategies, magnitude, and seriousness from the first section, and four variables including gender, age, internet experience, and computer experience from the last section were extracted and discussed in this research.

The survey questions were created based on previously established research instruments [44] or theories. Most of them were asked based on a 7-point Likert scale, with 1 representing “not at all” and 7 representing “extremely”). Deception strategies were asked with three options: falsification, concealment, and equivocation. Seriousness of deception is defined as “the degree to which you believe it is unacceptable to deceive on this issue.” (completely unacceptable or completely acceptable). Magnitude of deception refers to the degree of deviation from the fact. The question is stated as “SL does not make it mandatory for you to specify or discuss (certain) issues, but if it did, to what extent you would lie on the following issues in SL.” Age was split into five ranges, including under 25, 26-35, 36-45, 46-55, and over 55.

The issues on which to deceive were pre-categorized based on previous research on privacy in online social networks and online deception [26, 31]. We created seven issue categories, including physical appearance (e.g. hair color, gender, body type), social status (e.g., relationship status, occupation), interests (e.g. hobbies, musical preferences), beliefs (e.g., religious orientation, political views), identification (e.g., name, address, email), behavior (e.g., language style and internet purchase), and facts about events that I have observed.

The instruments were tested via a pilot study with undergraduate students at a large university. The selected constructs showed internal consistency levels ranging from .80 to .86, which exceeds the 0.70 alpha value suggested by [45].

Results

Table 1. Percentage Distribution of Deception Strategies

Strategies Issues	Falsification (%)	Concealment (%)	Equivocation (%)
Physical appearance	19	61	20
Social status	16	62	22
Interests	13	58	29
Beliefs	10	62	28
Identification	26	61	13
Behavior	13	58	29
Observed events	14	52	34

Deception Strategies

As shown in Table 1, the distribution of the three types of deception strategies show similar patterns across different issues, with concealment being the most popular, followed with equivocation, and finally falsification. The results indicate that, when it comes to sensitive topics, people choose to conceal information first; if it does not work, they would adopt strategic ambiguity about the issues; if both fail, they would turn to fabricating information.

Despite similar distributions, there are still distinct differences between the possible issues of deception. For example, falsification is preferred (26%) over equivocation (13%) when it comes to personal identification information. Since one is expected to know all the details about his/her own personal identity, the deceiver would easily arouse suspicion of the target by becoming ambivalent when asked for such information. Thus, compared with the other two types of deception strategies, making up a fake identity is a much safer strategy.

In contrast, the choice of equivocation is high and the choice of concealment is low for observed events relative to other issues. This suggests that, deceivers tend to speak up when it comes to issues that are not directly related to themselves, despite that details about those issues are not clearly disclosed.

Magnitude of Deception

The descriptive statistics for magnitude and seriousness of deception (ranging from 1 to 7) is reported in Table 2.

Table 2. Descriptive Statistics (mean [standard deviation]) for Magnitude and Seriousness of Deception

	Magnitude	Seriousness
Physical appearance	2.86 [1.7]	2.77 [1.6]
social status	2.60 [1.6]	3.03 [1.7]
Interests	2.12 [1.2]	2.81 [1.6]
Beliefs	1.99 [1.3]	3.12 [1.9]
Identification	4.17 [2.2]	3.29 [2.1]
Behavior	2.61 [1.7]	3.15 [1.8]
Observed events	2.29 [1.5]	3.35 [2.0]

If the respondents were to deceive on the seven issues in the virtual world, on average, the magnitude of deception would fall into the low-to-middle range (on a scale of 1 to 7). Nonetheless, there exist differences across different issues. For instance, respondents preferred to tell the biggest lies on personal identification (mean = 4.17) and the smallest lies on beliefs (mean = 1.99) such as religious orientation and political views. The next two issues that respondents prefer to tell small lies on are personal interests (mean = 2.12) and observed events (mean = 2.29). Further, it is noted that none of the respondents chose 7 for the magnitude of deception on the first four issues, namely physical appearance, social status, interests, and beliefs.

