Information Processing and Management 53 (2017) 21–41

Contents lists available at ScienceDirect

Information Processing and Management

journal homepage: www.elsevier.com/locate/infoproman

Gender deception in asynchronous online communication: A path analysis

Shuyuan Mary Ho[a,*], Paul Benjamin Lowry[b], Merrill Warkentin[c], Yanyun Yang[d], Jonathan M. Hollister[e]

[a] School of Information, College of Communication and Information, Florida State University, 142 Collegiate Loop, P.O. Box 3062100, Tallahassee, FL 32306-2100, USA
[b] Innovation and Information Management, School of Business, Faculty of Business and Economics, The University of Hong Kong, K. K. Leung Building, Hong Kong, China
[c] Information Systems, Dept. of Management and Information Systems, College of Business, Mississippi State University, P.O. Box 9581, Mississippi State, MS 39762-9581, USA
[d] Department of Educational Psychology & Learning Systems, College of Education, Florida State University, Stone Building 3204 K, P.O. Box 3064450, Tallahassee, FL 32306-4450, USA
[e] Information Institute, College of Communication and Information, Florida State University, 142 Collegiate Loop, P.O. Box 3062100, Tallahassee, FL 32306-2100, USA

ARTICLE INFO

Article history:
Received 15 February 2016
Revised 30 April 2016
Accepted 10 June 2016
Available online 29 August 2016

Keywords:
Human computer interaction
Computer-mediated deception
Human information behavior
Gender, deception
Online game

ABSTRACT

Gender is a salient feature of identity that is rarely questioned in our physical encounters. We are usually not confused about a person's gender—generally it's male or female. However, as the adoption of computer-mediated communication increases, our social reliance on these technologies has made gender easily disguised online. And yet, the phenomenon of gender deception has not been fully investigated. This study adopts a path analysis to examine interconnected cognitive factors that impact online users' ability to deceive—and detect deception—regarding gender. An asynchronous online game was developed to simulate situations where males were incentivized to communicate like females, and females were incentivized to communicate like males. Twelve hypotheses were tested using path analysis, which resulted in our realization that an actor's true gender can affect the motivation to deceive; males tend to have higher self-efficacy beliefs in gender deception, and females tend to have a higher success rate in detecting gender deception. Our research suggests that the gender of the message recipient could be a significant factor in uncovering gender deception.

1. Introduction

Online users must frequently make judgments or decisions based on computer-mediated interaction. It is common for individuals to receive emails with hypertext links or a popup messages from a website, or be asked to confirm or cancel some electronic procedure. Many online users receive phishing emails[1] requesting personal or sensitive information, or seeking a

* Corresponding author. Fax: 850.644.9473, Website: ischool.cci.fsu.edu.
E-mail addresses: smho@acm.org, smho@fsu.edu (S.M. Ho), Paul.Lowry.PhD@gmail.com (P.B. Lowry), m.warkentin@msstate.edu (M. Warkentin), yyang3@fsu.edu (Y. Yang), jmh09k@my.fsu.edu (J.M. Hollister).

[1] Phishing emails are sent out as one-to-many asynchronous online communication, which is to contrast the synchronous online chat communication.

http://dx.doi.org/10.1016/j.ipm.2016.06.004
0306-4573/

response (Wright & Marett, 2010). Phishing emails may also induce actions such as answering inquiries about social, financial, or business relationships, or confirming social media friend requests, resulting in online gender fraud (Brady & George, 2013). Repeatedly, online users must determine whether the source of a message is credible and legitimate (Hilligoss & Rieh, 2008; Liu, 2004; Rieh, 2002) in order to maintain privacy and safety (Lopez & Sebe, 2013; Twyman, Lowry, Burgoon, & Nunamaker, 2014).

A rise in the threat of deceptive communications has accompanied the increased reliance of individuals and organizations on computer-mediated communication (CMC[2]) systems. In a *New York Times* interview, Bruce Schneier, an American cryptographer, states that trust is "the glue that binds our societies" and deceptive communications in the digital age have destroyed this trust (Sengupta, 2012, p.1). Because virtual space lacks traditional face-to-face (FtF) visual cues of deception, it has become easier for online users to misrepresent not only the content of their messages but their identities. As technology changes the way we interact socially, it becomes ever more difficult to discern whether an email from our bank is authentic, and how much we can trust authorities with our online privacy. This threat of deception has been shown to be substantial in various domains and manifests in many ways, such as phishing and "spear phishing" attacks (Wright & Marett, 2010), deception in electronic commerce (Xiao & Benbasat, 2010), deception at workplace (da Cunha, Carugati, & Leclercq-Vandelannoitte , 2015), deception in group support systems (George, Marett, & Giordano , 2008), deception in professional virtual communities (Joinson & Dietz-Uhler, 2002), deceptive opinions in online reviews (Fusilier, Montes-y-Gomez, Rosso, & Cabrera, 2015; Ott ,Cardie, & Hancock, 2012), deception in 911 calls (Burns & Moffitt, 2014), deception in social media relationships (Hancock, Toma, & Ellison, 2007; Hancock, Woodworth, & Goorha, 2010; Zhou, Burgoon, Twitchell, Qin, & Nunamaker, 2004), deceptive opinions and reviews (Ott, Cardie, & Hancock 2012, 2013; Ott, Choi, Cardie, & Hancock, 2011), deception in story-telling (Rubin, 2010), and fake news (Conroy, Rubin, & Chen 2015). The consequences of successful deception range from harmless inconvenience to significant costs. Such deception can pose a major threat when it drives online transaction fraud (Twyman, Lowry, Burgoon, & Nunamaker, 2014), identity theft, theft of credentials, theft of intellectual property, or threats against national security.

One salient dimension of online deception is users' misrepresentation of their gender (Ho & Hollister, 2013). One's gender, which has been traditionally considered binary due to distinct biological differences at birth, has a tendency to be socially reconstructed (Bussey & Bandura, 1999). Bussey and Bandura (1999) suggested that gender roles are constantly being reconstructed by a broad network of peers and societal influences. Gender and gender role development are constantly mixed with experience and motivation. People's self-development can redefine their gender identity (e.g., recognition or realization of being gay), which eventually contributes to social change (e.g., legalization of gay marriage). Regardless of these social impacts, users' online identities are continually being constructed by a number of factors, including their redefined gender roles, their motivations, self-efficacy, social interactions with friends and colleagues, as well as personal desires and goals. The binary view of gender creates fundamental representation problems. Rodino (1997), for instance, observed inconsistencies in online chatters' language and presentation of their gender, and suggested that gender can be "performed" in an online environment. In other words, gender can be made more real and natural in virtual, imaginative communication. Gender, through linguistics, can be socially "constructed," and online actors may falsify the representation of gender to increase the probability of gaining trust.

Gender can represent a unique feature of online deception in that it can involve fairly nuanced clues and circumstances that one may not normally consider. In asynchronous online communication, individuals may attempt to misrepresent their gender, and recipients of online messaging may lack the ability to identify the gender of their communicators. Regardless of the reasons people may attempt to deceive others about their gender, empirical results show that 18% of males and 11% of females have lied about their gender (Whitty, 2002, p. 348) at some point when engaging in text-based communication. Gender deception can be highly disturbing to both males and females who have been deceived (Stieger, Eichinger, & Honeder 2009). Previous research has found gender-related influences, in the ways males and females communicate—in both FtF and online communication (Herring, 2000; Herring & Martinson, 2004; Savicki, Kelley, & Oesterreich, 1999; Whitty, 2002). Yet, little is understood about the role of gender deception in the complexity of computer-mediated deception. As gender misrepresentation or gender deception has become a major contributing factor in identity fraud, our research intends to explore, describe, and explain different cognitive factors that facilitate gender deception in computer-mediated communication. Our overarching research question is thus set as follows: *How are the cognitive factors of gender deception modeled in asynchronous online communication*?

That said, online users can adapt in ways that extenuate or diminish certain facets of their identities (including their gender) in certain social situations depending on social goals, conversational topics, context, or cultural situations (Herring, 1995, 2000). In other words, depending on the context and topic, it is possible for males to adjust their communication toward female styles, and females can employ communication style more like male utterances in order to disguise their true gender. This paper outlines our investigation to first review deception in FtF interaction as well as online communication when facilitated by computer-medicated technologies. Twelve research hypotheses—examining motivation and self-efficacy of both message senders and receivers that impact the outcome of deception—are discussed within the framework of gender deception. We then discuss our research design and considerations for an experiment deployed in the form of an online

[2] CMC broadly includes both synchronous (e.g., chat) and asynchronous (e.g., texting, email, etc.) communication.

game that mimics online users' asynchronous interactions. We address data collection and analysis to test our hypotheses. Contribution, limitations, and future research are discussed thereafter to conclude this paper.

2. Revelant background

Before we discuss our theoretical framework and hypotheses, we will review the research on FtF and computer-mediated deception.

2.1. Key deception research

Deceptive practices are frequently used to mislead a message recipient, and can take the form of fabrication, denial, omission, or exaggeration (Ebesu & Miller, 1994). Deceptive communication cues, such as the movements of eyes and lips, can be observed in FtF interactions (Ekman, 2009). But in general, humans are poor detectors of deception (Ekman & O'Sullivan, 1991). Research demonstrates that the probability of the general public detecting lies ranges from 50% to 58% (Frank, Paolantinio, Feeley & Servoss, 2004). However, the problem of detection is more complex than we think. Some studies have pointed out that message receivers are likely to be consciously aware of the potential for deception, and raise doubts when being deceived (Anderson, DePaulo, Ansfield, Tickle, & Green, 1999; DePaulo, 1994). DePaulo (1994) stressed that people can generally distinguish truth from lies, but that their ability to do so often varies based on the communication topic and context. Participants' confidence, as well as cognitive and affective factors influence the accuracy of their perceptions in the context of both honest and dishonest communications (Buller & Burgoon, 1996; Hurd & Noller, 1988). Furthermore, Anderson et al. (1999) claimed that linguistic cues (e.g., verbal cues) are referenced more frequently in the context of truthful communications, whereas nonverbal cues are often referenced in the context of deceptive communications.

Burgoon and Buller (1994) proposed that the interactions between participants, as the base of interpersonal deception theory (IDT), is a factor that complicates the deception phenomenon in which the interpersonal nature of deceptive (vs., truthful) behaviors requires that deception be an iterative and interactive process. Buller and Burgoon (1996) further explained the strategic process of deceptive communication based on their observations of deceivers' message content. For instance, a deceiving communicator's words and statements tend to be vague and uncertain because a deceiver may not have sufficient detailed information. In making a fabricated statement, the deceiver tends to be consciously disassociated from the act of deception. The deceiver seeks to influence the receiver's behavior, which in turn affects the strategy for how deceptive messages are delivered. In testing IDT, Buller, Burgoon, Buslig, & Roiger (1996) found that there was more variability than stability in the deceptive strategies and behaviors employed. Although some tests of this theory have relied on leakage cues (e.g., visual and tactile cues), others have uncovered the presence of *verbal* cues that may also be useful in detecting deception (Zhou, Shi, Zhang, & Sears, 2006; Zhou, Twitchell, Qin, Burgoon, & Nunamaker, 2003). And Buller et al. (1996) maintained that complex cognitive factors can cause a deceiver to leak the truth via verbal or nonverbal cues, despite covert intent.

