Virtual Lies and Digital Truths: A Review of Research on Deception in Online Communication

Other titles in Foundations and Trends® in Information Systems

The Technological Emergence of AutoML: A Survey of Performant Software and Applications in the Context of Industry
Alexander Scriven, David Jacob Kedziora, Katarzyna Musial and Bogdan Gabrys
ISBN: 978-1-63828-322-5

Knowledge Paths in Design Science Research
Andreas Drechsler and Alan Hevner
ISBN: 978-1-63828-088-0

The Computer Self-Efficacy Construct: A History of Application in Information Systems Research
George M. Marakas, Miguel Aguirre-Urreta, Amin Shoja, Eunyoung Kim and Shangjun Wang
ISBN: 978-1-63828-080-4

IT Use and Identity: A Review and a Research Agenda
Michelle Carter, Victoria Reibenspiess, Yafang Li and Varun Grover
ISBN: 978-1-63828-072-9

Innovative, Creative and Sustainable Decision-Making in Changing Contexts
Patrick Humphreys and Amy Luk
ISBN: 978-1-63828-010-1

Information Technology Alignment and Innovation: 30 Years of Intersecting Research
Yolande E. Chan, Rashmi Krishnamurthy and Ali S. Ghawe
ISBN: 978-1-68083-816-9

Virtual Lies and Digital Truths: A Review of Research on Deception in Online Communication

Akmal Mirsadikov
Wichita State University
akmal.mirsadikov@wichita.edu

Alaa Nehme
Mississippi State University
a.nehme@msstate.edu

Ali Vedadi
University of Tennessee
avedadi@utk.edu

Kent Marett
Mississippi State University
kent.marett@msstate.edu

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Information Systems

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

A. Mirsadikov *et al.*. *Virtual Lies and Digital Truths: A Review of Research on Deception in Online Communication*. Foundations and Trends® in Information Systems, vol. 7, no. 3, pp. 253–309, 2024.

ISBN: 978-1-63828-369-0

Foundations and Trends® in Information Systems
Volume 7, Issue 3, 2024

Editorial Board

Editorial Scope

Foundations and Trends® in Information Systems publishes survey and tutorial articles in the following topics:

- IS and Individuals
- IS and Groups
- IS and Organizations
- IS and Industries
- IS and Society
- IS Development
- IS Economics
- IS Management
- IS Research Methods

Information for Librarians

Foundations and Trends® in Information Systems, 2024, Volume 7, 4 issues. ISSN paper version 2331-1231. ISSN online version 2331-124X. Also available as a combined paper and online subscription.

Contents

Virtual Lies and Digital Truths: A Review of Research on Deception in Online Communication

Akmal Mirsadikov[1], Alaa Nehme[2], Ali Vedadi[3] and Kent Marett[4]

[1] *Wichita State University, USA; akmal.mirsadikov@wichita.edu*
[2] *Mississippi State University, USA; a.nehme@msstate.edu*
[3] *University of Tennessee, USA; avedadi@utk.edu*
[4] *Mississippi State University, USA; kent.marett@msstate.edu*

ABSTRACT

Whether we like it or not, deceptive communication is an ever-present aspect of personal interactions, and it should come as no surprise that it is deeply embedded in communication over computer-mediated means. Researchers in the field of information systems have studied deceptive communication for decades, borrowing theories from referent fields and ultimately developing their own. As the technology involved progresses and becomes more sophisticated, the manner in which deception is manifested online also becomes more complicated and the consequences become more severe, leading to renewed calls for research in this area.

This monograph reviews the theoretical foundations found in past IS research on computer-mediated deception, highlighting key studies that have contributed to our understanding

Akmal Mirsadikov, Alaa Nehme, Ali Vedadi and Kent Marett (2024), "Virtual Lies and Digital Truths: A Review of Research on Deception in Online Communication", Foundations and Trends® in Information Systems: Vol. 7, No. 3, pp 253–309. DOI: 10.1561/2900000035.

of attempts to deceive others. The discussion then examines new directions that research should take in the hopes of inspiring more work in this critical area.

1

Introduction

For as long as people have communicated, they have had the opportunity and the ability to lie to each other. Though much of early human history is unrecorded, instances of deception exist throughout the historical record, from Ramesses telling the Egyptian people that his loss in the Battle of Kadesh was actually a great victory, to the Watergate scandal that brought the Nixon presidency to an end. Deception does not necessarily have to be judged as immoral; in fact, much of polite society could not exist without friends and family telling "white lies" to each other. As Oscar Wilde once wrote, "Deceiving others . . . that is what the world calls a romance." But more often than not, deception tends to be resented by the people who are targeted by the communication, whether verbally or in written form.