Seriousness of Deception

Interestingly, the responses on the seriousness of deception are not in line with those on the magnitude of deception. We expect that people would create “small lies” on the issues that were perceived to be serious. However, the results show that deception on personal identification, where “biggest lies” was found, was among the worst kinds of deception and was perceived as bad as deception on observed events. In contrast, among the seven issues, physical appearance and interests are the most acceptable issue for deception.

Gender and Age

To answer the question about gender effect, we compared deception strategies, magnitude, and seriousness between male and female participants.

Table 3. Descriptive Statistics for Deception Strategies, Magnitude, and Seriousness by Gender

Issues	G	Strategies (%)			Magnitude	Serious-ness
		C	E	F		
Physical appearance	F	54.5	22.7	22.7	3.0 [1.7]	2.8 [1.6]
	M	72	16	8	2.5 [1.7]	2.7 [1.6]
Social status	F	61.4	22.7	15.9	2.7 [1.6]	3.2 [1.7]
	M	64	20	16	2.4 [1.6]	2.7 [1.8]
Interests	F	52.3	29.5	18.2	2.2 [1.2]	3.1 [1.6]
	M	68	28	4	1.9 [1.1]	2.4 [1.5]
Beliefs	F	61.4	25	13.6	2.1 [1.4]	3.2 [1.9]
	M	60	32	4	1.6 [.87]	2.8 [1.8]
Identifica-tion	F	59.1	13.6	27.3	4.6 [2.2]	3.7 [2.0]
	M	64	12	24	3.4 [2.1]	2.6 [1.9]
Behavior	F	52.3	29.5	18.2	2.9 [2.0]	3.4 [1.8]
	M	68	28	4	2.1 [.99]	2.8 [1.9]
Observed events	F	52.3	29.5	18.2	2.5 [1.6]	3.5 [2.0]
	M	52	36	8	1.9 [1.1]	3.0 [1.9]

It can be observed from Table 3 that there are considerable gender differences in the use of deception strategies for physical appearance, interests, and behavior. Compared with females,

males are more likely to choose concealment and less likely to use falsification when it comes to deceiving about their physical appearance, interests, and behavior.

There is also gender difference in the magnitude of deception, with female being higher on personal identification (p<.05) and behavior (p<.1). In addition, females perceived it more serious than their male counterparts to deceive about personal identification (p<.05) and interests (p<.1).

The respondents come from all five age groups with the majority falling into the first three groups. 52.7% of participants are under 25 years old, 29.1% are between 26 and 35, and 12.7% are between 36 and 45. The results of linear regression analysis show that older respondents consider deception on beliefs (β=.249; p<0.1) and observed facts (β=.238; p<0.1) more serious than younger ones.

Discussions

Findings

The results of this study provide a number of implications. People are mindful about their deception strategies. When people consider deceiving in the virtual world, they would generally try to withhold information first, then opt for vagueness and uncertainty if withholding does not work, and finally resorting to make up information if the first two fail. Such preferences in terms of deception strategy choice are similar to what interpersonal deception theory has predicted for face-to-face communication [46].

Respondents' willingness to deceive varies with the referenced issues. It is not surprising that personal identification is what people deceive the most about. Unlike face-to-face communication, online communities are perceived as an open space with free public access. Personal identification is the key to gaining access to various kinds of information about an individual. Our finding is consistent with that of a previous study of online deception [38]. That study also shows that age and residence, which belong to personal identification information, were ranked in the top two about which deceivers gave incorrect information. Additionally, the finding of the current study also implies that, if the issues are about religious orientation and political views, people would feel it easy and even important to share true beliefs. It is because that those beliefs are intended to be shared and adopted by many other advocates.

When people decide to lie, the magnitude of deception in the virtual world did not go above the middle point (i.e., 4). In other words, people try to avoid "big lies". The result suggests that most of everyday lies may be small deception. This is different from the findings of deception in IM, with 27.6% being rated as higher than the middle point [47]. One possible explanation for the different findings lies in the difference between intended and actual behavior. Deception that is being contemplated may be perceived to be at a less extent than actual deception behavior. When deception really takes place, deceivers may feel it more important or worse than when deception is being prepared.

