Why Lie?: Deception of Health Information

Emergent Research Forum (ERF)

Andrew S. Miller
Mississippi State University
asm357@msstate.edu

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Abstract

Individuals provide deceptive information in many contexts and for many reasons. We explore the phenomenon of medical patients providing deceptive information to their healthcare providers via both face-to-face and online interactions. We will employ the scenario-based factorial survey method to present research respondents with various situations in which they may consider whether or not to provide accurate or deceptive information. This method has been demonstrated to yield valid data for investigations of norm-violating behaviors. Results will be presented at the conference.

Keywords

Interpersonal deception theory, health information, patient data, NeuroIS, stigmatization

Introduction and Motivation

Deception has been studied in many contexts (Buller and Burgoon 1996; Faust 1995; Gross 2017; Lee and Welker 2015). Whereas the studies may vary in scope and research methods, most academic studies conclude that most humans practice deceptive behavior on a regular basis.

Deception can be harmful in several ways. First, it can have psychological impacts on those who are being deceived (Tsikerdekis 2017). Additionally, there can be financial burdens on those being deceived through fraud (Kirlidog and Asuk 2012; Proudfoot et al. 2016). However, there can also be harmful impacts that are self-inflicted by deception. Similarly, deceivers can inflict personal damage to themselves when the false information leads to negative outcomes, such as retribution from the deceived party.

Fraud and deception have been perpetrated by individuals in the business context, such as when Enron leaders defrauded their investors by misrepresenting their financial performance to investors (Wilson and Key 2012). Similarly, individuals engage in healthcare insurance fraud at an estimated cost in the billions of dollars every year (Rawte 2015). Within Information Systems research, online deception and digital deception detection have been investigated in the contexts of group support systems (George et al. 2008), information theft (Jenkins et al. 2018), gender identity (Ho et al. 2017), and fake malware warnings (Ormond et al. 2016). Deceptive information may be conveyed via direct (face-to-face) communication or via various computer-mediated technologies, and the ability to deceive the message recipient is media-dependent.

A critical context to investigate is the deception by patients who provide false information to healthcare providers. Unlike most deception in which the primary consequence is financial, the primary consequence of a patient withholding or lying about his or her health information is diminished care (Medin et al. 2016; Young et al. 2017). In some cases, this diminished care may lead to the patient's death. For example, if a person recently infected with human immunodeficiency virus (HIV) does not disclose that he or she has engaged in behaviors likely to lead to HIV when donating blood, contaminated blood may enter the blood supply (Brooks 2004). Healthcare-related deception is often difficult to detect, whether is it conveyed face-to-face or by computer-mediated means.

Theory

Patients deceive their health professionals for a variety of reasons, including fear of stigmatization, financial loss, and other personal loss. We will apply the interpersonal deception theory (IDT) to investigate how various scenarios are impacted by the components of this theory. IDT is a framework for determining the

process and common symptoms of deceptive behavior in face-to-face communication (Buller and Burgoon 1996). Specifically, IDT posits that senders of deceptive communication tend to exhibit certain communication patterns which are often detected by the receiving party (Buller and Burgoon 1996). Additionally, IDT research results have suggested individuals are likely to deceive in cases in which they fear stigmatization or financial loss or in cases where they seek sexual gratification or some perceived benefit (Burgoon 2006; Burgoon et al. 2014).

Stigmatization has negative effects in healthcare, and contributes to the failure to disclose sexual and disease history (Brooks 2004; Young et al. 2017). This fear typically occurs in marginalized communities, such as LGBT or economically disadvantaged people. This stigmatization stems from social pressure that is cast by community members. However, such fears have also been observed in the context of disclosing communicable diseases, such as HIV and Tuberculosis (TB) (Medin et al. 2016). Much of the fear of stigmatization felt by individuals infected with communicable diseases is a result of literal shunning by people for either health reasons or for religious/personal beliefs (Simpson 2017). It is with this background of stigmatization in the healthcare environment that our first hypothesis is developed.

H1: Perceived stigmatization is positively associated with intention to provide deceptive healthcare information.

Contrary to stigmatization, financial deception may be motivated by a desire for care (direct motivation) or a desire for money (indirect). When patients deceive to receive healthcare, they may fraudulently tell their doctor they are experiencing a type of pain that is covered by their health insurance plan, though they are actually experiencing a type of pain that is not covered by their health insurance plan (Palasinski 2009). This is an indirect deception that could allow them to obtain prescription pain medicine that is not normally covered by their health plan but will treat their actual condition. However, when patients deceive health professionals for personal financial gain, their deception is for direct gains. With this information, we develop our second hypothesis.

H2: The financial incentive to deceive is positively associated with intention to provide deceptive healthcare information.

An equally important research focus is the examination of the healthcare practitioner's ability to detect deception, whether it is conveyed orally (face-to-face) or via computer-mediated media, such as an electronic form entry. Deception detection in the healthcare context has been investigated from the healthcare practitioner's perspective (Fainzang 2002; Romanow et al. 2012; Simpson 2017; de Vries and Timmins 2016). However, there is not yet a study published in a high-impact journal which compares the difference in likelihood of deception in digital and face-to-face media.