The emergence of information systems (IS) as a practical modality for communication brought along the potential for deceptive communication. Almost immediately, researchers in the field of information systems saw the need to understand how computer-mediated deception was similar to verbal and written deception, as well as a mission to determine how best to detect deception when it occurs online. In the very first issue of *MIS Quarterly*, Jenkins and Johnson (1977) recommended that

systems users establish a baseline pattern of language and behavior with a communicative partner in order to perceive adaptive behaviors that signal the possibility of deception. A few years later, the first meeting of the International Conference on Information Systems featured a number of presentations on research methods, with some warning to be wary of the presence of deception when conducting interviews (Turner, 1980). Over the next few decades, the field of information systems research slowly began focusing on deceptive information and communication, including studies on how group members can take advantage of online communicative channels to deceive others (Burke and Chidambaram, 1999) and on how training may help alert decision makers toward false information hidden in data repositories (Biros *et al.*, 2002). As research progressed, theories developed in referent fields like communication and criminology drifted into mainstream IS research, leading to a deeper understanding of how computer-mediated communication can both help and hinder people with goals to deceive others. This monograph reviews much of the literature that has been presented and published in information systems research outlets since those early days.

We would be remiss if we failed to discuss the consequences of allowing deceptive communication to be transmitted unfettered. As this monograph will lay out, there are many types of computer-mediated deception, some criminal and some not. Social engineering alone is estimated to cost individuals and businesses hundreds of millions of dollars a year (Quader and Janeja, 2021). There are also non-pecuniary losses to consider. Within organizations, whose very existence relies on computer-mediated communication, deception can undermine trust, internal relationships, decision-making processes, and task performance (Fuller *et al.*, 2011; George *et al.*, 2023). Prospective customers and business partners may not know whether to put stock in feedback, reviews, or "word of mouth" about a particular organization (Greyson and Costello, 2021). The amount of trolling, catfishing, and astroturfing found online continues to increase year after year, with many believing that these forms of deception will eventually erode faith in cultural and societal foundations that have been taken for granted for centuries (Kim and Dennis, 2019).

Accordingly, the two purposes of this monograph are to review previous research lying at the intersection of deception and computer-mediated communication and to examine future directions that this research may be attuned to. Deception is a universal phenomenon, one that is part and parcel to human interaction and one that naturally interests both researchers and laypeople alike. While the popular press has covered extreme instances of deceptive online communication when it occurs (e.g., Martineau, 2019), and social media sources provide it attention at various times (e.g., Wang, 2023), scientific theorizing and experimentation in this area has been undertaken for decades and continues to evolve as the technologies and methods change with time. As new varieties of online deception attract new researchers to the research effort, particularly within the field of management information systems, reviewing where the research stream originated and where it appears to be heading could be enlightening to those who hope to engage further with the topic.

This monograph is organized as follows. Following discussion defining and contextualizing deception within the field of information systems research, we review some of the prominent theories that have helped inform studies on the topic. This includes seminal theories developed in the field of communication and other referent disciplines and IS theory that has helped explain deceptive communication and its detection across computer-based modalities. Key findings and implications from across research disciplines are reviewed. Then, the incidence of deceptive communication across generations of media and technology platforms is discussed. Finally, the monograph concludes with an overview of potentially important research gaps and a call for interested researchers to continue investigating deception in computer-mediated communication, in whatever forms that may evolve into with time.

1.1 Definitions of Deception

Before proceeding with a review of research investigating deceptive communication transmitted through the use of information systems, it is imperative to define the term deception itself. It has been defined by

many researchers in a variety of communicative contexts, but at their core, the definitions often share some commonalities.

An example of the general definition of deception is that described by Buller and Burgoon as "a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver" (Buller and Burgoon, 1996, p. 205). The key word in this definition is "knowingly," as the intention of the communicator matters. Honest mistakes and accidental phrasing often occur, but the intent to mislead others separates deceptive communication from mistaken communication. The definition also suggests that the false message has been strategically designed to fool the message receiver, ruling out intentionally transparent messaging with little chance of success. Instead, deceptive communication intentionally presents inaccurate information as true and utilizes strategic choices like fabrication, selectivity, oversimplification, and omission of information (Miller and Stiff, 1993).

Levine (2001) adds more nuance to the definition by questioning whether deception is dichotomous or continuous. In other words, deception is commonly treated as being completely present or completely absent based on whether the intent is to mislead and whether the message has been designed with that intent. Instead, Levine argues, deception should be thought of as multidimensional based on how the information being presented has been manipulated. A message could contain 100 percent false information, or it could feature half truthful, half false information while still maintaining the same intent. This consideration has led many researchers to opt for study participants to assess the truthfulness of a message along a continuous scale rather than a dichotomous, all-or-nothing judgment.