Similarly, the average ratings on the seriousness of deception range between 2.8 and 3.4. This suggests that people perceive it to be somewhat bad to deceive in the virtual world. In other words, the overall deception is considered neither inconsequential nor significant. Nonetheless, there exist differences in the degree of deception seriousness across different issues. On the one hand, deception on personal identification and on observed events are considered the worst. Interesting, it is noted that personal identification was also associated with the largest deception. On the other hand, physical appearance and personal interests were considered the most acceptable deception. This may have something to do with the virtual world environment. In SL, the avatars of residents would look more or less different from themselves. The difference is even greater for deceivers [10]. Virtual worlds such as SL are a type of Web-based communities [48], where residents can join groups or clubs based on common interests. It is important for a resident to express his/her interests to identify with a group. Moreover, people's interests may shift over time [49], making such deception difficult to detect and easy to succeed.

This study also finds that females tend to choose different deception strategies from males. For example, when they want to deceive, males are more likely to conceal their actual physical appearance, interests, and behavior, while females are more likely to make up information on those issues. Additionally, if they were to deceive on personal identification and behavior, females would deviate from the truth to a greater extent than males. Further, females perceived the deception on personal identification and interests more seriously. All these findings suggest that females are more sensitive than males about sharing personal information and less willing to accept deception in the virtual world. This may be due in part to that females are more vulnerable to cyber attacks [36]. Research has shown that males focus on status (e.g., success and competence) and independence while females value intimacy and social connection in their communications [50]. Therefore, males are more likely than females to defend their egos, and thus provide deceptive information, if challenged.

This study provides some preliminary evidence showing that age has positive impacts on the perceived seriousness of deception on beliefs and observed events. As people grow older, their expectations regarding ethics and cautions about possible consequences of deception increase. This potential heightening of expectations and awareness may have an influence on older respondents' low acceptance of deception, even in the virtual world. Nonetheless, the difference in perceived seriousness did not manifest itself in the magnitude of deception. This could be caused by skewness in the distribution of age groups, with the majority falling into the three groups toward the lower end.

To find out whether people's computer and Internet tenure have impacts on intended deception, we conducted linear regression analysis. The results show that daily time spent on the Internet (β=-.416; p=.056) and computers (β=.438; p=.05) have opposite effects on the magnitude of deception on personal identification. Specifically, the more time a user spent on the Internet and the less time on computers, the less extent one would deceive on his/her identification. This is likely because, as a user spends more time on the Internet, he/she would leave more traces for others to follow in countering deception. So users who are Internet addicts simply do not attempt to perpetrate deception on personal identification. Additionally, the time spent on the Internet influences the magnitude of deception on beliefs negatively (*β*=-.441; *p*=.031), and Internet skills affects the magnitude of deception on behavior positively (*β*=.321; *p*=.066). The latter suggests that, with a higher level of user competence [38], skilled Internet users are more likely to deceive than novice users.

Implications

This study suggests that the virtual world does not necessarily produce the results like other online communication media. In the past few years, deception has attracted increasing public attention, which has also increased public awareness of online deception. We explored the perception of deception in the virtual world through a survey in this study. The results indicate that users differentiate among different types of deception when it comes to communication in the virtual world. In addition, the finding that users expect deception to have different levels of seriousness suggests that deception has varying consequences depending on the motivations of deception.

The findings of this study also have implications to online deception research. The detection of deception relies on the leakage of behavioral cues, which in turn is driven by the underlying deception strategies. For instance, short and/or irrelevant messages could exemplify the concealment strategy. In contrast, falsification could lead to long messages or messages that lack expressions of perceptions or specific information. Therefore, understanding deception strategies can help us choose the most effective cues to deception, which in turn improves the performance of deception detection. Moreover, the predominance of concealment in the choice of deception strategies in SL suggests that deception theories should be adapted to account for the communication context in the virtual world.

