A new paradigm for the experimental study of Malintent

Charles R. Honts

Psychology Department

Boise State University

Abstract

A new laboratory paradigm for the study of credibility assessment and deception concerning malintent was tested. Malintent may be a distinct concept from the traditional deception for past action that has been the subject of numerous studies. Sixty participants were either innocent or were given information and malintent to commit a theft. Participants were then screened for malintent using a modified Test for Espionage and Sabotage (TES). The TES was scored with the Kircher and Raskin (1988) discriminant analysis algorithm and produced better than chance results that were comparable to the results for the TES in a forensic deception detection setting. (Honts & Alloway, 2007). This new paradigm provides an experimental framework for exploring the concept of malintent and efforts to detect it.

Key Words: *malintent, deception detection, national security screening, portals*

A large body of research indicates that unassisted individuals, including trained forensic and security professionals are only slightly better than chance at detection deception (Hartwig & Bond, 2011). In the post 9-11 environment, the United States Government responded to the problem of assessing credibility at portals in several ways involving new research and the application of new techniques to the field setting (Honts & Hartwig, 2014). Unfortunately, all of those efforts are scientifically problematic because of poor methodology, and because they fail to address the conceptual differences between assessing credibility for intent to perform bad acts and assessing credibility for the commission of past acts (Honts & Hartwig). Polygraph examiners who do employment screening examination in law enforcement and national security face a similar credibility assessment problem as that faced at portals. Individuals may present themselves for polygraph screening with the malintent to perform bad actions if they are hired, but they may not, at the time of the polygraph screening have actually committed any bad acts. It is not clear how polygraph screening tests would perform under such circumstances.

Honts and Hartwig (2014) note that the deceptive context for assessing malintent differs in critical ways from assessing credibility concerning a past act. Most of the research conducted on credibility assessment has focused on the problem of detecting deception concerning statements about acts that took place in the past while the study of deception for intent has received little attention (Granhag, 2010). Most research is typified by asking questions about some event that the person either did or did not participate in the the past. A typical study from the past event deception literature would have a mock crime where some participants stole money and some

Corresponding Author:

Charles R. Honts
Psychology Department
Boise State University
1910 University Drive MS-1715
Boise ID 83716-5664 USA
chonts@boisestate.edu
Voice: 208.867.2027
FAX: 208.426.4386

did not (see Honts & Reavy, 2015 for a recent example). In such a setting the guilty person has the episodic memories associated with the criminal act and a concern for deception detection. Concern about deception detection then results in a variety of sequelae that involve masking the deception, monitoring the receiver and associated physiological and behavioral responses (Vrij & Gannis, 2014). For the innocent person, the concern that her or his truthful statements will not be believed is energized by the same potential consequences and sequelae as those faced by the guilty.

The deceptive context for assessing malintent at a portal or at an employment screening session is quite different (Honts & Hartwig, 2014). At the portal, or in employment screening situation, the innocent person is not the accused in a criminal investigation, and it seems doubtful that many innocent people approaching border or transportation portals, or employment screening, feel anything near the equivalent of the emotional response felt by a falsely accused criminal suspect. However, Honts and Hartwig also note that the truthful person at a portal may well feel anxious about the general process of screening. Nevertheless, it seems likely that for most innocent individuals, approaching a portal is a necessary inconvenience that may cause the innocent aggravation and minor anxiety, but little concern of true jeopardy (Honts & Hartwig). In an employment screening situation, a person without malintent seems unlikely to have much concern about questions concerning malintent. Certainly the concern and jeopardy for truthful individuals in an employment screening situation is much less than that of a falsely accused suspect in a criminal investigation.

For those intending to do bad acts if granted access, the deceptive context may also be different from the traditional situation (Honts & Hartwig, 2014). Those intending to do bad acts, may not have, as yet, have committed any bad acts, nor may they know specifically what their future bad acts might be. Those with malintent want to pass the portal, or obtain the job, so that he or she can do bad acts in the future. The person with malintent may or may not have false credentials, but if it is their intention to do bad acts in the future, that is the central nature of their deception and the focus of a relevant credibility assessment. To date, little research has addressed credibility assessment for malintent in the deceptive context presented by portals or employment screening. It is simply not clear whether or not research done in a criminal/investigative context will generalize to a malintent situation.

There is a body of research concerning deception detection for intent. Typical of this research was a study by Vrij, Leal, Mann, and Granhag (2011). In Vrij, et al., participants were asked to pretend they were part of a mission to collect a package from a specified location and then deliver it somewhere else. Participants were told that they might be stopped by agents and were given a code exchange that would identify an agent as friendly or hostile. Participant were instructed to be truthful with friendly agents and to lie about their intent and mission to the hostile agents. While on the way to complete the mission participants were stopped and interviewed by either a friendly or a hostile agent. After completing the mission participants were stopped a second time and interviewed by a friendly or hostile agent. Data extracted from the interviews indicated that after the completed event were more markers of plausibility and they contained more details than the interviews about intention. However, when undergraduate college students were asked to evaluate transcripts of the interviews no significant effects of intention versus completed event were found.

Although Vrij et al., tested the detection of intent, I would argue that they did not test malintent because in both the truthful and deceptive conditions every participant had exactly the same knowledge. While this created a powerful experiment design, it is not representative of conditions in the field. The lack of any specific motivation associated with deception detection is also troubling. Kircher, Horowitz and Raskin (1988) reported a meta-analysis that found explicit motivation was an important variable in predicting laboratory accuracy rates with polygraph tests. Some other studies that tested intent, but without malintent or specific motivation associated with deception detection were reported by Meijer, Verschuere, and Merckelbach (2010), Sooniste, Granhag, Knieps and Vrij (2013), and Vrij, Granhag, Mann, and Leal, (2011).