Other definitions attempt to take the context of the deception into account, thereby introducing potential boundary conditions to the definition. One example is altruistic deception, which involves "circumstances in which lying is perceived as an act of kindness and love, such as when a lie might spare another person pain or suffering" (Kaplar and Gordon, 2004, p. 489). This type of deception appears to be most commonly associated with close interpersonal relationships in which one party hopes to spare the other person some pain by withholding the truth. In such cases, Kaplar and Gordon recommend referring to altruistic deceivers as

"lie tellers" rather than the harsher pejorative "liar." Another context receiving recent attention is whether the technology itself, in particular artificial intelligence, is capable of knowingly transmitting deceptive communication. As part of a larger debate around anthropomorphizing artificial agents, this subset of deception research challenges the traditional definitions of deception by questioning whether AI can truly form intentions to deceive others (Masters *et al.*, 2021).

References

Adzima, K. (2020). "Examining online cheating in higher education using traditional classroom cheating as a guide". *Electronic Journal of E-Learning*. 18(6): 476–493.

Alawadh, H. M., A. Alabrah, T. Meraj, and H. T. Rauf (2023). "Discourse analysis based credibility checks to online reviews using deep learning based discourse markers". *Computer Speech & Language*. 78.

Albayati, M. B. and A. M. Altamimi (2019). "An empirical study for detecting fake Facebook profiles using supervised mining techniques". *Informatica*. 43(1): 77–86.

Anderson, P. (2022). "On moderate and radical government whistleblowing: Edward Snowden and Julian Assange as theorists of whistleblowing ethics". *Journal of Media Ethics*. 37(1): 38–52.

Bagui, S. and H. Brock (2022). "Machine learning for Android scareware detection". *Journal of Information Technology Research*. 15(1): 1–15.

Banerjee, A. (1992). "A simple model of herd behavior". *The Quarterly Journal of Economics*. 107(3): 797–817.

Bareket-Bojmel, L., S. Moran, and G. Shahar (2016). "Strategic self-presentation on Facebook: Personal motives and audience response to online behavior". *Computers in Human Behavior*. 55: 788–795.

Berghel, H. (2023). "911 swatting, VoIP, and doxxing". *Computer*. 56(3): 135–139.

Biros, D. P., J. F. George, and R. W. Zmud (2002). "Inducing sensitivity to deception in order to improve decision making performance: A field study". *MIS Quarterly*. 26(2): 119–144.

Bond, C. and B. M. DePaulo (2006). "Accuracy of deception judgements". *Personality and Social Psychology Review*. 10: 214–234.

Bond, C., T. R. Levine, and M. Hartwig (2015). "New findings in nonverbal lie detection". In: *Detecting Deception: Current Challenges and Cognitive Approaches*. Ed. by P. A. Granhag, A. Vrij, and B. Verschuere. Wiley-Blackwell. 37–58.

Bozok, D. (2023). "Attitudes of students towards violations of academic integrity in online english courses". *Journal of Learning and Teaching in Digital Age*. 8(2): 209–220.

Briscoe, E. J., D. S. Appling, and H. Hayes (2014). "Cues to deception in social media communications". In: *Proceedings of the 47th Hawaii International Conference on System Sciences*. Waikoloa, HI, USA. 1435–1443.

Broeker, F. (2021). "We went from the anonymity of the internet into my private WhatsApp': Rituals of transition among dating app users in Berlin". *New Media & Society*.

Buller, D. and J. Burgoon (1996). "Interpersonal deception theory". *Communication Theory*. 6: 203–242.

Burgoon, J. K., J. P. Blair, and R. E. Strom (2008). "Cognitive biases and nonverbal cue availability in detecting deception". *Human Communication Research*. 34(4): 572–599.

Burgoon, J. K., F. Chen, and D. P. Twitchell (2010). "Deception and its detection under synchronous and asynchronous computer-mediated communication". *Group Decision and Negotiation*. 19: 345–366.

Burke, K. and L. Chidambaram (1999). "How much bandwidth is enough? A longitudinal examination of media characteristics and group outcomes". *MIS Quarterly*. 23(4): 557–580.

Calabro, S. (2018). "From the message board to the front door: Addressing the offline consequences of race and gender based doxxing and swatting". *Suffolk University Law Review*. 51(1): 55–74.

Cao, N., S. Ji, D. K. Chiu, and M. Gong (2022). "A deceptive reviews detection model: Separated training of multi-feature learning and classification". *Expert Systems with Applications*. 187.

Carlson, J. R. and R. W. Zmud (1999). "Channel expansion theory and the experiential nature of media richness perceptions". *Academy of Management Journal*. 42(2): 153–170.

Carlson, J. R. and J. F. George (2004). "Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity". *Group Decision and Negotiation*. 13(2): 191–210.

Carlson, J. R., S. Zivnuska, R. B. Harris, K. J. Harris, and D. S. Carlson (2016). "Social media use in the workplace: A study of dual effects". *Journal of Organizational and End User Computing*. 28(1): 15–31.

Che Ku Kassim, C. K. H. and N. R. Mohd Sallem (2023). "Intention to deceive: Undergraduates' perception of fraudulent excuse-making". *International Journal of Educational Management*. 37(1): 55–69.