Deception can be initiated for profit (e.g., identify fraud) or for convenience (e.g., Butler lie) (Hancock et al., 2009). To better understand how motivation affects deceptive activity, Gneezy (2005) offered a perspective on deception from the standpoint of consequences, or the balance between harm and reward. He categorized the tactics used for deception into four levels of consequences: (1) lies that benefit both deceiver and deceived (e.g., white lie), (2) lies that benefit the deceived person, possibly at the expense of the deceiver, (3) lies that harm the deceived but not the deceiver, and (4) lies with potential reward for the deceiver increases as the benefit for the deceived decreases. Gneezy (2005) found that as the cost to the deceived increases, the deceiver is less motivated to lie. This finding was further confirmed by Dreber and Johannesson's (2008, p. 198) experiment of gender differences in deception regarding economics settings that 55% of men versus 38% of women ($p = .032$) lied to secure a higher reward. Men tend to lie about their socio-economic status (Whitty, 2002), and monetary benefit (Dreber & Johannesson, 2008; Erat & Gneezy, 2011) than women. Motivation to deceive is not only found in cost/ reward calculation, but in other aspects of cognition, such as to falsely represent the self-image (DePaulo, 1992; DePaulo, Kashy, Kirkendol, Wyer, & Epstein, 1996). Toma, Hancock, & Ellison (2008) for example reported in their online dating study that males lie more about their height, and females lie more about their weight. Females employ higher levels of deception in misrepresenting themselves in photographs than do males (Lo, Hsieh, & Chiu, 2013), but males also tend to exaggerate their positive characteristics in computer-mediated communication (Guadagno, Okdie, & Kruse, 2012). Both genders strategically represent or even exaggerate their self-image online to facilitate romantic relationships.

2.2. Computer-Mediated deception

Online actors may use computer-mediated technologies to support their social presence, to enhance communication quality (Nowak, 2003), and to have a positive impact on trust within decision-making groups (Lowry,Zhang, Zhou, & Fu, 2010). Computer-mediated deception typically occurs when an online actor sends text messages[3] in an effort to create false beliefs (Buller & Burgoon, 1996; Buller et al., 1996; Zhou, Burgoon, & Twitchell, 2003). However, the ability to detect computer-mediated deception is generally constrained by lacks of ground truth verification (or, a truthful baseline history) to which

[3] Our assumption is that spoken words in the F2F communication are equivalent to text-based communication.

potential deceptive communications can be compared. Although deceptive communication cues in FtF interactions (e.g., eyes rolling and lips moving etc.) are not present in text-based online environments, research supports that certain linguistic cues may indicate deceptive intent (e.g., the use of self-reference, negation, exclusivity, cognitive mechanism, affective, or social process) (Hancock et al., 2009; Hancock et al., 2010).

Online actors may also construct their identity through conveying relevant information in an online profile, or by using visual avatars and/or textual references. Research has found that people are motivated by "play" to engage in deceptive online environments (Caspi & Gorsky, 2006). People enjoy the sense of excitement that accompanies engaging in online deception such as a Butler lie (Hancock et al., 2009), or griefing[4] strategies (Rubin & Camm, 2013). In online dating profiles, deception can frequently be identified in daters' photographs and communicative cues (Guadagno et al., 2012; Hancock et al., 2007; Hancock et al., 2010; Toma et al., 2008). Despite the fact that users can be suspicious of the authenticity of a dater's visual self-presentation in photographs (Hancock et al., 2009; Toma et al., 2008), they still participate in online dating (Hancock et al., 2007; Lo et al., 2013; Toma & Hancock, 2010; Toma et al., 2008).

Whitty, Buchanan, Joinson, & Meredith, (2012) further differentiated the significance of deception based on various modes of communication. Deception occurring in everyday life tends to be spontaneous (DePaulo et al., 1996; Whitty et al., 2012). In order to avoid discomfort, deceivers tend to choose text-based social media where the cues of daily self-presentation are not available (Hancock, Thom-Santelli, & Ritchie, 2004). On the other hand, the media richness theorists believe that deceivers prefer to use media that can give out conflicting cues. The richer the media is, the easier it is for the deceivers to disguise their deceptive intent (Daft,Lengel, & Trevino, 1987; Trevino, Lengel, Boodensteiner, Gerloff, & Muir, 1990; Trevino, Lengel, & Daft, 1987). Hancock et al. (2004) further proposed a feature-based model, and suggested that deception tends to occur in a synchronous, non-recordable, and distributed (i.e., not co-located) environment facilitated by computer-mediated technologies. Ho, Hancock, Booth, Liu, et al. (2016); Ho, Hancock, et al. (2015) simulated online deception in a synchronous communication mode, and proposed that language-action cues can effectively identify spontaneous deception. Ho, Liu, et al. (2016) moreover suggested that a machine learning approach could automate the detection of interpersonal deception in synchronous communication mode. Furthermore, Ho, Hancock, Booth, Burmester, et al. (2016); Ho, Fu, et al. (2015) identified cognitive- and affect-based language-action cues to detect deceptive intent in computer-mediated group communication.

Nonetheless, the above deception research did not consider the phenomenon of gender deception and gender fraud as depicted by the case of Manti Te' o (cf., Brady & George, 2013). The popular American football player was the victim of a long-term online gender fraud regarding a woman who never existed. Te' o told the world that his "girlfriend," Kekua (a fictitious name), had died in a car accident, but it was later disclosed that there was no Kakua and the communications were, in fact, from a male who perpetuated a hoax. The deceiver adopted the communication styles and the cognitive aspects of the opposite gender to deceive the other conversational partner. This catfish story is an extreme case where gender is the object of deception, and an activity commonly found in online dating communications.

Beyond the undesirable consequences of gender deception in the context of online dating, more serious threats exist when gender misrepresentation is used to gain trust for the purposes of social engineering, identity theft, or phishing attacks (Tsikerdekis & Zeadally, 2014). Eckel and Grossman (2008) found support that both men and women trust women more than they do men. Based on this logic, if message senders would represent themselves as female, they would increase the perception of their trustworthiness. The case of the "Nigerian Scam," where deceptive phishing emails (offering large sums of money after an initial transfer of funds) were sent purporting to be from the wife or widow of an African leader, is an example of gender deception. While money can be a motivational trigger for deception, there is a tendency displayed in how a deceiver manipulates perception of gender, subject of interest, and communication medium (in this case, email as an asynchronous online communication). Moreover, a message receiver's ability to detect gender deception is crucial, but consequently influenced by the deceivers' motivation and self-efficacy in imitating the opposite gender. Unfortunately, there has been a lack of empirical research regarding cognitive factors that influence a deceiver's ability to deceive as well as a message receiver's ability to detect gender deception. These factors affecting computer-mediated deception in terms of gender manipulation for deception have yet to be fully explored.

3. Theory and hypotheses

Deception is established as the dependable variable in our framework, which is hypothetically detectable in social communication. Our research model, based on these theoretical considerations, is illustrated in Fig. 1. This model identifies several critical factors as independent (predictor) variables that may affect the success of gender deception and successful detection of gender deception. Gender is depicted as independent variables, which includes: (1) "(s)Gender" referring to the message sender's gender, (2) "(d)Gender" referring to the detector's gender, and (3) "(p)Gender" referring to the perceived gender of the message sender by the detector. This model also includes actors' cognitive factors, such as self-efficacy and motivation as independent variables to predict the act of deception. To be specific, "(s)Self-Efficacy" refers to the message sender's self-efficacy and "(d)Self-Efficacy" to the detector's self-efficacy.

[4] An act of play intended to cause grief to game players.

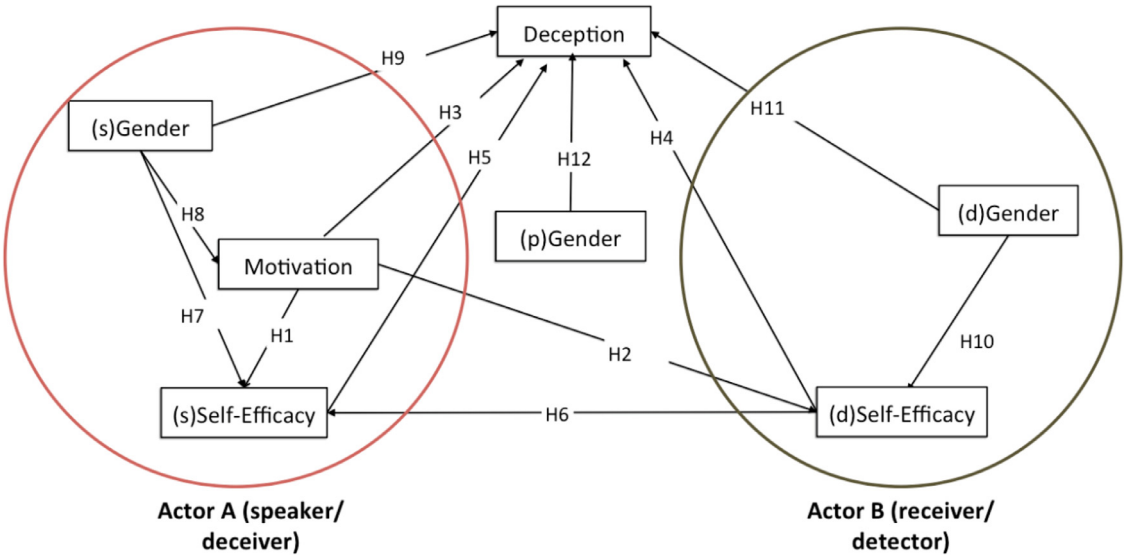

Fig. 1. Proposed Model of Gender Deception in Asynchronous Online Communication.

3.2. Motivation and self-efficacy of deception

Deceivers' motivations may relate to their level of confidence, or self-efficacy, which is their *ability* to deceive. Simply stated, self-efficacy constitutes an individual's beliefs about his or her capability to perform a certain task (Bandura, 1977, 1986, 2006). One may be motivated to accomplish an anticipated outcome but still lack confidence in one's ability to do so. That is, lacking confidence in one's ability to deceive may make one less likely to engage in deception. Bandura (1977) stated that these perceived outcomes may act as motivators for further action and that "self-motivation involves standards against which to evaluate performance" (p. 193). More specifically, self-reflection and evaluation in terms of one's ability to deceive can produce a standard or baseline of performance that influences whether a deceit will be a success.

DePaulo, Kirkendol, Tang, & O'Brien, (1988) proposed the motivational impairment effect (MIE), in which highly motivated liars tend to be less successful in deceiving others, especially when others can observe their nonverbal deceptive cues. This study also found that women tend to show more MIE than men, and those more attractive speakers are less susceptible to the MIE than less attractive speakers. Because their study was conducted with video recordings, the degree of speakers' attractiveness may have influenced the observers' judgment. However, Burgoon and Floyd (2000) conducted a study on both verbal and nonverbal styles, empirically capturing the deceiver's performance and the observer's accuracy, and argued that motivation provides limited support to the MIE hypotheses. Similarly, Hancock et al. (2010) discovered that highly motivated deceivers were more successful in their deceptions within text-based online environments. Thus, we assume that motivation can be a predictive factor but may not be a strong predictor of self-efficacy beliefs and the ability to deceive in the context of asynchronous online communication. We hypothesize that:

H1. The higher the motivation of message senders to deceive, the higher their self-efficacy beliefs.
H2. The higher the motivation of message senders to deceive, the higher their self-efficacy to detect others' online gender deception.
H3. The higher the motivation of message senders to deceive, the easier it is for them to deceive others about their true gender.

Bandura (1977) suggested that the perceived outcomes of actions or behaviors may serve as motivators. However, he noted that there is a necessary difference between outcome expectations and efficacy expectations. Efficacy expectations refer to the beliefs that an individual can actually perform the action or behavior needed to accomplish the desired outcome. Outcome expectations refer to an individual's belief that a particular behavior will have a particular result (Bandura, 1977). Although self-efficacy can influence behavioral outcomes, it is not the sole determinant of behavior, and does not alone produce the desired performance. Self-efficacy is a cognitive expectation generated from four sources of information: first, self-instructed performance, or personal mastery experiences; second, another's performance, which can influence an individual's perception of his or her own performance; third, verbal persuasion from others; and fourth, self-emotional arousal (Bandura, 1977). These information sources influence three interrelated dimensions of self-efficacy: magnitude of the task (or task difficulty), strength of conviction in the belief, and level of task-specific confidence (Bandura, 1977).

Regardless of the magnitude of the task, self-efficacy beliefs are critical to the success, or the attempts at success (Bandura, 1977, 1986, 2006) of the gender deception. As we further consider the correlation among self-efficacy of the

detector (i.e., message recipient) in relation to the success of the gender attribution, and self-efficacy of the message sender in relation to the success of the gender imitation, we hypothesize that:

H4. The higher the self-efficacy beliefs of detectors, the easier it is for them to identify online gender deception.
H5. The higher the self-efficacy beliefs of message senders, the higher their chances of succeeding in online gender deception.