The seriousness and magnitude of deception are found to be independent of each other. In other words, although some kinds of deception are perceived to be relatively severe, people still choose to create "big lies". This could be the result of weighing conflicting goals. For example, if personal identification is at risk for misuse, one may have to bend his value system by giving way to deception. Therefore, perceived seriousness alone cannot explain intended deception. Instead, perceived risks, which take into account of subjective assessment of negative or unexpected consequences that one fears may occur as a result of providing true information [51], may be a better predictor for online deception.

The impact of gender on deception has implications for the development of deception detection tools. If the suspect is a female, the content of her deception would be more distant from the truth and less uncertain than a man. This is attributed to females' higher preference for falsification strategy and lower preference for concealment than men.

Limitations

This study exposes several limitations. First, the participants were university students and most of the graduate students were working professionals. The survey respondents may not truly represent the virtual world population. Second, this survey was conducted prior to the respondents' adoption of SL to assess their perceptions. It would be interesting to ask SL residents about their actual deception behavior after they have interacted with others in SL. Nonetheless, given the well-recognized problems associated with self-reported measures, especially on sensitive subjects like deception, it would be easier to measure perception than measure actual behavior. Additionally, the introduction of virtual worlds and SL in both text and video has oriented the respondents to a relatively complete picture of the virtual world.

Third, this study is exploratory in nature, which does not directly provide explanations for deception behavior.

Conclusion and Future Research

This study not only provides a preliminary understanding of deception in the virtual world in general but also looks into specific aspects of deception, including deception strategy, seriousness, and magnitude. Additionally, it investigates whether intended deception and deception perception vary with gender and age.

The research can be continued in a number of directions. First, it is worth conducting a longitudinal study to investigate whether and how deception perception and deception intent change as respondents' experience with the virtual world increases. Second, future research is recommended to examine typical motivations of online deception (e.g., benefiting someone vs. malicious). Third, the categorization of deception issues could be refined with regard to deception seriousness. Ultimately, we expect to develop theories that can explain why and how people deceive in online environments such as the virtual world.

References

[1] http://secondlife.com/.

[2] D. Zhang and P. Shrestha, "Doing Business in Second Life: e-Commerce in a 3D Online Environment," *International Journal of electronic Business,* vol. 8, pp. 148 - 169, 2010.

[3] F. Sudweeks and S. Simoff, "Culturally commercial: a cultural e-commerce framework," in *OZCHI*, Fremantle, Western Australia, 2001, pp. 148–153.

[4] A. Davis, J. Murphy, D. Owens, D. Khazanchi, and I. Zigurs, "Avatars, people, and virtual worlds: foundations for research in metaverses," *Journal of the Association for Information Systems,* vol. 10, 2009.

[5] S. Grazioli and S. L. Jarvenpaa, "Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers," *IEEE Transactions on Systems, Man and Cybernetics,* vol. 30, pp. 395-410, July 2000 2000.

[6] A. Hummerston, "Digital world, digital life" TNS Global Interactive, http://www.tnsglobal.com/_assets/files/TNS_Market_Research_Digital_World_Digital_Life.pdf, accessed in July 2010.

[7] N. C. Rowe, "The Ethics of Deception in Virtual Communities," 2005.

[8] J. Matusitz, "Deception in the Virtual World: A Semiotic Analysis of Identity," *Journal of New Media & Culture,* vol. 3, 2005.

[9] J. S. Donath, "Identity and deception in the virtual community," in *Communities in Cyberspace,* M. A. Smith and P. Kollock, Eds.: Routledge, 1999, pp. 29-56.

[10] H. Galanxhi and F. F.-H. Nah, "Deception in cyberspace: A comparison of text-only vs. avatar-supported medium," *International Journal of Human-Computer Studies,* vol. 65, pp. 770-783, September 2007.

[11] J. R. Suler, "Do boys and girls just wanna have fun?," in *Gender Communication*, A. Kunkel, Ed.: Kendall/Hunt Publishing, 2004.