Cross, K. (2019). "Toward a formal sociology of online harassment". *Human Technology*. 15(3): 326–346.

Cross, C., K. Holt, and T. J. Holt (2023). "To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud". *Criminology & Criminal Justice*.

Daft, R. L. and R. H. Lengel (1986). "Organizational information requirements, media richness and structural design". *Management Science*. 32(5): 554–571.

Daft, R. L., R. H. Lengel, and L. K. Trevino (1987). "Message equivocality, media selection, and manager performance: Implications for information systems". *MIS Quarterly*. 11(3): 355–366.

DeLuca, D. (2008). "A new model and theory of asynchronous creativity". In: *Encyclopedia of E-Collaboration*. Ed. by N. Kock. Hershey PA USA: IGI Global. 463–471.

Dennis, A. R. and S. T. Kinney (1998). "Testing media richness theory in the new media: The effects of cues, feedback, and task equivocality". *Information Systems Research*. 9(3): 256–274.

Dennis, A. R. and J. S. Valacich (1999). "Rethinking media richness: Towards a theory of media synchronicity". In: *Proceedings of the Hawaii International Conference on System Sciences*.

Dennis, A. R., R. M. Fuller, and J. S. Valacich (2008). "Media, tasks, and communication processes: A theory of media synchronicity". *MIS Quarterly*. 32(3): 575–600.

DePaulo, B. M., J. L. Lindsay, B. E. Malone, L. Muhlenbruck, K. Charlton, and H. Cooper (2003). "Cues to deception". *Psychological Bulletin*. 129: 74–118.

Derrick, D. C., T. O. Meservy, J. L. Jenkins, J. K. Burgoon, and J. F. Nunamaker Jr. (2013). "Detecting deceptive chat-based communication using typing behavior and message cues". *ACM Transactions on Management Information Systems*. 4(2): 1–21.

Di Salvo, P. (2021). "Securing whistleblowing in the digital age: SecureDrop and the changing journalistic practices for source protection". *Digital Journalism*. 9(4): 443–460.

Donath, J. S. (1999). "Identity and deception in the virtual community". In: *Communities in Cyberspace*. Ed. by M. Smith and P. Kollock. London, UK: Routledge. 37–68.

Donath, J. and D. Boyd (2004). "Public displays of connection". *BT Technology Journal*. 22: 71–82.

Dunbar, N. E., M. L. Jensen, D. C. Tower, and J. K. Burgoon (2014). "Synchronization of nonverbal behaviors in detecting mediated and non-mediated deception". *Journal of Nonverbal Behavior*. 38: 355–376.

D'Urso, S. C. (2006). "Channel expansion theory: A test of the dynamic nature of media richness perceptions". *Journal of Business Communication*. 43(3): 256–280.

D'Urso, S. C. and S. A. Rains (2008). "Examining the scope of channel expansion: A test of channel expansion theory with new and traditional communication media". *Management Communication Quarterly*. 21(4): 486–507.

Ekman, P. and W. V. Friesen (1969). "Nonverbal leakage and clues to deception". *Psychiatry*. 32(1): 88–106.

Ekman, P. (1985). *Telling Lies: Clues to Deceit in the Marketplace, Politics and Marriage*. New York, NY, USA: W. W. Norton.

Elmogy, A. M., U. Tariq, M. Ammar, and A. Ibrahim (2021). "Fake reviews detection using supervised machine learning". *International Journal of Advanced Computer Science and Applications*. 12(1).

Emery-Wetherell, M. and R. Wang (2023). "How to use academic and digital fingerprints to catch and eliminate contract cheating during online multiple-choice examinations: A case study". *Assessment & Evaluation in Higher Education*: 1–16.

Ewing, H., A. Anast, and T. Roehling (2016). "Addressing plagiarism in online programmes at a health sciences university: A case study". *Assessment and Evaluation in Higher Education*. 41(4): 575–585.

Federal Trade Commission (2017). Consumer Review Fairness Act: What Businesses Need to Know. URL: https://www.ftc.gov/business-guidance/resources/consumer-review-fairness-act-what-businesses-need-know.

Fernandez, V., P. Simo, J. M. Sallan, and M. Enache (2013). "Evolution of online discussion forum richness according to channel expansion theory: A longitudinal panel data analysis". *Computers & Education*. 62: 32–40.

Foltýnek, T., D. Dlabolová, A. Anohina-Naumeca, S. Razı, J. Kravjar, L. Kamzola, and D. Weber-Wulff (2020). "Testing of support tools for plagiarism detection". *International Journal of Educational Technology in Higher Education*. 17: 1–31.

Fuller, C., K. Marett, and D. Twitchell (2011). "An examination of deception in virtual teams: Effects of deception on task performance, mutuality, and trust". *IEEE Transactions on Professional Communication*. 55(1): 20–35.