Considering the generalizability dimension of self-efficacy, confidence in one's behavior (or, a set of skills) may be positively associated with confidence in other behaviors (Bandura, 1977). Bandura (2006) further stated that cultivated, higher self-efficacy in one area or skill may be transferable to other areas and skills. Accordingly, high self-efficacy beliefs regarding the attribution of correct gender (or, more specifically, the detection of gender deception) may be positively associated with high self-efficacy beliefs regarding gender imitation and/or deception. Thus, we hypothesize that:

H6. The higher one's self-efficacy in attributing correct gender, the higher one's self-efficacy in gender deception.

3.3. Gender-based Communication, motivation and efficacy

The extensive research on the psychological, social, and biological differences between males and females (conducted mostly in the context of Western cultures) supports the position that, in general, males and females exhibit significant differences in their use of language. Holmes (1988); (1995) argued that women tend to be more polite, give more compliments, reference their emotions more often, use more tentative language, and ask more questions, whereas men tend to be more opinionated, refer (or defer) more often to facts (Mulac,Bradac, & Gibbons, 2001; Mulac, Lundell, & Bradac, 1986), and use more direct forms of speech (Mulac et al., 2001; Mulac, Wiemann, Widenmann, & Gibson, 1988). Similar linguistic patterns have been found in electronic discourse, specifically in written text (Herring, 1995). Herring (1995) found many linguistic features that serve as clues to one's gender in FtF environments can also serve as salient cues in online communications: verbosity, assertiveness, use of profanity, politeness (and rudeness), types of representations of smiling and laughter, and degree of interactive engagement. Thomson and Murachver (2001) found that participants could accurately identify a conversational partner's gender based on gendered-linked linguistic features and styles.

The extent to which people use gender-linked language in cue-lean asynchronous online communication (e.g., email, blog, or text) has been characterized as lacking social presence (Nowak, 2003). Herring (1995) conducted a study of men and women's conversation on academic electronic bulletin boards and found interesting differences in terms of participation levels (men were more active and assertive) and linguistic style (women emoted more). Herring (1995) characterized men as being more forceful in their assertions, more self-promoting, presumptuous, rhetorical, authoritative, and confrontational, and exhibiting more humor and sarcasm. Women, by contrast, were more tenuous and apologetic in their assertions, made more justifications, asked more questions, were more personal and supportive of others, and tended toward language that maintains rapport. Nowak (2003) reported that women tended to exhibit more social presence than men do in CMC environment. And, Lee (2007) found that males in particular conformed to masculine gender norms, and stereotypical men tended to resist social influence more than stereotypical women.

Extant research also showed that males demonstrate increased levels of general self-efficacy in mathematic problem-solving (Pajares & Kranzler, 1995; Pajares & Miller, 1994) and are also more likely to exhibit higher levels of specific self-efficacy in multiple contexts such as reading, learning (Pajares, 2002, 2003) and technology use (Huffman, Whetten, & Huffman, 2013). In an elementary school information search study, Large, Beheshti, and Rahman, (2002) found gender differences in boys and girls' collaborative Web search activities. Generally, boys tend to use fewer keywords when conducting a search and query online. Boys spent less time on single webpages, click hyperlinks more frequently, and are more active than girls. Lorigo, et al. (2006) also found statistical significance in gender difference in terms of their information search behavior. Based on evaluating users' interaction with the search task assignments using eye tracking technologies in the experiments, males tend to search further down on the abstract results lists of the returned query results, and represented more linear path in their eye movements whereas females tend to have repeated viewings on the abstracts and thus demonstrated more regression patterns.

In general, males tend to display higher positive self-efficacy in task assignments online, and gender differences can typically play a role in the motivation to complete tasks. Thus, we must investigate gender-lined cognitive factors to understand how self-efficacy and motivation influence gender deception. Specifically, in the next hypothesis we examine gender differences based on self-efficacy in deception:

H7. Males have more positive self-efficacy beliefs in gender deception than females.

Likewise, to determine whether males or females are more motivated to deceive, irrespective of context or topics, we further hypothesize that:

H8. Males and females differ significantly in their motivation to deceive.

Gender may influence not only a message sender's motivation to deceive but also the success rate of the message sender's deception. In a study of small task group communication in asynchronous online environments, Savicki, Kelley, and Lingenfelter (1996a); (1996b) found that in contrast to all-male groups, all-female groups were less likely to argue, more satisfied with the group decision-making process, and more expressive in asynchronous online communication environment. This

behavior is linked with high group development communication style (HCS), in contrast to the opposite behavior seen in all-male or in mixed-gender groups, called low group development communication style (LCS) (Savicki et al., 1999). Savicki et al. (1999) used this paradigm to study people's ability to deceive and attribute gender, and found that accuracy in gender attribution is higher (around 71%) when the message senders are male and when their language is in the typical all-male group style (M-LCS). The attribution accuracy is lower (around 55%) when the message senders are female and their language is in the typical female group style (F-HCS).

However, something interesting happens when research participants exhibit reverse gender stereotypes such as when participants communicate "contra-gendered" messages in cases of F-LCS and M-HCS. Messages are considered contra-gendered when they demonstrate the opposite of previously identified language–gender relationships (Savicki et al., 1999). In these instances, accuracy in gender attribution for M-HCS is much lower (around 40%), but accuracy for F-LCS is higher (around 66%). If we think of contra-gendered communication as a kind of "pretend" or "performed" gender category—in which males use language that is more stereotypically female and vice versa—then gender is socially reconstructed and can be used to form a virtual reality (Rodino, 1997). This is a scenario similar to what we explore in this research: the extent to which deception succeeds when males successfully communicate like females and females communicate like males. To understand how contra-gendered messages affect the successful outcome of deception, we hypothesize that:

H9. Male message senders are more likely than female message senders to succeed in deceiving others about their gender in online communication.

3.4. Gender-based impersonation and attribution

How good are people at pretending to be the opposite gender? Herring and Martinson (2004) suggested that even when individuals are intentionally trying to deceive others about their gender, their use of words and sentences significantly relate to their real-life gender (p. 428). Herring and Martinson (2004) found that in a Turing game, participants assessed one another's gender on the basis of stereotypical content in their utterances (the action of speaking the words) rather than their use of gendered discourse styles (i.e., the overall flow of the debate or communication). They investigated how online users determine the veracity of stated identity from a message source and, moreover, how they imitate gender—as measured by people's ability to attribute gender accurately. Their results showed that participants' judgments were wrong about half the time, with no better accuracy than random chance. Nowak (2003) also found that people tended to make wrong attribution about other participants' biological gender. Rodino (1997) speculated that since the use of language in chats is more malleable than in FtF situations, the poor accuracy of gender attribution might be caused by the fact that gender can be socially reconstructed. Some chat players present gender with stable representations, whereas others may give contradictory performances, break out of binary gender categories, and re-create and redefine their gender attributes (Rodino, 1997).

Moreover, men and women tend to adopt different communication skills depending on self-efficacy factors. Bussey and Bandura (1984); (1992) reported that gender does influence respondents' judgments as well as observers' cognitive competencies for making judgments. As people attribute the behavior of others, their attributions are often guided by preconceptions due to gender differences. For example, Bussey and Bandura (1999) found that boys tend to pay more attention to gender stereotypes than girls. Other contextual factors such as the social structural arrangements or social networks of human interactions also play critical roles in how gender is attributed. Previous research demonstrates that males typically have higher self-efficacy beliefs in mathematical problem-solving, reading and writing skills (2002, 2003; 1995; 1994), and we have hypothesized that males have more positive self-efficacy beliefs in the ability to deceive regarding gender (H7). To further understand how gender affects self-efficacy in attributing online gender deception, we further hypothesize that:

H10. Males demonstrate higher self-efficacy beliefs than females in attributing online gender.

While we may assert the importance of self-efficacy in gender attribution, the analysis by Savicki et al. (1999) notably showed no significant differences between male and female judges. Males were not more confident in their judgments (or attributions of gender-based messages) than females, and individuals' beliefs in the accuracy of their judgments did not correspond to accuracy in gender attribution. Likewise, Lee (2007) reported in a study of gendered language that yielded results suggesting that people are not skilled at detecting gender stereotypes online. In Lee's (2007) experiments, he set up an online game to facilitate the study of dispositional and situational factors that relate to the use of gender-linked language. This study found that individuals who do not exchange descriptive personal profiles (e.g., age, hobby, and preferences) were more likely to attribute correct gender from their communicators' linguistic cues.

Beliefs, perceptions, and preferences often vary between genders. Croson and Gneezy (2009) reported that males tend to be more trustful than females, but that males also tend to take more risks and be more confident; and their preferences tend to be context-specific. Interestingly, Eckel and Wilson (2004) found that gender influences trust decisions. Trust is not a problem of risk, but a problem of judgment. In a trust game, males tended to be more trusting than females when given only textual information about a game partner. However, other contextual factors (e.g., attractiveness and ethnicity) also influence trust decisions. For example, females were more trusting than males when participants were given a photo of the partner. When a participant was uncertain about a situation, he or she would inference all possible source of information to determine whether their game participant is trustworthy. Nowak's (2003) study of gender attribution in participants

who engaged in a desert survival exercise across networked computers found that the majority of participants were either wrong or unsure (69%) about the gender of their partner, and those who were unsure (confederate) were more likely to assign credibility to their partner (e.g., respondents were asked whether "the confederate was knowledgeable on the topic, professional, cooperative, and influential" (Nowak, 2003, pp. 91 & 94). Even when women demonstrated higher ability in developing social presence on social media than men, Nowak (2003) found that attribution of credibility and immediacy involvement were not significantly different for men or women. Based on Nowak's (2003) discovery, we investigate whether an observer's (i.e., detector's or message recipient's) gender has an effect on the success outcome of deception, and thus hypothesize that:

H11. Females have a higher success rate than males in detecting online gender deception.

In a study of gender-preferential language during informal electronic exchanges, Thomson and Murachver (2001) found that per 100 words, female language was significantly more likely than male language to contain emotion, personal information, modals, hedges, and intensive verbs. Other differences were observed: Female language contained apologies and self-effacing comments, whereas males' often did not; moreover, females asked more questions, whereas males stated more opinions. However, when Thomson and Murachver (2001) asked respondents to judge the gender of the author of these messages in the second experiment, they found, much like Savicki et al. (1999), that the gender of the judges had no effect on accuracy. Sixty percent of judges attributed gender successfully for 14 out of 16 messages (Thomson & Murachver, 2001). In a third experiment, Thomson and Murachver (2001) asked respondents to evaluate the gender of an author writing about gender-neutral topics by using a rating scale. The female version of these messages contained additional references to emotion, an apology, and an intensive adverb (e.g., "really"); the male version contained no apologies or intensive adverbs but did contain insults and longer sentences (Thomson & Murachver, 2001). These findings show that preconceptions of stereotypical gender-preferential language do play a significant role in how people attribute gender. People do judge a communicator's gender based on gender-preferential language, such as the use of more apologies by females and of more insults by males. Because male language styles are easier to recognize than female language styles, it may be easier for female deceivers to imitate a male than vice versa. Therefore, we hypothesize that:

H12. Detectors that perceive message senders' gender as male are less likely to attribute correct gender.

Based on the review and above discussion, we have identified self-efficacy, motivation, and gender as major contributing predictor-factors in an online communicator's ability to deceive, and to the success rate of his or her deception. These factors may also influence a detector's ability to uncover deception. Our research hypotheses were further studied and tested in controlled experiments through an asynchronous online game.

3.5. Methodology

We designed an asynchronous online game for the purpose of controlled experiments where participants are assigned both gender roles at different times as they progressed through the study. This online game was designed to mimic social interactions in one-to-many[5] asynchronous communication while preserving each participant's privacy. The communication initiator was the message sender, whereas the message recipient was called the receiver (or detector). The influence of peripheral factors, such as affect and time were not measurable due to the asynchronous, randomized, and anonymous nature of the design and the difficulties of determining sentiment via textual communication. The research was specifically designed to study participants' attribution of language use, and their cognitive perception of gender from online messages in the context of deception. Participants' language use was not the subject of this investigation.