[12] L. Zhou, J. K. Burgoon, J. F. Nunamaker, and D. Twitchell, "Automated linguistics based cues for detecting deception in text-based asynchronous computer-mediated communication: An empirical investigation," *Group Decision & Negotiation,* vol. 13, pp. 81-106, 2004.

[13] J. T. Hancock, J. Thom-Santelli, and T. Ritchie, "Deception and design: The impact of communication technologies on lying behavior," in *ACM Conference on Computer Human Interaction*, Vienna, Austria, 2004, pp. 129-134.

[14] J. F. George and J. R. Carlson, "Media selection for deceptive communication," in *Hawaii International Conference on System Sciences*, Big Island, HI, 2005.

[15] A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model," *IEEE Transactions on dependable and secure computing,* vol. 5, pp. 37-48, 2008.

[16] C. E. H. Chua, J. Wareham, and D. Robey, "The role of online trading communities in managing Internet auction fraud," *MIS Quarterly*, vol. 31, pp. 759-781, 2007.

[17] J. R. Carlson, J. F. George, J. K. Burgoon, M. Adkins, and C. White, "Deception in Computer-Mediated Communication," *Group Decision and Negotiation,* vol. 24, pp. 5-28, 2004.

[18] S. Utz, "Types of Deception and Underlying Motivation: What People Think," *Social Science Computer Review,* vol. 23, pp. 49-56, 2005.

[19] L. Zhou and D. Zhang, "A Comparison of Deception Behavior in Dyadic and Triadic Group Decision Making in Synchronous Computer-mediated Communication," *Small Group Research,* vol. 37, pp. 140-164, April 2006.

[20] L. Zhou, D. Twitchell, J. Burgoon, T. Qin, and J. Nunamaker, "A comparison of classification methods for predicting deception in computer-mediated communication," *Journal of Management Information Systems,* vol. 20,

pp. 139-165, 2004.

[21] D. B. Buller and J. K. Burgoon, "Interpersonal Deception Theory," *Communication Theory,* vol. 6, pp. 203-242, August 1996 1996.

[22] D. B. Buller, J. K. Burgoon, C. H. White, and A. S. Ebesu, "Interpersonal Deception VII: Behavioral Profiles of Falsification, Equivocation, and Concealment," *Journal of Language and Social Psychology,* vol. 13, pp. 366-395, 1994.

[23] E. M. Eisenberg, "Ambiguity as strategy in organizational communication," *Communication Monographs,* vol. 51, pp. 227–242, 1984.

[24] J. T. Hancock, C. Toma, and N. Ellison, "The truth about lying in online dating profiles," in *Proceedings of the SIGCHI conference on Human factors in computing systems* San Jose, California, USA: ACM, 2007.

[25] J. F. George, K. Marett, and P. Tilley, "Deception Detection under Varying Electronic Media and Warning Conditions," in *Hawaii International Conference on System Sciences*, Big Island, HI, 2004.

[26] C. C. Lewis and J. F. George, "Cross-cultural deception in social networking sites and face-to-face communication," *Computers in Human Behavior,* vol. 24, pp. 2945-2964, September 2008.

[27] C. R. Crowell, D. Narvaez, and A. Gomberg, "Moral Psychology and Information Ethics: Psychological Distance and the Components of Moral Action in a Digital World," in *Information Ethics: privacy and intellectural property*, L. A. Freeman and A. G. Peace, Eds. Hershey, PA: Information Science Publishing, 2005, pp. 19-37.

[28] B. M. DePaulo, D. A. Kashy, S. E. Kirkendol, M. M. Wyer, and J. A. Epstein, "Lying in everyday life," *Journal of personality and social psychology,* vol. 70, pp. 979–995, 1996.

[29] S. Brundage, "Playing with death," in *Computer Gaming World*, 2001, pp. 29-31.

[30] M. Vanden Abeele and K. Roe, "White cyberlies: The use of deceptive instant messaging statuses as a social norm," in *the Conference of the International Communication Association*, Montreal, Canada, 2008.