Furnell, S. (2013). "Still on the hook: The persistent problem of phishing". *Computer Fraud & Security*. (10): 7–12.

Furner, C. P. and J. F. George (2012). "Cultural determinants of media choice for deception". *Computers in Human Behavior*. 28(4): 1427–1438.

Gao, L. (2020). "Technology advancements for whistleblowing reporting platforms and employees' decision to blow the whistle". *Accounting and the Public Interest*. 20(1): 172–192.

George, J. F. and A. Robb (2008). "Deception and computer-mediated communication in daily life". *Communication Reports*. 21(2): 92–103.

George, J. F., J. R. Carlson, and J. S. Valacich (2013). "Media selection as a strategic component of communication". *MIS Quarterly*. 37(4): 1233–1251.

George, J. F., P. Tilley, and G. Giordano (2014). "Sender credibility and deception detection". *Computers in Human Behavior*. 35: 1–11.

George, J. F., A. Mirsadikov, and B. E. Mennecke (2016). "Website credibility assessment: An empirical-investigation of prominence-interpretation theory". *AIS Transactions on Human-Computer Interaction*. 8(2): 40–57.

George, J. F., M. Gupta, G. Giordano, A. Mills, V. Tennant, and C. Lewis (2018). "The effects of communication media and culture on deception detection accuracy". *MIS Quarterly*. 42(2): 551–575.

George, J. F. and J. Luo (2019). "The effects of media differences and expertise on deception detection accuracy". *Journal of the Midwest Association for Information Systems*. 1(5).

George, J. F., A. Mills, G. Giordano, M. Gupta, V. Tennant, and C. Lewis (2023). "Toward a greater understanding of the use of nonverbal cues to deception in computer-mediated communication". *IEEE Transactions on Professional Communication*.

Gibbs, J., N. Ellison, and R. Heino (2006). "Self-presentation in online personals: The role of anticipated future interaction, self-disclosure, and perceived success in internet dating". *Communication Research*. 33: 1–26.

Gisondi, M. A., R. Barber, J. S. Faust, A. Raja, M. C. Strehlow, L. M. Westafer, and M. Gottlieb (2022). "A deadly infodemic: Social media and the power of COVID-19 misinformation". *Journal of Medical Internet Research*. 24(2).

Glazier, R. A. (2016). "Building rapport to improve retention and success in online classes". *Journal of Political Science Education*. 12(4): 437–456.

Greyson, D. and K. L. Costello (2021). *Emotional Strip-Mining: Sympathy Sockpuppets in Online Communities*. New Media & Society. 1–22.

Grice, P. (1989). *Studies in the Way of Words*. Harvard University Press.

Hancock, J. T., J. Thom-Santelli, and T. Ritchie (2004). "Deception and design: The impact of communication technology on lying behavior". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 129–134.

Hancock, J. T., K. Gee, K. Ciaccio, and J. M. H. Lin (2008). "I'm sad you're sad: Emotional contagion in CMC". In: *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*. 295–298.

Harrison, A. (2018). "The effects of media capabilities on the rationalization of online consumer fraud". *Journal of the Association for Information Systems*. 19(5): 408–440.

Hartwig, M., P. A. Granhag, L. A. Strömwall, and A. Vrij (2005). "Detecting deception via strategic disclosure of evidence". *Law and Human Behavior*. 29(4): 469–484.

Herdian, H., I. N. Mildaeni, and F. R. Wahidah (2021). "There are always ways to cheat academic dishonesty strategies during online learning". *Journal of Learning Theory and Methodology*. 2(2): 60–67.

Himelein-Wachowiak, M., S. Giorgi, A. Devoto, M. Rahman, L. Ungar, H. A. Schwartz, and B. Curtis (2021). "Bots and misinformation spread on social media: Implications for COVID-19". *Journal of Medical Internet Research*. 23(5).

Ho, S. M., J. T. Hancock, C. Booth, and X. Liu (2016). "Computer-mediated deception: Strategies revealed by language-action cues in spontaneous communication". *Journal of Management Information Systems*. 33(2): 393–420.

Ho, S. M. and J. T. Hancock (2018). "Computer-mediated deception: Collective language-action cues as stigmergic signals for computational intelligence". In: *Proceedings of the 51st Hawaii International Conference on System Sciences*. 1671–1680.

Hollis, L. (2018). "Ghost-students and the new wave of online cheating for community college students". *New Directions for Community Colleges*. 183: 25–34.

House, R., A. Watt, and J. M. Williams (2004). "Teaching Enron: The rhetoric and ethics of whistle-blowing". *IEEE Transactions on Professional Communication*. 47(4): 244–255.

Inwood, O. and M. Zappavigna (2021). "Ambient affiliation, misinformation and moral panic: Negotiating social bonds in a YouTube internet hoax". *Discourse & Communication*. 15(3): 281–307.