Our study's framework was designed to illuminate how a deceptive communicator (or deceiver) interacts with a potentially deceived participant in a one-to-many asynchronous online communication environment. It was also designed to determine to what extent people online are capable of deceiving message recipients about their gender, and whether people are capable of attributing gender when people are truthful or not truthful, and whether the level of knowledge about a topic influences efficacy in gender imitation and deception attribution. Within this framework, asynchronous social interactions were enabled by computer-mediated technologies.

3.6. Research design

To create the contextually rich data structure needed to pursue our research aims, we invited users of diverse existing social media "societies" to a new sociotechnical game portal called the *Virtual Funhouse*[6] (see Fig. 2), which was staged on a social media platform (i.e., Facebook) and contained controlled scenarios in order to simulate social interactions.

Virtual Funhouse is a live laboratory for conducting sociotechnical research in a game environment. During structured game-playing, we assess social actors' cognitive constructs e.g., motivation, self-efficacy, and perceived gender based on

[5] One-to-many refers to a game setting where one player is given multiple chances to evaluate online communications from multiple players.

[6] *Virtual Funhouse* is hosted at http://isensoranalytics.com/ where users (players) are authenticated through their Facebook accounts, with data collected and stored locally at the Florida State University.

Fig. 2. Virtual Funhouse Game Portal.

Table 1
Study design.

Study Phase	Steps for Study Respondents
Phase 1 (truth-telling)	■ Choose four topics and rate their own levels of domain knowledge. ■ Provide statements or stories about those topics.
Phase 2 (attribution/detection)	■ Attribute gender of the author of two anonymous statements. ■ Rate their own knowledge and self-efficacy of given topics. ■ Provide reasons for their attribution (gender assignment).
Phase 3 (imitation/deception)	■ Imitate the opposite gender (provide statements as if they were the OPPOSITE gender).
Exit game	■ Provide self-efficacy and motivation ratings. ■ *Re*-enter the game at Phase 2 to attribute a new set of statements and create new gender-deceptive statements (optional).

their written language (i.e., asynchronous messages as users' information behavior) in various online interactive scenarios. Through this portal, we examine how online actors assess and attribute each other's language (i.e., information behavior expressed in text communication) when gender is not explicit or apparent.

In our study, participants were invited to endorse and tag statements based on their personal opinions. The *Guess Who*? game was designed to allow for random invitation of participants who entered the game through a Facebook portal. After participants gave their consent, they provided demographic information such as their gender (declared on the Facebook profile), which was considered ground-truth data in the context of the sampling frame. Game players were asked for their names and contact details and were told this information was for the purposes of remuneration. Table 1 shows the three phases of the study.

This online game mechanism was designed to include three phases, and the game could be played multiple times. The first phase was the baseline phase (P1 in Fig. 3). In this phase, we asked players to choose two topics and wrote their truth-telling statements based on the selected. We provided 62 topics, ranging from categories of current events to random topics

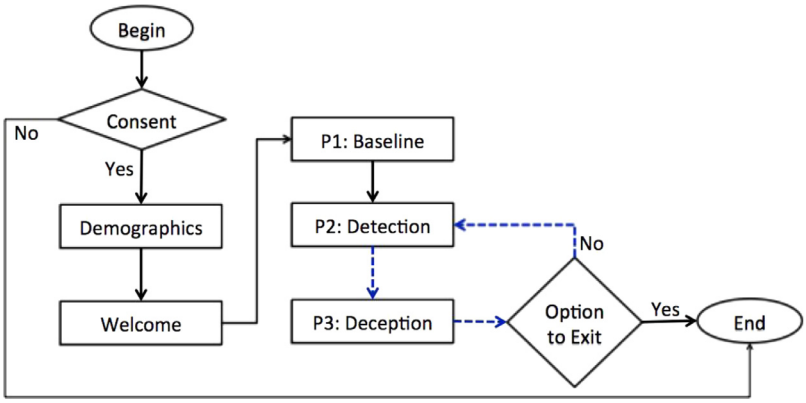

Fig. 3. Game Design Schematics.

(e.g., biking, laws, ways to waste time). Our goal was to provide categorical topics that were as (culturally) gender neutral as possible. Game players were then asked to write about these topics in a few sentences—either to explain what they knew about a particular topic or to tell a story about a particular topic.

The second phase (P2 in Fig. 3) also collected baseline data of the players' natural state of attribution (detection phase). After players attributed gender based on the randomly displayed statements (by default randomness of the RAND() function in the MySQL database), the result of gender attribution (where 0 refers to successful gender deception/failed gender attribution, and 1 refers to successful gender attribution/failed gender deception) was immediately shown to the players. To ensure that players were not suspicious about the gender of respondents who wrote the statements they were attributing, the section in which players were asked to provide two statements about the same topics as if they were the opposite gender was shown last. In this phase, players were shown two statements written by other participants in the study, but players were not told under what circumstances (P1 baseline truth-telling or P3 deception) the statement was written. Two of these statements were randomly generated by the default RAND() function in the MySQL database to randomly display the questions from the dataset collected from the previous section. In this phase, respondents were asked to attribute gender to the statements and provide their confidence rating based on their attribution to those statements.

The third phase of the game started the participant's training for gender deception (P3 in Fig. 3; measures illustrated in Appendix A) by asking them to imitate the opposite gender; males were asked to give a statement using a female tone, and females were asked to give a statement using a male tone. In this phase, we asked players to provide one statement for each of the two topics they selected in Phase 1 but to write these statements with the purpose of imitating the opposite gender. In this statement, players were asked to write their statement based on the topic.

Although this online game could be played multiple times by each player, based on the systems' design, players did not evaluate their own statement, nor did they observe the same statement twice. After completion, players were given the choice to either replay or exit the game. However, we treated the data from these participants who re-entered into the study as a treatment group in Fig. 3 and entered into the detection phase (P2 in Fig. 3). If the players chose to replay the game, they were shown two statements written by other participants, asked to attribute gender to the statements, and asked to provide their confidence rating based on their attribution of the statements. In our database, we marked these players as the deception-training dataset because they were influenced by the P3 phase in which they' d been told to imitate the opposite gender. Then, players entered the deception phase (P3 in Fig. 3; measures presented in Appendix A) where they selected two topics about which to write statements. Before exiting the game, players were asked questions about the strategies they used when pretending to be the opposite gender, the factors contributing to their successful gender attribution, their efficacy rating for writing the deceptive statements, and their level of motivation.

3.7. Participants

Data were collected during the spring of 2013. The appropriate institutional human subjects committee approved the study.[7] All participants gave full informed consent. Participants were recruited through FtF campus activities, and also Facebook based on their availability from several US-based universities with an incentive of the chance to win an iPod shuffle. Participants were given options to select and deposit their statements based on 62 topics (Appendix B). The total number of participants was 134, and they consisted of 64 females (47.8%) and 70 males (52.2%). The participants directly assigned these gender categorizations from Facebook, which was verifiable with their biological gender. For all gender variables, the male

[7] Florida State University Institutional Review Board (IRB) approved human subject research with the approval protocols #2012.8928 and #2013.10760.

Table 2
Descriptive statistics and Pearson correlation matrix (n = 413).

Measure	Mean	*SD*	1	2	3	4	5	6
1. Gender of sender	.49	.50						
2. Perceived gender of sender	.51	.50	−.14**					
3. Gender of receiver	.56	.49	−.006	.058				
4. Motivation	4.79	1.71	−.245**	−.102*	−.04			
5. Attribution efficacy	4.65	1.75	.025	.086*	.034	−.194**		
6. Imitation efficacy	4.24	1.14	.19**	.071	−.028	.382**	.272**	
7. Outcome	.43	.49	.025	−.008	−.094*	−.063	.027	−.047

* $p < .05$;
** $p < .01$; Outcome: 0 = Successful Gender Attribution; 1 = Successful Gender Imitation/Deception

group was coded as "1" and the female group as "0." In our sample, there was no transgender representation. Therefore, the mean of each of these variables indicates the proportion of males in the variable. The 134 unique participants generated 413 records ($n = 413$) that were usable for statistical analysis. Of the 413 records, 50.6% of the message senders were female and 49.4% were male. Females accounted for 44.3% and males for 55.7% of the detectors. The average age of the overall sample was 22.6 years (mode and median age was 21) within a range of 18–58 years. The average age was 23.2 years for female participants and 22.1 years for male participants.

4. Analysis and results

4.2. Gender and topics

We ran a chi-square test for the dependency between the actual gender of the message sender and the choice of topics. The chi-square (χ^2) result is significant ($\chi^2 = 409.33$, $df = 58$, $p < .001$) meaning that the participants selected a wide range of topics of interests in their responses. The phi = .996 ($p < .001$) indicates a strong positive relationship between actual gender of the sender and 62 topics of interests. Additionally, we also ran a chi-square test for the dependency between the perceived gender of the message sender, and the frequency in choosing the topics. The chi-square (χ^2) result is significant ($\chi^2 = 117.51$, $df = 58$, $p < .001$) meaning that the participants selected a wide range of topics of interests in their responses. The phi = .533 ($p < .001$) indicates a strong positive relationship between actual gender of the sender and 62 topics of interests. Although there are significant associations between topic and the (perceived) gender of the sender, (actual) gender of the sender, and task outcome (successful attribution of the actual gender), the expected count was less than 5 for each topic in greater than 20% of the cells in all of the chi-square tests.

In the overall sample, the likelihood ratio is 143.945 ($df = 58$, $p < .001$) between topic and perceived gender of the sender; 565.595 between topic and gender of the sender ($df = 58$, $p < .001$); and 138.463 ($df = 58$, $p < .001$) between topic and successful gender attribution. In the first two cases, there was no significance in the directional measure of Somers' d suggesting that these variables are not necessarily associated in a directional relationship. Certain topics are gendered simply based on cultural/societal norms, which is not something we can control. However, 413 participants utilized 59 of our 62 topics across both genders. The exception occurred in the deceptive state subsample of the topic and gender of the sender analysis. Here the likelihood ratio is 372.421 ($df = 40$, $p < .001$) with Somers' d values of –.098 for symmetrical, –.074 ($p < .05$) for gender of the sender dependent, and –.144 for topic dependent ($p < .05$). These negative and weak values imply that the participants may have been trying to be deceptive about their gender. Since topical statements presented to the participants for attribution were randomized, the chances of each participant getting a truthful, deceptive, or a particular topic should be equal.

Table 2 presents the mean (M) and standard deviation (SD) of each variable as well as the Pearson correlation coefficients among the variables. As expected, motivation to deceive was positively correlated with gender imitation self-efficacy ($r = .382$, $p < .01$) and negatively correlated with self-efficacy of correct gender attribution ($r = -.194$, $p < .01$).

Gender attribution efficacy was positively correlated with gender imitation self-efficacy ($r = .272$, $p < .01$). Gender of the sender was negatively correlated with the motivation to deceive ($r = -.245$, $p < .01$). Females ($M = 5.21$, $SD = 1.36$, $n = 209$) were significantly ($t = 5.10$, $df = 365.26$, $p < .01$, equal variances not assumed) more motivated to deceive than males ($M = 4.37$, $SD = 1.92$, $n = 204$) in the overall sample. Gender of the communicator was also correlated with gender imitation efficacy ($r = .19$, $p < .01$); males ($M = 4.46$, $SD = .99$) were more confident ($t = -3.99$, $df = 411$, $p < .01$, equal variances not assumed) in their ability to imitate gender than females ($M = 4.02$, $SD = 1.23$).

Our findings support studies that show humans are generally ineffectual lie detectors (Buller & Burgoon, 1996; Ekman & O'Sullivan, 1991). In our sample, participants were correct in attributing gender only 43% ($SD = .49$, $n = 413$) of the time, 7% less than chance. This result is similar to what Herring and Martinson (2004) found in their Turing game study but much lower than the 50–58% lie detection rate of the general public as found by Frank et al. (2004). Our findings further suggest

Table 3
Mean differences between male and female participants.