Individuals often prefer to discuss embarrassing situations and conditions via digital media rather than face-to-face medium (Asher et al. 2017) to preclude the paraverbal and visual cues that are absent in digital media (Hart et al. 2010). In the healthcare context, this phenomenon could result in patients omitting "embarrassing" symptoms during in-person meetings with their healthcare provider.

H3: Patients who perceive their healthcare conditions to be embarrassing are more likely to engage in deception using face-to-face media than digital communication media.

Research results indicate that individuals are more capable of detecting deception in face-to-face contexts than in in digital communication contexts (Burgoon et al. 2010; Kahai and Cooper 2003). This is partially due to the relative "richness" of the in-person communication medium, as it allows for additional information to be communicated which can subconsciously convey deception (Kahai and Cooper 2003). Knowing this, individuals may prefer to use digital media when engaging in deception. Therefore, the fourth hypothesis is developed.

H4: Patients who intend to engage in financial fraud are more likely to engage in deceptive communication using digital communications media than face-to-face media.

Proposed Research

Research subjects asked about their use of deception are likely to be influenced by social desirability bias, making simple survey results problematic, so we will design and administer a scenario-based factorial survey research design which has been shown to be an effective way to study various deviant behaviors. The

general adult US population is our population of interest, given they are all potential healthcare patients. We will sample adults in the US, which has a unique healthcare environment. Appropriate sampling frames include Amazon Mechanical Turk or Qualtrics survey recipients. This research design and sampling frame have been successfully employed in similar research contexts (Barlow et al. 2013; Johnston et al. 2016; Trinkle et al. 2014; Willison et al. 2018)

The factorial survey design will present typical scenarios in which deception may occur, asking the respondents to anonymously indicate the likelihood that they may employ deception as the scenario character has in that situation, thereby uncovering more truthful responses. Versions of the scenarios will represent orthogonally-distinct levels of the independent variables that may be related to the dependent variable of deception intention.

We will also pursue the examination of deception detection by healthcare professionals by administering another set of scenario-based factorial surveys to healthcare professionals, in which we manipulate levels of various independent variables to determine their impact on deception detection outcomes.

Future Research

There is significant potential for future research in health information deception. Traditional research methods may enable us to evaluate the likelihood of attempts to deceive health professionals with self-report surveys or scenario-based factorial surveys. However, recent developments in so-called "NeuroIS" methods, including electroencephalography (EEG), galvanic skin response (GSR), eye-tracking, and other techniques, it may now be possible to determine intent more accurately (Krokoszinski and Hosser 2016) and explore the cognitive and affective processes associated with deceptive behaviors and communications.

Healthcare deception detection is another area that warrants investigation. How can healthcare organizations and healthcare providers utilize various methods to detect patient deception in face-to-face contexts and in computer-mediated media, such as online forms?

Additionally, there is the potential for future research that studies the impact of the deception more. In addition to the impacts of deception on patient care and outcomes mentioned above, future work could examine actual cases in which deception was used by the patient and the resulting outcomes.

Discussion

There are several practical applications of future research studies in this area. First, a healthcare provider could better understand why a patient may deceive them, enabling them to implement solutions to alleviate such reasons, such as making the medical facility more private. Additionally, healthcare providers may gain insight into common signs of deception and be better equipped to gain the information they need to perform quality medical care. Lastly, public health should increase, as the healthcare providers provide effective treatment to those with communicable diseases, thereby reducing their spread (Medin et al. 2016).

REFERENCES

Asher, Y., Stark, A., and Fireman, G. D. 2017. "Comparing Electronic and Traditional Bullying in Embarrassment and Exclusion Scenarios," *Computers in Human Behavior* (76), Elsevier Ltd, pp. 26–34.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers and Security* (39:PART B), pp. 145–159.

Brooks, J. P. 2004. "The Rights of Blood Recipients Should Supersede Any Asserted Rights of Blood Donors," *Vox Sanguinis* (87:4), pp. 280–286.

Buller, D. B., and Burgoon, J. K. 1996. "Interpersonal Deception Theory," *Communication Theory*, pp. 203–242.

Burgoon, J. K. 2006. "The Dynamic Nature of Deceptive Verbal Communication," *Journal of Language and Social Psychology* (25:1), pp. 76–96.

Burgoon, J. K., Chen, F., and Twitchell, D. P. 2010. "Deception and Its Detection under Synchronous and

Asynchronous Computer-Mediated Communication," *Group Decision and Negotiation* (19:4), pp. 345–366.

Burgoon, J. K., Proudfoot, J. G., Schuetzler, R., and Wilson, D. 2014. "Patterns of Nonverbal Behavior Associated with Truth and Deception: Illustrations from Three Experiments," *Journal of Nonverbal Behavior* (38:3), pp. 325–354.

Fainzang, S. 2002. "Lying, Secrecy and Power within the Doctor-Patient Relationship," *Anthropology & Medicine* (9:2), pp. 117–133.