Jenkins, A. M. and R. D. Johnson (1977). "What the information analyst should know about body language". *MIS Quarterly*. 1(1): 33–47.

Judi, H. M. (2022). "Integrity and security of digital assessment: Experiences in online learning". *Global Business and Management Research*. 14(1): 97–107.

Jung, J., R. Bapna, J. Ramaprasad, and A. Umyarov (2019). "Love unshackled: Identifying the effect of mobile app adoption in online dating". *MIS Quarterly*. 43(1): 47–72.

Kahai, S. S. and R. B. Cooper (2003). "Exploring the core concepts of media richness theory: The impact of cue multiplicity and feedback immediacy on decision quality". *Journal of Management Information Systems*. 20(1): 263–299.

Kaplar, M. E. and A. K. Gordon (2004). "The enigma of altruistic lying: Perspective differences in what motivates and justifies lie telling within romantic relationships". *Personal Relationships*. 11(4): 489–507.

Karnouskos, S. (2020). "Artificial intelligence in digital media: The era of deepfakes". *IEEE Transactions on Technology and Society*. 1(3): 138–147.

Khan, W., K. Crockett, J. O'Shea, A. Hussain, and B. M. Khan (2021). "Deception in the eyes of deceiver: A computer vision and machine learning based automated deception detection". *Expert Systems with Applications*. 169.

Kim, A. and A. R. Dennis (2019). "Says who? The effects of presentation format and source rating on fake news in social media". *MIS Quarterly*. 43(3): 1025–1039.

Kristensen, R. (2017). "Extortion". *Anthropology and Humanism*. 42(2): 210–220.

Lamb, J. B. (2020). "Death by swat: The three elements of swatting". In: *Video Games Crime and Next-Gen Deviance*. Ed. by C. Kelly, A. Lynes, and K. Hoffin. Birmingham, UK: Emerald Publishing Limited. 73–89.

LaRose, R., R. Connolly, H. Lee, K. Li, and K. D. Hales (2014). "Connection overload? A cross cultural study of the consequences of social media connection". *Information Systems Management*. 31(1): 59–73.

Lazar, T. (2022). "Organizational scandal on social media: Workers whistleblowing on YouTube and Facebook". *Information and Organization*. 32(1).

Levine, T. R. (2001). "Dichotomous and continuous views of deception: A reexamination of deception ratings in information manipulation theory". *Communication Research Reports*. 18(3): 230–240.

Lim, C. P. and S. S. Sundar (2016). "Modality redundancy in multimedia learning: A cognitive load perspective". *Journal of Computer-Mediated Communication*. 21(5): 393–406.

Lo, S. K., A. Y. Hsieh, and Y. P. Chiu (2013). "Contradictory deceptive behavior in online dating". *Computers in Human Behavior*. 29(4): 1755–1762.

Madison, T. P., D. K. David Kim, and W. R. Davie (2022). "The COVID-19 infodemic: Algorithmic gatekeeping, confirmation bias, and social identity". In: *The Emerald Handbook of Computer-Mediated Communication and Social Media*. Ed. by J. H. Lipschultz, K. Freberg, and R. Luttrell. Bingley, UK: Emerald Publishing Limited. 103–116.

Marett, K. and J. F. George (2004). "Deception in the case of one sender and multiple receivers". *Group Decision and Negotiation*. 13(1): 29–44.

Marett, K. and M. Nabors (2021). "Local learning from municipal ransomware attacks: A geographically weighted analysis". *Information & Management*. 58(7).

Martineau, P. (2019). "Internet deception is here to stay – So what do we do now?" Accessed on April 1, 2024 from the December 30, 2019 edition of *Wired*.

Masters, P., W. Smith, L. Sonenberg, and M. Kirley (2021). "Characterising deception in AI: A survey". In: *Deceptive AI: First International Workshop, DeceptECAI 2020. Proceedings 1*. Santiago de Compostela, Spain, Montreal, Canada: Springer International Publishing. 3–16.

McCornack, S. A. (1990). *The Logic Behind Lies: A Rational Approach to Deceptive Message Production*. University of Illinois at Urbana-Champaign.

McCornack, S. A. (1992). "Information manipulation theory". *Communications Monographs*. 59(1): 1–16.

McCornack, S. A., K. Morrison, J. E. Paik, A. M. Wisner, and X. Zhu (2014). "Information manipulation theory 2: A propositional theory of deceptive discourse production". *Journal of Language and Social Psychology*. 33(4): 348–377.

McCornack, S. A. (2015). "Information manipulation theory". In: *The International Encyclopedia of Interpersonal Communication*. John Wiley & Sons, Inc.

Meservy, T., M. Jensen, J. Kruse, J. K. Burgoon, J. F. Nunamaker, D. Twitchell, G. Tsechpenakis, and D. Metaxas (2005). "Deception detection through automatic, unobtrusive analysis of nonverbal behavior". *IEEE Intelligent Systems*. 20(5): 36–43.