[31] A. Kobsa, "Privacy-enhanced Web personalization," in *The Adaptive Web: Methods and Strategies of Web Personalization*, P. Brusilovsky, A. Kobsa, and W. Nejdl, Eds. Verlag: Springer, 2007, pp. 628--670.

[32] A. F. Stuhlmacher and A. E. Walters, "Gender differences in negotiation outcome: A meta-analysis," *Personnel Psychology,* vol. 52, pp. 653-677, 1999.

[33] R. G. Harper, A. N. Wiens, and J. D. Matarazzo, *Non-verbal communication: The state of the art*. New York: John Wiley & Sons, 1978.

[34] C. McDaniel, N. Shoeps, and J. Lincourt, "Organizational Ethics: Perceptions of Employees by Gender " *Journal of Business Ethics,* vol. 33, October 2001.

[35] P. Tilley, J. F. George, and K. Marett, "Gender Differences in Deception and Its Detection under Varying Electronic Media Conditions," in *the 38th Annual Hawaii International Conference on System Sciences*, 2005.

[36] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," *Communications of the ACM,* vol. 50, pp. 94-100, 2007.

[37] L. A. Jackson, Y. Zhao, W. Qiu, I. Anthony Kolenic, H. E. Fitzgerald, R. Harold, and A. v. Eye, "Culture, gender and information technology use: A comparison of Chinese and US children." vol. 24: Elsevier Science Publishers B. V., 2008, pp. 2817-2829.

[38] A. Caspi and P. Gorsky, "Online Deception: Prevalence, Motivation, and Emotion," *CyberPsychology & Behavior,* vol. 9, pp. 54-59, Feb. 2006.

[39] D. Koehn, "Rewriting history: Resume falsification more than a passing fiction," *Houston Business Journal,* vol. 30, p. 30, 1999.

[40] T. Prater and S. B. Kiser, "Lies, lies, and more lies," *SAM Advanced Management Journal,* pp. 9–36, Spring 2002.

[41] N. I. Bowker, "Understanding Online Communities Through Multiple Methodologies Combined Under a Postmodern Research Endeavour," *Forum: Qualitative Social Research,* vol. 2, February 2001.

[42] B. M. DePaulo, A. Jordan, A. Irvine, and P. S. Laser, "Age Changes in the Detection of Deception," *Child Development,* vol. 53, pp. 701-709, June 1982.

[43] P. Linden, "M Linden's Interview with the BBC," 2009.

[44] N. K. Choudhry, R. H. Fletcher, and S. B. Soumerai, "Systematic review: The relationship between clinical experience and quality of health care," *Annals of Internal Medicine,* vol. 142, pp. 260–273, 2005.

[45] J. C. Nunnally, *Psychometric Theory*. New York: McGraw-Hill Book Co., 1978.

[46] J. K. Burgoon, D. E. Buller, L. K. Guerrero, W. A. Afifi, and C. M. Feldman, "Interpersonal Deception: XII. Information management dimensions underlying deceptive and truthful messages," *Communication Monographs,* vol. 63, pp. 50-69, March 1996.

[47] J. Hancock, J. Birnholtz, N. Bazarova, J. Guillory, J. Perlin, and B. Amos, "Butler lies:

awareness, deception and design," in *Proceedings of the 27th international conference on Human factors in computing systems* Boston, MA, USA: ACM, 2009.

[48] J. Bishop, "Enhancing the understanding of genres of web-based communities: The role of the ecological cognition framework," *International Journal of Web-Based Communities,* vol. 5, 2009.

[49] L. Wai and M. Javed, "Modeling user interest shift using a bayesian approach," *Journal of the American Society for Information Science and Technology,* vol. 52, pp. 416-429, 2001.

[50] D. Tannen, *You Just Don't Understand: Women and Men in Conversation*, 1st ed. New York: Ballantine Books, 1990.

[51] P. Slovic, "Perception of risk: Reflections on the psychometric paradigm," in *Social theories of risk,* S. Krimsky and D. Golding, Eds. New York: Praeger, 1992, pp. 117-152.