Faust, D. 1995. "The Detection of Deception," *Neurologic Clinics* (13:2), pp. 255–265.

George, J. F., Marett, K., and Giordano, G. 2008. "Journal of the Association for Information Systems Deception : Toward an Individualistic View of Group Support Systems * Deception : Toward an Individualistic View of Group Support Systems," *Journal of the Association for Information Systems* (9:10), pp. 653–676.

Gross, B. 2017. "Theft by Deception," *Annals of the American Psychotherapy Association* (7:1), pp. 36–37.

Hart, C. L., Fillmore, D., and Griffith, J. 2010. "Deceptive Communication in the Workplace: An Examination of Beliefs about Verbal and Paraverbal Cues," *Individual Differences Research* (8:3), pp. 176–183.

Ho, S. M., Lowry, P. B., Warkentin, M., Yang, Y., and Hollister, J. M. 2017. "Gender Deception in Asynchronous Online Communication: A Path Analysis," *Information Processing and Management* (53:1), Elsevier Ltd, pp. 21–41.

Jenkins, J. L., Proudfoot, J. G., Valacich, J. S., and Nunamaker Jr., J. F. 2018. "Identifying Malicious Insider Threats through the Monitoring of Mouse-Cursor Movements," *Journal of the Association for Information Systems* (forthcomin).

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. 2016. "Dispositional and Situational Factors: Influences on Information Security Policy Violations," *European Journal of Information Systems* (25:3), pp. 231–251.

Kahai, S. S., and Cooper, R. B. 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), pp. 263–299.

Kirlidog, M., and Asuk, C. 2012. "A Fraud Detection Approach with Data Mining in Health Insurance," *Procedia - Social and Behavioral Sciences* (62), pp. 989–994.

Krokoszinski, L., and Hosser, D. 2016. "Emotion Regulation during Deception: An EEG Study of Imprisoned Fraudsters," *Journal of Criminal Psychology* (6:2), pp. 76–88.

Lee, C. C., and Welker, R. B. 2015. "Impressions That Arouse an Auditor's Suspicion of Lying in an Interview," *International Journal of Auditing* (19:3), pp. 295–306.

Medin, G., Garcia-Navarro, C., Navarro Gomez, M., Ramos Amador, J. T., Mellado, M. J., Jimenez, S., Munoz-Fernandez, M. A., Rojo Conejo, P., Saavedra, J., Garcia Hortelano, M., Guillen, S., and Gonzalez-Tome, M. I. 2016. "Disease Disclosure, Treatment Adherence, and Behavioural Profile in a Cohort of Vertically Acquired HIV-Infected Adolescents. NeuroCoRISpeS Study," *AIDS Care* (28:1), pp. 124–130.

Ormond, D., Warkentin, M., Johnston, A. C., and Thompson, S. C. 2016. "Perceived Deception: Evaluating Source Credibility and Self-Efficacy," *Journal of Information Privacy and Security* (12:4), Routledge, pp. 1–21.

Palasinski, M. 2009. "Testing Assumptions about Naivety in Insurance Fraud," *Psychology, Crime and Law* (15:6), pp. 547–553.

Proudfoot, J. G., Boyle, R., and Schuetzler, R. M. 2016. "Man vs. Machine: Investigating the Effects of Adversarial System Use on End-User Behavior in Automated Deception Detection Interviews," *Decision Support Systems* (85), The Authors, pp. 23–33.

Rawte, V. 2015. *Fraud Detection in Health Insurance Using Data Mining Techniques*.

Romanow, D., Cho, S., and Straub, D. W. 2012. "Riding the Wave : Past Trends and Future Directions for Health IT Research," *MIS Quarterly* (36:3), Iii–X.

Simpson, C. 2017. "Covering It Up ? Questions of Safety, Stigmatization, and Fairness in Covert Medication Administration," *The Journal of Law, Medicine & Ethics* (45), pp. 204–211.

Trinkle, B. S., Crossler, R. E., and Warkentin, M. 2014. "I'm Game, Are You? Reducing Real-World Security Threats by Managing Employee Activity in Online Social Networks," *Journal of Information Systems* (28:2), pp. 307–327.

Tsikerdekis, M. 2017. "Identity Deception Prevention Using Common Contribution Network Data," *IEEE Transactions on Information Forensics and Security* (12:1), pp. 188–199.

de Vries, J. M. A., and Timmins, F. 2016. "Deception and Self-Deception in Health Care," *Nursing Philosophy* (17:3), pp. 163–172.

Willison, R., Warkentin, M., and Johnston, A. C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal* (28:2), pp. 266–293.

Wilson, A. C., and Key, K. G. 2012. "Enron: A Case of Deception and Unethical Behavior," *Feature Edition* (2012:1), pp. 88–98.

Young, L. E., Jonas, A. B., Michaels, S., Jackson, J. D., Pierce, M. L., and Schneider, J. A. 2017. "Social-Structural Properties and HIV Prevention among Young Men Who Have Sex with Men in the Ballroom House and Independent Gay Family Communities," *Social Science and Medicine* (174), Elsevier Ltd, pp. 26–34.