Miller, G. and J. Stiff (1993). *Deceptive Communication*. Newbury Park, CA: Sage Publications, Inc.

Miranda, S. M. and C. S. Saunders (2003). "The social construction of meaning: An alternative perspective on information sharing". *Information Systems Research*. 14(1): 87–106.

Mirsadikov, A. and J. George (2023). "Can you see me lying? Investigating the role of deception on gaze behavior". *International Journal of Human-Computer Studies*. 174.

Mirsadikov, A., A. Vedadi, and K. Marett (2024). "Detecting deception in computer-mediated communication: The role of popularity information across media types". *Information & Computer Security*. Forthcoming.

Modgil, S., R. K. Singh, S. Gupta, and D. Dennehy (2021). "A confirmation bias view on social media induced polarisation during Covid-19". *Information Systems Frontiers*: 1–25.

Moore, S. (2023). "The momo challenge and the intersection of contemporary legend and moral panic". *Contemporary Legend*. 1: 1–34.

Natale, S. (2023). "AI, human-machine communication and deception". In: *The Sage Handbook of Human-Machine Communication*. Ed. by A. Guzman, R. McEwen, and S. Jones. London UK: Sage Publications. 401–408.

Novak, A. N. (2020). "Lawsuits and organizational control". In: *The New Review Economy*. New York City, NY USA: Routledge. 76–89.

Olesen, T. (2022). "Whistleblowing in a time of digital (in)visibility: Towards a sociology of 'grey areas'". *Information, Communication & Society*. 25(2): 295–310.

O'Malley, R. L. and K. M. Holt (2022). "Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime". *Journal of Interpersonal Violence*. 37(1–2): 258–283.

Ormond, D., M. Warkentin, A. Johnston, and S. C. Thompson (2016). "Perceived deception: Evaluating source credibility and self-efficacy". *Journal of Information Privacy and Security*. 12(4): 197–217.

Perry, N. (1998). "Indecent exposures: Theorizing whistleblowing". *Organization Studies*. 19(2): 235–257.

Pethers, B. and A. Bello (2023). "Role of attention and design cues for influencing cyber-sextortion using social engineering and phishing attacks". *Future Internet*. 15(1): 29.

Pienta, D., J. B. Thatcher, and A. Johnston (2020). "Protecting a whale in a sea of phish". *Journal of Information Technology*. 35(3): 214–231.

Qin, L., Q. Sun, Y. Wang, K. F. Wu, M. Chen, B. C. Shia, and S. Y. Wu (2020). "Prediction of number of cases of 2019 novel coronavirus (COVID-19) using social media search index". *International Journal of Environmental Research and Public Health*. 17(7).

Quader, F. and V. P. Janeja (2021). "Insights into organizational security readiness: Lessons learned from cyber-attack case studies". *Journal of Cybersecurity and Privacy*. 1(4): 638–659.

Qureshi, K. A., R. A. S. Malick, M. Sabih, and H. Cherifi (2021). "Complex network and source inspired COVID-19 fake news classification on Twitter". *IEEE Access*. 9.

Rains, S. A. (2007). "Understanding the dynamic nature of media choice: A theoretical framework for the study of media selection". *Communication Theory*. 17(2): 145–175.

Randall, D. (2011). "Ten red balloons: Virtual teams and online communities". *iS Channel*. 6(1): 13–21.

Rockmann, K. W. and G. B. Northcraft (2008). "To be or not to be trusted: The influence of media richness on defection and deception". *Organizational Behavior and Human Decision Processes*. 107(2): 106–122.

Roulet, T. J. and R. Pichler (2020). "Blame game theory: Scapegoating, whistleblowing and discursive struggles following accusations of organizational misconduct". *Organization Theory*. 1(4): 1–30.

Sallnäs, E. L., K. Rassmus-Gröhn, and C. Sjöström (2000). "Supporting presence in collaborative environments by haptic force feedback". *ACM Transactions on Computer-Human Interaction*. 7(4): 461–476.

Saxton, G. D. and D. Neu (2022). "Twitter-based social accountability processes: The roles for financial inscriptions-based and values-based messaging". *Journal of Business Ethics*. 181(4): 1041–1064.

Sharabi, L. L. and J. P. Caughlin (2019). "Deception in online dating: Significance and implications for the first offline date". *New Media & Society*. 21(1): 229–247.

Sharmeen, S., Y. A. Ahmed, S. Huda, B. Koçer, and M. M. Hassan (2020). "Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches". *IEEE Access*. 8: 24522–24534.

Sheen, S., K. A. Asmitha, and S. Venkatesan (2022). "R-Sentry: Deception based ransomware detection using file access patterns". *Computers and Electrical Engineering*. 103.