Factor		Males			Females			Analysis		
		M	SD	n	M	SD	n	t	df	p
Successful Gender Attribution	O	.387 (38.7%)	.48	230	.481 (48%)	.50	183	1.91	385.8	<.05*†
	T	.44	.50	78	.56	.50	60	1.37	136	>.05
	D	.35	.48	152	.43	.49	123	1.40	257.0	>.05†
Successful Gender Imitation	O	.559 (55.9%)	.49	204	.584 (58.4%)	.49	209	−.51	411	>.05
	T	.47	.50	55	.51	.50	83	−.51	136	>.05
	D	.59	.49	149	.62	.48	126	−.61	273	>.05

Note: O=Overall; T=Truthful; D=Deceptive;
† = equal variances not assumed

Table 4
Differences between truthful and deceptive states.

Factor	Truthful State			Deceptive State			Analysis		
	M	SD	n	M	SD	n	t	df	*P*
Motivation of Deception	5.14	1.16	138	4.61	1.69	275	*2.99*	*411*	*<.01*
*Males	4.85	1.84	55	4.19	1.92	149	2.22	202	<.05
Successful Gender Attribution	.5 (50%)	.50	138	.393 (39.27%)	.48	275	2.06	268.3	*<.05*†
Successful Gender Imitation	.5 (50%)	.50	138	.607 (60.73%)	.48	275	2.06	268.3	*<.05*†

† = equal variances not assumed

that humans are bad gender deception detectors in text-based online environments. In contrast to findings by Thomson and Murachver (2001), our results show in Table 3 which indicates that females were significantly more accurate (48.08%, SD = .50, n = 183) in attributing gender than males (38.69%, SD = .48, n = 230) in the overall sample.

4.3. Order effects

Our study distinguished between the performances of participants playing the game for the first time from performance on subsequent attempts. It is possible that a learning curve might be involved where participants had not only submitted truthful and deceptive statements of their own already, but had also appraised the statements of other participants after the Phase 3. In order to identify whether a learning curve occurred where a participant could be a better imitator of the opposite gender by the end round of the game, an order effect was observed in the overall sample (including male and female participants) between the first and subsequent attempts (see Table 4). Successful gender attribution occurred at a rate of 50% (SD = .50, n=138) in the first attempt (or truthful state) and at 39.27% (SD = .48, n = 275) in subsequent attempts at the deceptive state. This drop in rate was significant (t = 2.06, df = 268.33, p < .05 with equal variances not assumed). Inversely, the rate of successful gender imitation significantly (t=2.06, df=268.33, p < .05 with equal variances not assumed) increased from a rate of 50% (SD = .50, n=138) to 60.73% (SD = .48, n = 275) in the overall sample.

In summary, Table 4 suggests that subsequent attempts through the game may decrease the participants' ability to correctly attribute gender and increase their ability to successfully imitate the opposite gender. However, this order effect was insignificant when comparing the rates for male and female participants as separate subsamples (see Table 3).

4.4. Path analysis

A path analysis was conducted in M*plus* 7 (Muthén & Muthén, 1998–2012) to further test the research hypotheses based on the proposed theoretical model (see Fig. 1). The initial model had 19 parameters. A parameter was added to the model because it was theoretically meaningful and significantly improved the fit of data to the model. To compare models, the following indices were considered: the Akaike information criterion (AIC) (Akaike, 1973), the Bayesian information criterion (BIC) (Schwarz, 1978), and the chi-square difference test ($\Delta\chi^2$). Because the key outcome variable, *deception*, was dichotomous (failure or success), a binary logistic regression function was used to conduct the path analysis. For each outcome variable, R^2 was obtained.

The initial model resulted in AIC=4900.13 and BIC=4976.58. Adding a regression line from perceived gender to the message sender's self-efficacy decreased AIC to 4888.99 and BIC to 4969.45. This added parameter significantly improved the fit of the data to the model ($\Delta\chi^2$=13.36, p < .01). Using perceived gender to predict the message sender's self-efficacy was theoretically meaningful because, according to social cognitive theory, gender role development is continually being

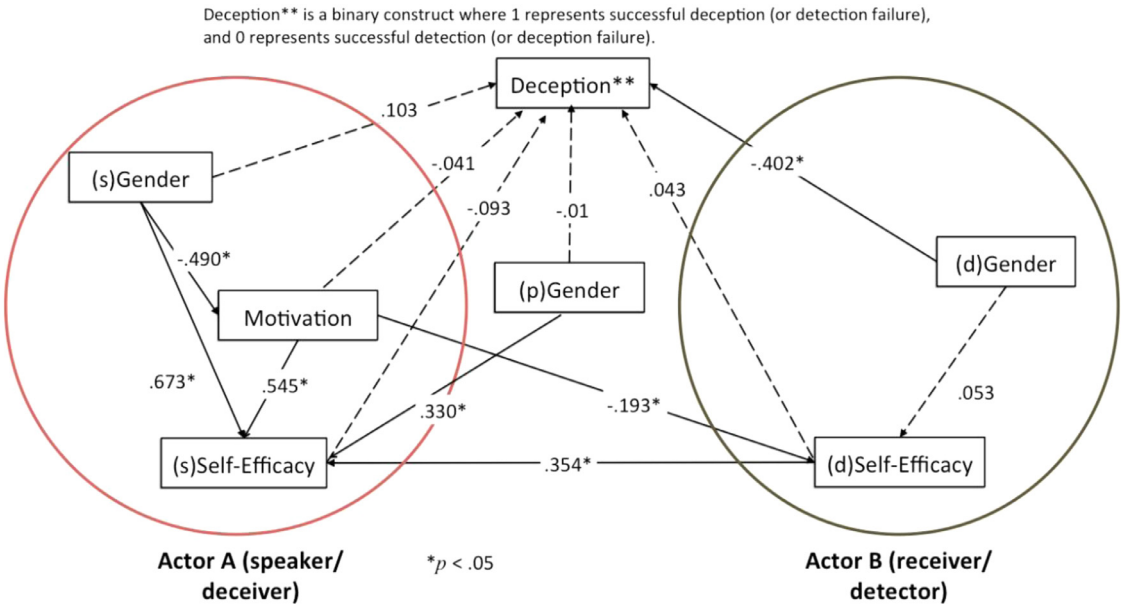

Fig. 4. Parameter Estimates from the Final Path Analytic Model.

constructed by a broad network of peers and societal influences (Bussey & Bandura, 1999). Although perceived gender of the message sender in an online communication context may affect the message sender's self-efficacy in deception, the current research design is not equipped to explain this relationship. Fig. 4 presents the standardized path coefficients from the revised model. For the variables predicting the dichotomous outcome variable *deception*, path coefficients were presented in the logit unit. A positive value, zero, or negative value of a logit means the likelihood of deception success is respectively higher, equal to, or lower than the likelihood of deception failure. Solid lines indicate that the path coefficients were significantly different from zero at α of .05, whereas dashed lines indicate that the path coefficients were not significantly different from zero.

4.4.1. Self-Efficacy and motivation

Among the six hypotheses related to self-efficacy and motivation (H1–H6), only H1 and H6 were supported. As expected, the message sender's motivation ($b = .545$, $p < .05$) and self-efficacy to detect deception ($b = .354$, $p < .05$) positively predicted the message sender's self-efficacy to deceive.

The H1 findings correspond to Bandura's (Bandura, 1977) claim that there is a close relationship between motivation and self-efficacy. Additionally, Bandura suggested that self-efficacy in one area may be related to self-efficacy in other areas. Our study shows that the higher one's self-efficacy in attributing correct gender, the higher one's self-efficacy in gender deception (H6). Contrary to the H2 hypothesis, the message sender's motivation negatively predicted his or her self-efficacy to detect deception ($b = -.193$, $p < .05$). In addition, detectors who perceived the gender of the message sender as male had higher self-efficacy ($b = .330$, $p < .05$). The percentage of variance in the message sender's motivation, self-efficacy to detect, and self-efficacy to deceive as indicated by R^2 was 6%, 4%, and 39%, respectively.

Hancock et al. (2010) suggested that motivated liars are more successful in computer-mediated online environments than in F2F circumstances. However, our study did not support H3 in that no significant difference was found between motivation levels of successful and unsuccessful gender imitators, and no significant relationship was found between motivation level and successful gender attribution. This might be caused by the motivational impairment effect posited by DePaulo et al. (1988) that the stronger the deceivers are motivated to deceive, the more they will deliberately control their verbal and nonverbal cues, which reduced success in deceiving others. Our study confirms the findings by Burgoon and Floyd (2000) that motivation is not a good predictor of liars' deceptive behavior. We speculate that the contrast between these studies' findings was due to differences in research design. Participants were given a list of discussion topics as task assignments in Hancock et al. (2010), whereas participants in the present study were asked to write intentionally as the opposite gender on a chosen topic in the online communication environment.

Previous research has indicated that individuals perform poorly when trying to identify deception in interpersonal relationships (Buller & Burgoon, 1996; Ekman & O'Sullivan, 1991; Frank et al., 2004). In online environment, the path coefficient from self-efficacy to successful gender deception was insignificant at an alpha level of .05. Therefore, H4 was not supported.

Similarly, there was no significant path coefficient from gender imitation self-efficacy to successful gender deception; hence, H5 was not supported.

4.4.2. Gender

Among the six hypotheses related to gender (H7–H12), only H7, H8, and H11 were supported. The positive path coefficient indicated that males have higher mean scores on the outcome variable than females. The three hypotheses that were supported by the data are discussed in the following paragraphs.

(1) Compared with females, males tended to report more positive self-efficacy beliefs in gender deception. The standardized mean difference between the two groups was .673, $p < .05$. It seems that males are more confident than females in their ability to deceive others about their gender in text-based online environments. Therefore, H7 was supported. This finding corresponds with findings seen in (Croson & Gneezy, 2009; Dreber & Johannesson, 2008; Feingold, 1994).
(2) Compared with males, females tended to be more positively motivated to deceive. The standardized mean difference between the two groups was $b = .490$, $p < .05$. Overall, although males tended to be more confident (H7), they were not more effective at imitating the opposite gender in practice. Interestingly, we found that female message senders were significantly more motivated than male message senders to imitate the opposite gender (H8). Accordingly, it seems that females who chose to replay the game were more motivated to imitate the opposite gender (H8). However, the factors behind this motivation and self-selection need to be investigated in future research.
(3) Compared with males, females were more likely to be successful in gender detection, with $b = -.402$, $\exp(b) = .669$, and $p < .05$. Thus, H11 was supported. However, the six predictors (message sender's gender, motivation of the message sender to deceive, self-efficacy of the message sender, perceived gender of the message sender, detector's gender, and self-efficacy of the detector) explained only a very small percentage of variance (2%) in the deception.

The other three hypotheses (H9, H10, and H12) were not supported by the data. There was no significant difference in successful gender imitation rates between males and females (H9). Our findings suggest that neither gender is better than the other at imitating the opposite gender in text-based online environments. Thus, H9 was rejected. In addition, there was no significant difference in gender attribution efficacy between males and females (H10). In other words, while males have more positive self-efficacy beliefs in gender deception than females, (H7), males do not demonstrate higher self-efficacy in identifying gender fraud than females (H10). Thus, H10 was not supported.

Our findings concerning the accuracy of perceived gender seem to support the finding by Savicki et al. (1999) that gender attributions based on female-gendered language are more accurate in the context of contra-gendered messages. However, we found no significant differences in the likelihood of detection failure or success between detectors who perceived the message senders as males and those who perceived the message senders as females (H12). This means that the outcome of gender fraud is not influenced by people's perception of the deceivers' gender as being male or female. Thus, H12 was not supported. This suggests that the deceptive priming at the end of Phase 3 (see Fig. 3) may have affected the participants' ability to perceive gender accurately.