Siddiqi, M. A., W. Pak, and M. A. Siddiqi (2022). "A study on the psychology of social engineering-based cyberattacks and existing countermeasures". *Applied Sciences*. 12(12).

Statista (2023). "Most popular social networks worldwide". URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

Stephens, J. M., P. W. S. J. Watson, M. Alansari, G. Lee, and S. Turnbull (2021). "Can online academic integrity instruction affect university students' perceptions of and engagement in academic dishonesty? Results from a natural experiment in New Zealand". *Frontiers in Psychology*. 12: 569133.

Tambe Ebot, A. C., M. Siponen, and V. Topalli (2023). "Towards a cybercontextual transmission model for online scamming". *European Journal of Information Systems*.

Toma, C. L., J. T. Hancock, and N. B. Ellison (2008). "Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles". *Personality and Social Psychology Bulletin*. 34(8): 1023–1036.

Turner, R., C. Edgley, and G. Olmstead (1975). "Information control in conversations: Honesty is not always the best policy". *Kansas Journal of Sociology*. 11(1): 69–89.

Turner, J. A. (1980). "Improving the quality of information systems research". In: *Proceedings of the 1980 International Conference on Information Systems*. Philadelphia, PA, USA.

Vedadi, A., M. Warkentin, and A. Dennis (2021). "Herd behavior in information security decision-making". *Information & Management*. 58(8).

Vishwanath, A. (2015). "Diffusion of deception in social media: Social contagion effects and its antecedents". *Information Systems Frontiers*. 17: 1353–1367.

Vishwanath, A. (2017). "Getting phished on social media". *Decision Support Systems*. 103: 70–81.

Vrij, A. (2008). *Detecting Lies and Deceit: Pitfalls and Opportunities*. John Wiley & Sons.

Wang, Y. and S. S. Sundar (2016). "The role of redundancy in perceived interactivity: Effects of message and system redundancy on user engagement with a health website". *Journal of Computer-Mediated Communication*. 21(1): 50–64.

Wang, F. (2023). "Online romance scams: Research reveals scammers' tactics – and how to defend against them". Accessed on April 1, 2024 from the August 4, 2023 edition of *The Conversation*.

White, C. L. and B. Boatwright (2020). "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations". *Public Relations Review*. 46(5).

Whitty, M. T. and T. Buchanan (2016). "The online dating romance scam: The psychological impact on victims-both financial and non-financial". *Criminology & Criminal Justice*. 16(2): 176–194.

Whitty, M. (2019). "Who can spot an online romance scam?" *Journal of Financial Crime*. 26(2): 623–633.

Windeler, J. B. and A. Harrison (2018). "Rethinking media synchronicity theory: Examining the cooperative assumption". *DATABASE for Advances in Information Systems*. 49(4): 15–29.

Wright, R. T., M. Jensen, J. Thatcher, M. Dinger, and K. Marett (2014). "Research note—Influence techniques in phishing attacks: An examination of vulnerability and resistance". *Information Systems Research*. 25(2): 385–400.

Wright, R. T. and K. Marett (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.

Wright, R. T., S. L. Johnson, and B. Kitchens (2023). "Phishing susceptibility in context: A multi-level information processing perspective on deception detection". *MIS Quarterly*. 47(2): 803–832.

Xiao, B. and I. Benbasat (2011). "Product-related deception in e-commerce: A theoretical perspective". *MIS Quarterly*. 35(1): 169–195.

Young, J. A., J. F. Courtney, R. J. Bennett, T. S. Ellis, and C. Posey (2021). "The impact of anonymous, two-way, computer-mediated communication on perceived whistleblower credibility". *Information Technology & People*. 34(3): 1119–1151.

Zhang, P. and I. Benbasat (2004). "Online consumer behavior: An empirical study of factors influencing website browsing and purchasing". *Journal of the Association for Information Systems*. 5(1): 1–32.

Zhang, D., L. Zhou, and J. Lim (2020). "From networking to mitigation: The role of social media and analytics in combating the COVID-19 pandemic". *Information Systems Management*. 37(4): 318–326.

Zhou, L., J. K. Burgoon, J. F. Nunamaker, and D. Twitchell (2004). "Automating linguistics-based cues for detecting deception in text-based asynchronous computer-mediated communications". *Group Decision and Negotiation*. 13: 81–106.

Zhou, L. and D. Zhang (2006). "A comparison of deception behavior in dyad and triadic group decision making in synchronous computer-mediated communication". *Small Group Research*. 37(2): 140–164.

Zhou, L., J. Tao, and D. Zhang (2022). "Does fake news in different languages tell the same story? An analysis of multi-level thematic and emotional characteristics of news about COVID-19". *Information Systems Frontiers*. 25: 493–512.

Zuckerman, M., B. M. DePaulo, and R. Rosenthal (1981). "Verbal and nonverbal communication of deception". *Advances in Experimental Social Psychology*. 14: 1–59.