4.5. Summary of hypotheses testing results

In the hypothesized model, four variables (including message sender's self-efficacy, motivation, detector's self-efficacy, and deception success) were outcome variables. The percentage of variance explained by their predictors ranged from very small—only 2% for deception—to large—39% for message sender's self-efficacy. It suggests that for those outcome variables where only small percentages of variance are explained, the predictors included in this model (including gender, message sender's self-efficacy, and motivation) are not good predictors for success of deception. Particularly for deception (with 2% variance explained), only one out of the six predictors showed a significant path coefficient (i.e., detector's gender). Although the detector's gender was a significant path coefficient for successful gender attribution (females were better than males), the rate of successful gender attribution was still below chance. The hypotheses of this research model are summarized in Table 5.

5. Contributions to research and practice

This study informs ongoing computer-mediated gender deception research and illuminates the multifactorial process of online deception. Our work has contextualized extant research findings by evaluating gender deception within the very environmental conditions—computer-mediated asynchronous communication systems—where the problem is found to be most prevalent in the real world (Brady & George, 2013). Context-specific factors (e.g., asynchronous online communication, random display of discussion topics, and random assignment of gender role play) were incorporated into our research design to ensure that the findings address our theoretical understanding of this phenomenon, and validate the complex social-cognitive process of gender influence on self-efficacy and motivation of the deceiver in relation to the message recipient's gender and self-efficacy in detecting deception. Previous research has found that humans are not reliable detectors of deception (Ekman & O'Sullivan, 1991; Frank et al., 2004; Whitty, 2002). Our study confirms that female participants were better than male participants at attributing gender in asynchronous online environments. However, this finding further suggests that the concept of gender is complex and multifaceted, and warrants further research—particularly in the areas of gender

Table 5
Research findings.

Hypotheses	Results
Hypotheses Related to Motivation and Self-Efficacy	
H1. The higher the motivation of message senders to deceive, the higher their self-efficacy beliefs.	Supported
H2. The higher the motivation of message senders to deceive, the higher their self-efficacy to detect others' online gender deception.	Not Supported (but statistically significant)
H3. The higher the motivation of message senders to deceive, the easier it is for them to deceive others about their true gender.	Not Supported
H4. The higher the self-efficacy beliefs of detectors, the easier it is for them to identify online gender deception.	Not Supported
H5. The higher the self-efficacy beliefs of message senders, the higher their chances of succeeding in online gender deception.	Not Supported
H6. The higher one's self-efficacy in attributing correct gender, the higher one's self-efficacy in gender deception.	Supported
Hypotheses Related to Gender	
H7. Males have more positive self-efficacy beliefs in gender deception than females.	Supported
H8. Males and females differ significantly in their motivation to deceive.	Supported
H9. Male message senders are more likely than female message senders to succeed in deceiving others about their gender in online communication.	Not Supported
H10. Males demonstrate higher self-efficacy beliefs than females in attributing online gender.	Not Supported
H11. Females have a higher success rate than males in detecting online gender deception.	Supported
H12. Detectors that perceive message senders' gender as male are less likely to attribute correct gender.	Not Supported

identity and deception in online spaces. Deceivers may tend to adopt contra-gendered strategies to hide their deceptive motives. Cognitive factors (such as motivation and self-efficacy) for both message senders and recipients may not be good predictors of deception largely due to the interchangeable play of the gender roles (based on the study design). As people are more aware of the gender deception phenomenon, they become more skeptical about stereotypical gender-linked language representation, which may influence the ability to attribute and identify correct gender. To increase the predictive power of these cognitive variables, further research should include behavioral predictors, such as message senders' perceived credibility, competence for social presence, consistency of information presentation, language use, and message recipients' trustfulness and degrees of bias.

Nonetheless, this study contributes to the understanding of online gender deception by examining gender difference as a key control factor. Gender appears to have an effect on a message sender's motivation to deceive. Our study found that males have higher positive self-efficacy beliefs in gender deception, whereas females have a higher success rate in detecting gender deception. However, no gender difference was found associated with successful deception (i.e., the success of gender deception). Likewise, there was no gender difference associated with self-efficacy beliefs related to correctly attributing gender online. Although message senders may be motivated to deceive, their motivation does not make it easier for them to do so. Their chances for actual success in online deception are not positively correlated with self-efficacy beliefs. Overall, the higher the motivation of message senders to deceive, the lower the belief in their ability to detect online gender deception. Likewise, the higher the message recipient's self-efficacy belief, the easier it is for them to identify online gender deception.

Our sample comprised experienced users of online social media environments, which represent the context of our investigation. Although the majority of the participants were undergraduate students and the sample may not be representative of the general population in all dimensions, increased generalizability was achieved because our research participants were randomly recruited and data from participants' truthful and deceptive statements were randomly displayed to participants who were in the detector mode by using the RAND() function in MySQL. This indicates that the chances of participants getting a truthful, deceptive, or a particular topic should be equal. Our study also suggested that no significant differences were found in the likelihood of gender attribution success or failure based on the perceived gender of the message sender. Thus, while topics of discussion may be perceived as gendered (e.g., knitting s vs. football), these perceptions did not impact the success or failure of the deception.

Deceptive communications can pose a considerable threat when they drive online transaction fraud, theft of credentials and intellectual property, and threats against national security. Online communicators must frequently determine whether the source of messages is legitimate and whether the identity of the communicator is validly represented. An online user's ability to assess credible information (Hilligoss & Rieh, 2008; Liu, 2004; Rieh, 2002) is essential in protecting their information privacy and online safety (Lopez & Sebe, 2013). A practical finding of this study is its identification of gender as a factor in detecting gender deception in social media relationships, and deceptive friend requests for social, financial or business relationships. The study also contributes to the domains of detecting "spear phishing" attacks where targeted online users are psychologically manipulated by deceivers with various strategies in the context of asynchronous communication.

6. Limitations and future research

As with all laboratory experiments, the proposed research design did not aim to maximize predictions through a complete path model and thus exhibits certain inherent limitations. In our laboratory experiments, certain controls (i.e., users' limited interactions were controlled in asynchronous online environment, interchangeable gender role plays were randomly displayed, and different phases of deception and detection on randomized topics) were implemented at the expense of contextual realism and generalizability of results in pursuit of precise measurement of online users' behaviors. Although one may argue that using online games as a research medium may be overly simplified or artificial, that social cues are few in text-only online environments, and that no actual face-to-face interactions were drawbacks in this study, these limitations can help clarify online deceptive communications in a significant percentage of incidents such as gender fraud, where a communicator might be deceptive in an asynchronous online transaction.

In contrast to the synchronous interpersonal computer-mediated discussions designed and conducted by Ho, Hancock, Booth, Liu, et al. (2016, 2015); Ho, Liu, et al. (2016), our research design displayed asynchronous, randomized true or deceptive text messages to participants. The difference in research design may have introduced different results. First, this research design may decrease the participants' ability to correctly attribute gender and increase their ability to successfully imitate the opposite gender. However, the order effect was not observed as being significant when comparing the rates for male and female participants as separate subsamples. Second, as McCornack (1992a); McCornack (1992b) suggested, relationships and historical knowledge between actors can be an important baseline factor in attributing truth or deception to communications. Our study design did not foster long-term relationships between participants. Participants in this asynchronous text-based game were unable to interpret or attribute deceptive or truthful behavior through the kind of cues and behaviors readily observable in synchronous and/or FtF communication. Likewise, participants were unable to build on the knowledge of previous interactions with each other. There was no chronology and trust-building activities in participants' relationships over time.

Participants were recruited from the universities located in the United States, which indicates that the samples were drawn from Western, Educated, Industrialized, Rich and Democratic (WEIRD) population (Henrich, Heine & Norenzayan, 2010). Although the thin slice of the samples does not represent the general humanity, this study however represents those who regularly communicate using modern computer-mediated technologies. Due to random recruitment, the numbers of participants in the study were slightly unequal in terms of gender. This unequal distribution of male and female participants may have been an issue and produced a bias in the analysis and findings. Although no player was given this information, the randomness of the research design affords message recipients an equal chance to attribute gender. In addition, participants who had non-binary genders were not appropriately represented or facilitated by our choice of authentication and research design.

Future research will include investigation of cognitive factors related to the identification of trustworthy message sources, as well as communicators who seek to obfuscate their identities in terms of gender, trust, topic of interest, as well as other characteristics. We expect that our findings will assist both practitioners and researchers in developing a richer understanding of the phenomenon of deceptive online communication and the role of gender in computer-mediated deception, including identity fraud. We plan to conduct content analysis of strategies and language use for gender imitation as provided by respondents, with linguistic analysis of the actual text they employed to imitate the opposite gender so as to compare them with grammatical concepts and gender-linked language features, respectively. Future research designs may use synchronous online environments to clarify the influence of time and relationship history on acts of deception.

7. Conclusion

The dangers of deceptive communications have grown over the past several years as more individuals have crossed the digital divide to participate in a wide range of online activities, from transactional electronic commerce to digital government and a wide range of computer-mediated social interactions. In this milieu, the critical role of trusted online communication requires that we understand the cognitive factors involved in detecting deception. This study can inform the future construction of gender deception research models, including computational deception learning systems. Through these efforts, we hope to establish the basis for a practical understanding of the multifactorial aspects of gender deception in online communication.

Acknowledgement

The first author acknowledges the National Science Foundation Secure and Trustworthy Cyberspace (SaTC) Program for support of EAGER #1347113 award, the Florida State University Council of Research & Creativity for support of Planning Grant (PG #034138) and the First Year Assistant Professor grant (FYAP #033114). The authors also wish to thank IFIP Working Group WG8.11/WG11.13 on Information Systems Security Research in conjunction with the Dewald Roode Information Security Workshop.

Appendix A. Measurement details

P1: Gender Imitation (Truth-Telling Baseline Phase)							
Topic (Selected from dropdown menu): Please choose a topic and describe what you know about a given topic or tell a story involving that topic.							
Topic 1:	Topic 2:						
Describe what you know about the topic you select or tell a story involving that topic. Please write a few statements about this topic. (Textbox has a 200-character limit.)							
P2: Gender Attribution (Detection Phase)							
Display [Topic 1] statement	Outcome selection: Male or Female?						
Display [Topic 2] statement	Outcome selection: Male or Female?						
Gender Attribution Self-Efficacy							
How confident you were in choosing the gender of the message sender for the topic?							
Topic 1: (From Phase 2)	1	2	3	4	5	6	7
Topic 2: (From Phase 2)	1	2	3	4	5	6	7
P3: Gender Imitation (Deception Phase)							
For this section, we'd like you to imagine you were trying to fool someone about your gender. Please write a couple of sentences about each of the four topics you discussed earlier, only this time, please pretend you are the opposite gender. Again, please write 3 to 5 sentences. You could describe what you know about a given topic or tell a story involving that topic, *but you must do so as if you are the opposite gender*.							
Topic (Selected from dropdown menu): Please choose a topic and describe what you know about a given topic or tell a story involving that topic.							
Topic 1:	Topic 2:						
Describe what you know about the topic you select or tell a story involving that topic. Please write a few statements about this topic. (Textbox has a 200-character limit.)							
Gender Imitation Motivation							
Finally, on a scale of 1 to 7, where 1 is "not at all motivated," 4 is "average," and 7 is "extremely motivated," how motivated were you to successfully come across as the opposite gender?							
Topic 1:	1	2	3	4	5	6	7
Topic 2:	1	2	3	4	5	6	7
Gender Imitation Self-Efficacy							
How confident you were in successfully imitating the opposite gender for the topic?							
Topic 1:	1	2	3	4	5	6	7
Topic 2:	1	2	3	4	5	6	7

Appendix B. 62 Topics

Topics					
Cricket	Horror Movies	Stamp collecting	Comedy Movies	Scrapbooking	Club
Spelunking	Painting	Volleyball	The Hunger Games-Literature	Documentaries	Gospel-Music
Recycling	Cars	Information Security	Camping	The Great Gatsby-Literature	Gangnam style
World of War Craft	Video Gaming	Hockey	Harry Potter	Fox News	Model building
Knitting	Baseball	Dubstep-Music	Tubing	Decorating	Basketball
Canoeing	Cooking	CNN News	Tennis	Crime Novels	Rally Racing
Shopping online	K-Pop-Music	Metal-Music	Fishing	Rock-Music	Ballet
RTS (real-time strategy)	Samba	NASCAR	To Kill a Mockingbird-Literature	Warcraft	Accounting
Romantic Novels	Ways to Waste Time	Environment Issues	Macarena	Facebook Privacy	Country-Music
Football	MMORPGs	Olympics	Theatre	Hunting	YouTube
Soccer	Hiking				

References

Akaike, H. (1973). Information theory and an extension of the maximum likelihood principle. In B. N. Petrov, & F. Caski (Eds.), *Proceedings of the Second International Symposium on Information Theory* (pp. 267–281). Budapest: Akademiai Kiado.

Anderson, D. E., DePaulo, B. M., Ansfield, M. E., Tickle, J. J., & Green, E. (1999). Beliefs about cues to deception: Mindless stereotypes or untapped wisdom? *Journal of Nonverbal Behavior, 23*(1), 67–89.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215.

Bandura, A. (1986). *Social foundations of thought and action*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (2006). Guide for constructing self-efficacy scales. In F. Paiares, & T. C. Urdan (Eds.), *Self-efficacy beliefs of adolescents* (pp. 307–337). Greenwich, Conn: IAP-Information Age.

Brady, E., & George, R. (2013). Manti Te'o's 'catfish' story is a common one, Sports. *USA Today* 01/18/2013.
Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory, 6*(3), 203–242. doi:10.1111/j.1468-2885.1996.tb00127.x.
Buller, D. B., Burgoon, J. K., Buslig, A., & Roiger, J. (1996). Testing interpersonal deception theory: The language of interpersonal deception. *Communication Theory, 6*(3), 268–289. doi:10.1111/j.1468-2885.1996.tb00129.x.
Burgoon, J. K., & Buller, D. B. (1994). Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics. *Journal of Nonverbal Behavior, 18*(2), 155–184.
Burgoon, J. K., & Floyd, K. (2000). Testing for the motivation impairment effect during deceptive and truthful interaction. *Western Journal of Communication, 64*(3), 243–267. doi:10.1080/10570310009374675.
Burns, M. B., & Moffitt, K. C. (2014). Automated deception detection of 911 call transcripts. *Security Informatics, 3*(8), 1–9. doi:10.1186/s13388-014-0008-2.
Bussey, K., & Bandura, A. (1984). Influence of gender constancy and social power on sex-linked modeling. *Journal of Personality and Social Pyschology, 47*, 1292–1302.
Bussey, K., & Bandura, A. (1992). Self-regulatory mechanisms governing gender development. *Child Development, 63*, 1236–1250.
Bussey, K., & Bandura, A. (1999). Social cognitive theory of gender development and differentiation. *Psychological Review, 106*(4), 676–713. doi:10.1037/0033-295X.106.4.676.
Caspi, A., & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *Cyber Psychology & Behavior, 9*(1), 54–59.
Conroy, N. J., Rubin, V. L., & Chen, Y. (2015). Automatic deception detection: Methods for finding fake news. doi:82. *American Society for Information Science*, 1–4.
Croson, R., & Gneezy, U. (2009). Gender differences in preferences. *Journal of Economic Literature, 47*(2), 1–27. doi:10.1257/jel.47.2.1.
da Cunha, J. V., Carugati, A., & Leclercq-Vandelannoitte, A. (2015). The dark side of computer-mediated control. *Information Systems Journal, 25*, 319–354. doi:10.1111/isj.12066.
Daft, R. L., Lengel, R. H., & Trevino, L. K. (1987). Message equivocality, media selection, and manager performance: Implications for information systems. *MIS Quarterly, 11*(3), 355–366.
DePaulo, B. M. (1992). Nonverbal behavior and self-presentation. *Psychological Bulletin, 111*(2), 203–243.
DePaulo, B. M. (1994). Spotting lies: Can humans learn to do better? *Current DIrections in Pyschological Science, 3*, 83–86.
DePaulo, B. M., Kashy, D. A., Kirkendol, S. E., Wyer, M. M., & Epstein, J. A. (1996). Lying in everyday life. *Journal of Personality and Social Pyschology, 70*(5), 979–995. doi:10.1037/0022-3514/96.
DePaulo, B. M., Kirkendol, S. E., Tang, J., & O'Brien, T. P. (1988). The motivational impairment effect in the communication of deception: Replications and extensions. *Journal of Nonverbal Behavior, 12*(3), 177–202. doi:10.1007/BF00987487.
Dreber, A., & Johannesson, M. (2008). Gender differences in deception. *Economics Letters, 99*, 197–199. doi:10.1016/j.econlet.2007.06.027.
Ebesu, A. S., & Miller, M. D. (1994). Verbal and nonverbal behaviors as afunction of deception type. *Journal of Language and Social Psychology, 13*(4), 418–442. doi:10.1177/0261927X94134004.
Eckel, C. C., & Grossman, P. J. (2008). Differences in the economic decisions of men and women: Experimental evidence. In C. Plott, & V. Smith (Eds.). In *Handbook of experimental economics results: 1* (pp. 509–519). New York, NY: Elsevier.
Eckel, C. C., & Wilson, R. K. (2004). Is trust a risky decision? *Journal of Economic Behavior & Organization, 55*(2004), 447–465. doi:10.1016/j.jebo.2003.11.003.
Ekman, P. (2009). In *Telling lies: Clues to deceit in the marketplace, politics, and marriage: 416* (pp. 978–0393337457). New York, NY: W.W. North & Company.
Ekman, P., & O'Sullivan, M. (1991). Who can catch a liar? *American Phychologist, 46*(9), 913–920.
Erat, S., & Gneezy, U. (2011). White lies. *Management Science, 58*(4), 723–733. doi:10.1287/mnsc.1110.1449.
Feingold, A. (1994). Gender differences in personality: A meta-analysis. *Psychological Bulletin, 116*(3), 429–456. doi:10.1037/0033-2909.116.3.429.
Frank, M. G., Paolantinio, N., Feeley, T. H., & Servoss, T. J. (2004). Individual and small group accuracy in judging truthful and deceptive communication. *Group Decision Support Systems, 13*, 45–59.
Fusilier, D. H., Montes-y-Gomez, M., Rosso, P., & Cabrera, R. G. (2015). Detecting positive and negative deceptive opinions using PU-learning. *Information Processing & Management, 51*(4), 433–443. doi:10.1016/j.ipm.2014.11.001.
George, J. F., Marett, K., & Giordano, G. (2008). Deception: Toward an individualistic view of group support systems. *Journal of the Association for Information Systems, 9*(10), 653–676.
Gneezy, U. (2005). Deception: The role of consequences. *American Economic Review, 95*(1), 384–394. doi:10.1257/0002828053828662.
Guadagno, R., Okdie, B. M., & Kruse, S. A. (2012). Dating deception: Gender, online dating, and exaggerated self-presentation. *Computers in Human Behavior, 28*, 642–647. doi:10.1016/j.chb.2011/11.010.
Hancock, J., Birnholtz, J., Bazarova, N., Guillory, J., Perlin, J., & Amos, B. (2009). Butler lies: Awareness, deception and design. *ACM.*.
Hancock, J., Thom-Santelli, J., & Ritchie, T. (2004). Deception and design: The impact of communication technology in lying behavior. *ACM*, 129–134.
Hancock, J., Toma, C., & Ellison, N. (2007). The truth about lying in online dating profile. *ACM*, 449–452.
Hancock, J. T., Woodworth, M. T., & Goorha, S. (2010). See no evil: The effect of communication medium and motivation on deception detection. *Group Decision and Negotiation, 19*(4), 327–343. doi:10.1007/s10726-009-9169-7.
Henrich, J., Heine, S. J., & Norenzayan, A. (2010). The weirdest people in the world? *Behavioral and Brain Sciences, 33*(2-3), 61–135. doi:10.1017/S0140525X0999152X.
Herring, S. C. (1995). Gender and democracy in computer-mediated communication. In R. Kling (Ed.), *Computerization and controversy: Value conflicts and social choices* (pp. 476–489). Orlando, FL: Academic Press, Inc.
Herring, S. C. (2000). Gender differences in CMC: Findings and implications. *Computer Professionals for Social Responsibility Journal, 18*(1), 0.
Herring, S. C., & Martinson, A. (2004). Assessing gender authenticity in computer-mediated language use: Evidence from an identity game. *Journal of Language and Social Psychology, 23*(4), 424–446. doi:10.1177/0261927X04269586.
Hilligoss, B., & Rieh, S. Y. (2008). Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. *Information Processing & Management, 44*(4), 1467–1484. doi:10.1016/j.ipm.2007.10.001.
Ho, S. M., Fu, H., Timmarajus, S. S., Booth, C., Baeg, J. H., & Liu, M. (2015). Insider threat: Language-action cues in group dynamics. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (pp. 101–104). New York, NY: ACM. doi:10.1145/2751957.2751978.
Ho, S. M., Hancock, J. T., Booth, C., Burmester, M., Liu, X., & Timmarajus, S. S. (2016). Demystifying insider threat: Language-action cues in group dynamics. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences* (pp. 2729–2738). IEEE Computer Society. doi:10.1109/HICSS.2016.343.
Ho, S. M., Hancock, J. T., Booth, C., Liu, X., Liu, M., Timmarajus, S. S., et al. (2016). Real or Spiel? A decision tree approach for automated detection of deceptive language-action cues. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences* (pp. 3706–3715). IEEE Computer Society. doi:10.1109/HICSS.2016.462.
Ho, S. M., Hancock, J. T., Booth, C., Liu, X., Timmarajus, S. S., & Burmester, M. (2015). Liar, Liar, IM on Fire: Deceptive language-action cues in spontaneous online communication. In *Proceedings of the IEEE Intelligence and Security Informatics* (pp. 157–159). IEEE. doi:10.1109/ISI.2015.7165960.
Ho, S. M., & Hollister, J. M. (2013). Guess who? An empirical study of gender deception and detection in computer-mediated communication. doi:117. *American Society for Information Science*, 1–4.
Ho, S. M., Liu, X., Booth, C., & Hariharan, A. (2016). Saint or Sinner? Language-action cues for modeling deception using support vector machines. In K. S. Xu, D. Reitter, D. Lee, & N. Osgood (Eds.), *Social, Cultural and Behavioral Modeling (SBP-BRiMS), LNCS 9708* (pp. 325–334). Springer International Publishing Switzerland. doi:10.1007/978-3-319-39931-7_31.
Holmes, J. (1988). Paying compliments: A sex-preferential politeness strategy. *Journal of Pragmatics, 23*(4), 445–465.
Holmes, J. (1995). *Women, men and politeness*. London: Longman.
Huffman, A. H., Whetten, J., & Huffman, W. H. (2013). Using technology in higher education: The influence of gender roles on technology self-efficacy. *Computers in Human Behavior, 29*(4), 1779–1786. doi:10.1016/j.chb.2013.02.012.

Hurd, K., & Noller, P. (1988). Decoding deception: A look at the process. *Journal of Nonverbal Behavior, 12*(3), 217–233.
Joinson, A. N., & Dietz-Uhler, B. (2002). Explanations for the perpetration of and reactions to deception in a virtual community. *Social Science Computer Review, 20*(3), 275–289. doi:10.1177/089443930202000305.
Large, A., Beheshti, J., & Rahman, T. (2002). Gender differences in collaborative Web search behavior: An elementary school study. *Information Processing & Management, 38*(3), 427–443. doi:10.1016/S0306-4573(01)00034-6.
Lee, E.-J. (2007). Effects of gendered language on gender stereotyping in computer-mediated communication: The moderating role of depersonalization and gender-role orientation. *Human Communication Research, 33*(4), 515–535. doi:10.1111/j.1468-2958.2007.00310.x.
Liu, Z. (2004). Perceptions of credibility of scholarly information on the web. *Information Processing & Management, 40*(6), 1027–1038. doi:10.1016/S0306-4573(03)00064-5.
Lo, S.-K., Hsieh, A.-Y., & Chiu, Y.-P. (2013). Contradictory deceptive behavior in online dating. *Computers in Human Behavior, 29*, 1755–1762. doi:10.1016/j.chb.2013.010.
Lopez, N., & Sebe, F. (2013). Privacy preserving release of blogosphere data in the presence of search engines. *Information Processing & Management, 49*(4), 833–851. doi:10.1016/j.ipm.2013.01.002.
Lorigo, L., Pan, B., Hembrooke, H., Joachims, T., Granka, L., & Gay, G. (2006). The influence of task and gender on search and evaluation behavior using Google. *Information Processing & Management, 42*(4), 1123–1131. doi:10.1016/j.ipm.2005.10.001.
Lowry, P. B., Zhang, D., Zhou, L., & Fu, X. (2010). Effects of culture, social presence, and group composition on trust in technoloyg-supported decision-making groups. *Information Systems Journal, 20*(3), 297–315. doi:10.1111/j.1365-2575.2009.00334.x.
McCornack, S. A. (1992a). Information manipulation theory. *Communication Monographs, 59*, 1–16.
McCornack, S. A., Levine, T. R., Solowczuk, K. A., Torres, H. I., & Campell, D. M. (1992b). When the alteration of information is viewed as deception: An empirical test of information manipulation theory. *Communication Monographs, 59*, 17–29.
Mulac, A., Bradac. , J. J., & Gibbons, P. (2001). Empirical support for the gender-as-culture hypthothesis: An intercultural analysis of male/female language differences. *Human Communication Research, 27*(1), 121–152.
Mulac, A., Lundell, T. L., & Bradac, J. (1986). Male/female language differences and attributional consequences in a public speaking situation: Toward an explanation of the gender-linked language effect. *Communication Monographs, 53*, 115–129.
Mulac, A., Wiemann, J. M., Widenmann, S. J., & Gibson, T. W. (1988). Male/female language differences and effects in same-sex and mixed-sex dyads: The gender-linked language effect. *Communication Monographs, 55*, 315–335.
Muthén, L. K., & Muthén, B. O. (1998–2012). *Mplus user's guide*. Los Angeles, CA: Muthen & Muthen.
Nowak, K. L. (2003). Sex categorization in computer-mediated communication: Exploring the utopian promise. *Media Psychology, 5*, 83–103.
Ott, M., Cardie, C., & Hancock, J. T. (2012). Estimating the prevalence of deception in online review communities. In *Proceedings of the World Wide Web (WWW'12)* (pp. 201–210). ACM. doi:10.1145/2187836.2187864.
Ott, M., Cardie, C., & Hancock, J. T. (2013). Negative deceptive opinion spam. In *Proceedings of the north american chapter of the association for computational linguistics: Human language technologies (NAACL-HLT 2013)* (pp. 497–501). Association for Computational Linguistics.
Ott, M., Choi, Y., Cardie, C., & Hancock, J. T. (2011). *Finding deceptive opinion spam by any stretch of the imagination* (pp. 309–319). Association for Computational Linguistics.
Pajares, F. (2002). Gender and perceived self-efficacy in self-regulated learning. *Theory Into Practice, 41*(2), 116–125. doi:10.1207/s15430421tip4102_8.
Pajares, F. (2003). Self-efficacy beliefs, motivation and achievement in writing: A review of the literature. *Reading & Writing Quarterly: Overcoming learning difficulties, 19*(2), 139–158. doi:10.1080/10573560308222.
Pajares, F., & Kranzler, J. (1995). Self-efficacy beliefs and general mental ability in mathmetical problem-solving. *Contemporary Educational Psychology, 20*(4), 426–443. doi:10.1006/ceps.1995.1029.
Pajares, F., & Miller, D. (1994). Role of self-efficacy and self-concept beliefs in mathematical problem solving: A path analysis. *Journal of Educational Psychology, 86*(2), 193–203. doi:10.1037/0022-0663.86.2.193.
Rieh, S. Y. (2002). Judgment of information quality and cognitive authority in the Web. *Journal of the American Society for Information Science and Technology, 53*(2), 145–161. doi:10.1002/asi.10017.
Rodino, M. (1997). Breaking out of binaries: Reconceptualizing gender and its relationship to language in computer-mediated communication. *Journal of Computer Mediated Communication, 3*(3), 0. doi:10.1111/j.1083-6101.1997.tb00074.x.
Rubin, V. (2010). On deception and deception detection: Content analysis of computer-mediated stated beliefs. In *Proceedings of the 73rd ASIS&T Annual Meeting on Navigating Streams in an Information Ecosystem, October 22–27, 2010: Vol. 47* (pp. 1–10). Pittsburgh, PA: ASIST. Article No. 32.
Rubin, V. L., & Camm, S. C. (2013). Deception in video games: Examining varieties of griefing. *Online Information Review, 37*(3), 369–387.
Savicki, V., Kelley, M., & Lingenfelter, D. (1996a). Gender and group composition in small task group using computer-mediated communication. *Computers in Human Behavior, 12*(2), 209–224. doi:10.1016/0747-5632(96)00003-9.
Savicki, V., Kelley, M., & Lingenfelter, D. (1996b). Gender, group composition and task type in small task groups using computer-mediated communication. *Computers in Human Behavior, 12*(4), 549–565. doi:10.1016/S0747-5632(96)00024-6.
Savicki, V., Kelley, M., & Oesterreich, E. (1999). Judgments of gender in computer-mediated communication. *Computers in Human Behavior, 15*(2), 185–194. doi:10.1016/S0747-5632(99)00017-5.
Schwarz, G. (1978). Estimating the dimension of a model. *Annals of Statistics, 6*(2), 461–464.
Sengupta, S. (2012, August 11). *Trust: Ill-advised in a digital age*. The New York Times Sunday Review.
Stieger, S., Eichinger, T., & Honeder, B. (2009). Can mate choice strategies explain sex differences? The deceived persons' feelings in reaction to revealed online deception of sex, age, and appearance. *Social Psychology, 40*(1), 16–25. doi:10.1027/1864-9335.40.1.16.
Thomson, R., & Murachver, T. (2001). Predicting gender from electronic discourse. *British Journal of Social Psychology, 40*, 193–208. doi:10.1348/014466601164812.
Toma, C. L., & Hancock, J. T. (2010). Reading between the lines: Linguistic cues to deception in online dating profiles. 978-1-60558-795-0/10/02. *ACM*.
Toma, C. L., Hancock, J. T., & Ellison, N. B. (2008). Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin, 34*, 1023–1036. doi:10.1177/0146167208318067.
Trevino, L. K., Lengel, R. H., Boodensteiner, W., Gerloff, E., & Muir, N. (1990). The richness imperative and cognitive style: The role of individual differences in media choice behavior. *Management Communication Quarterly, 4*(2), 176–197. doi:10.1177/0893318990004002003.
Trevino, L. K., Lengel, R. H., & Daft, R. L. (1987). Media symbolism, media richness and media choice in organizations. *Communication Research, 14*(5), 553–574. doi:10.1177/009365087014005006.
Tsikerdekis, M., & Zeadally, S. (2014). Online deception in social media. *Communications of the ACM, 57*(9), 72–80. doi:10.1145/2629612.
Twyman, N. W., Lowry, P. B., Burgoon, J. K., & Nunamaker, J. F., Jr. (2014). Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *Journal of Management Information Systems, 31*(3), 106–137. doi:10.1080/07421222.2014.995535.
Whitty, M. T. (2002). Liar, liar! An examination of how open, supportive and honest people are in chat rooms. *Computers in Human Behavior, 18*(4), 343–352. doi:10.1016/S0747-5632(01)00059-0.
Whitty, M. T., Buchanan, T., Joinson, A. N., & Meredith, A. (2012). Not all lies are spontaneous: An examination of deception across different modes of communication. *Journal of the Association for Information Science and Technology, 63*(1), 208–216. doi:10.1002/asi.21648.
Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1), 273–303. doi:10.2753/MIS0742-1222270111.
Xiao, B., & Benbasat, I. (2010). Product-related deception in e-Commerce: A theoretical perspective. *MIS Quarterly, 35*(1), 169–195.
Zhou, L., Burgoon, J. K., & Twitchell, D. P. (2003). *A longtudinal analysis of language behavior of deception in email* (pp. 102–110). Berlin Heidelberg: Springer-Verlag.

Zhou, L., Burgoon, J. K., Twitchell, D. P., Qin, T., & Nunamaker, J. F., Jr. (2004). A comparison of classification methods for predicting deception in computer–mediated communication. *Journal of Management Information Systems, 20*(4), 139–165.

Zhou, L., Shi, Y., Zhang, D., & Sears, A. (2006). Discovering Cues to Error Detection in Speech Recognition Output: A User-Centered Approach. *Journal of Management Information Systems, 22*(4), 237–270. doi:10.2753/MIS0742-1222220409.

Zhou, L., Twitchell, D. P., Qin, T., Burgoon, J. K., & Nunamaker, J. F., Jr. (2003). An exploratory study into deception detection in text-based computer-mediated communication. *IEEE*. doi:10.0-7695-1874-5/03.

Shuyuan Mary Ho is an assistant professor at School of Information, College of Communication and Information, at Florida State University. Her research focuses on trusted human-computer interactions, specifically addressing issues of cyber insider threats and online deception. She founded the iSensor Lab in 2010. iSensor Lab is primarily dedicated to sociotechnical research related to human factors (e.g., behavioral threat) in cyberspace. Experiments are conducted in a live but virtual laboratory. Her research utilizes social-psychological theories along with pragmatic viewpoints on language cues to create an innovative methodology for computational modeling of next generation behavioral inference systems. Her research has been funded by National Science Foundation as well as Florida State University Council of Research and Creativity, and appears in *Journal of Management Information Systems, Journal of the American Society for Information Science and Technology, Information Systems Frontiers, Information Processing and Management, IEEE, ACM*, and *Springer* etc. refereed publications.

Paul Benjamin Lowry is a Full Professor of Information Systems at the Faculty of Business and Economics, at the University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona and an MBA from the Marriott School of Management. He has published 85+ journal articles in *MIS Quarterly, Information System Research, J. of Management Information Systems, J. of the AIS, Information Systems J., European J. of Information Systems, IJHCS, JASIST, I&M, CACM, DSS*, and many others. He is an SE at*Decision Sciences* and *AIS-Transactions on HCI*. He serves as an AE at *MIS Quarterly* (regular guest), *European Journal of IS, Information & Management, Communications of the AIS*, and the *Information Security Education Journal*. He has also served as an ICIS, ECIS, and PACIS track chair in various security/privacy tracks. His research interests include organizational and behavioral security/privacy issues; HCI and decision sciences; e-commerce and supply chains; and scientometrics.

Merrill Warkentin is Professor of MIS and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual behaviors in the context of information security and privacy, has appeared in *MIS Quarterly, Decision Sciences, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Information & Management*, and others. He is the author or editor of seven books, and serves (or has served) as Associate Editor for *MIS Quarterly, Information Systems Research, Decision Sciences, European Journal of Information Systems, Information & Management*, and other journals. He is Senior Editor of the *AIS Transactions on Replication Research* and an Eminent Area Editor for *Decision Sciences*. His work has been funded by NATO, NSF, NSA, DoD, Homeland Security, IBM, and others. He is the Program Co-Chair for the 2016 AIS Americas Conference on Information Systems (AMCIS).

Yanyun Yang is an associate professor in the Department of Educational Psychology and Learning Systems at Florida State University. Her research interests include structural equation modeling, reliability estimation methods, factor analysis, and applications of advanced statistical techniques to applied research. She has published in journals such as *Behavioral Research methods, Educational and Psychological Measurement, Journal of Psychoeducational Assessment, Methodology, Psychometrika,* and *Structural Equation Modeling.* She is an associate editor for *Journal of Psychoeducational Assessment*.

Jonathan M. Hollister is a postdoctoral researcher at the Information Institute, College of Communication and Information, at Florida State University. His research interests include social information behaviors and digital literacy practices in massively multiplayer online role-playing games (MMORPGs), online research methods and ethics, as well as the depictions and uses of digital and critical literacies in popular media for both digital youth and adults.