The paradigm described in this study was an attempt to model the critical aspects of malintent detection in a laboratory paradigm. For purely pragmatic reasons we decided to use psychophysiological deception detection (PDD) methods and technology. There is a substantial literature on the use of PDD to assess credibility in both forensic and screening settings (Raskin & Kircher, 2014). Although clearly not perfect, PDD has consistently shown better

than chance performance in both forensic and screening settings and provides a substantial amount of information gain over unassisted deception across a wide range of base rates (Honts & Schweinle, 2009). Although PDD in its present form is clearly not applicable to airport portals, it is used in national security, and law enforcement employment screening situations. Moreover, the substantial database of deception detection in traditional settings provides a stable reference for initial efforts to detect malintent.

Method

Participants

Participants were 60 college students enrolled in General Psychology classes. The participants received course credit for their participation and as part of the manipulation described below some participants had the possibility to win $14 in movie passes. Participants average age was 20.7 years, *SD* = 3.16, and 37 (62%) of the participants were men.

Apparatus

The apparatus was the same as that used in Honts and Alloway (2007). Physiological data were collected with a Stoelting commercial polygraph instrument running version 3.2 of the Computerized Polygraph System (CPS) software (Kircher & Raskin, 2002). Respiration data were collected from Pneumotrace sensors placed over the upper chest and the abdomen. Skin conductance was collected from two Ag-AgCl electrodes placed on the palmar surface of the distal phalanx of the first and third finger of the participant's left hand. Relative blood pressure was recorded from an inflated cuff placed around the participant's upper right arm. Vasomotor activity was recorded from the palmar surface of the participant's left thumb. Movement was monitored with a sensor placed under the legs of the participant's chair. The CPS software was used to edit artifacts from data and evaluate the data.

Procedure

Participants were recruited through the General Psychology course signup software. They were responding to an ad for a research project where participants might be asked to lie and then take a polygraph test. On arrival, participants watched a video about their rights as research participants and were then given an informed consent form to review and sign. The video and form indicated to the participants that they could withdraw from participation at any time and still received their participation credit in General Psychology.

After agreeing to continue, the research assistant instructed the participants chose an envelope from a box. The research assistant then left the participant alone in the room. Participants thus opened that envelope in private. The envelope contained instructions to watch a second video and a password for that video. Two participation videos defined the two conditions of the study. The Innocent Participant video provided the following instructions: Some people approaching the portal polygraph examination were given the combination to the safe in Room A and those people have the intention of opening the safe and stealing something valuable within. However, as an innocent person you do not know the combination to the safe and you have no intention to steal anything. You will be given a polygraph test about knowing the combination to the safe, and about your intention to open the safe in Room A. Maintain your innocence and lack of knowledge during the polygraph and if you pass your polygraph you will be admitted to Room A. There you will be immediately debriefed and your participation will be over. However, if you fail the polygraph you will be taken to Room B where you will watch a 30-minute educational film (TV Eye, 1983) and then you will be debriefed.

The Malintent Participant video (with the same person as shown in the Innocent Video) provided the following instructions: Some of the participants are going to be given the combination to the safe in Room A. You are one of those persons. The combination to the safe is 1 0 6 A. You will be given a polygraph about your knowledge of the combination and about your intention to rob the safe. If you are successful in passing the polygraph, you will be admitted to Room A where you can open the safe and take movie passes worth $14. You will be allowed to keep those movie passes. To pass the polygraph you must maintain your lack of knowledge and intention through the entire examination. If you fail the polygraph you will be taken to Room B where you will watch a 30-minute educational video and then you will be debriefed. Failing the polygraph means you will never have the chance to take the movie passes.

Using methods similar to those used

by Honts and Alloway (2007) all Participants were then tested with a standard field polygraph instrument and they were given a complete polygraph using a modified version of Test for Espionage and Sabotage (TES; Department of Defense Polygraph Institute Research Division Staff, 1999). The TES was chosen so that the results of our malintent polygraph could be directly compared to the results Honts and Alloway. The relevant questions of this examination were: Do you know the combination to the safe in Room A? Do you have a plan to open the Safe in Room A? If you are admitted to Room A, will you attempt to open the safe? Are you taking part in a plan to take something from the safe in Room A? Physiological data were collected from three repetitions of each relevant question. Following data collection the examiner used the discriminant analysis classification algorithm included in the CPS software (Kircher and Raskin, 1988; 2002) to classify the participant as truthful or deceptive. Depending upon the classification the participant was then taken to the room associated with their outcome. Participants who passed their examinations were given the movie passes and those who produced deceptive results on their examinations were asked to watch the educational film. Participants were then debriefed by a research assistant and were fully informed about the design of the experiment. Participant questions were answered.

Results

The discriminant analysis procedure used in this study (Kircher & Raskin, 1988); provided as part of the CPS software) produced an a posteriori probability of truthfulness (p|T) that can be considered by itself for its direct informative value or used against a cut score for classification. Those $p|T$ values were then tested to see if deception detection was possible in this setting. An independent groups t-test of the $p|T$ values indicated that significant detection was obtained, $t(58) = 3.26$, $p = 0.002$. The $p|T$ for Innocent participants ($M = 0.69$, $SD = 0.37$) was higher than for Malintent participants ($M = 0.39$, $SD = 0.34$). The correlation between the guilt criterion and the $p|T$ values was 0.394, $p < .01$. These results are similar to those reported by Honts and Alloway (2007) for the TES in a forensic setting (Innocent $M = 0.72$ and Guilty $M = 0.40$). If decisions were made so that $p|T > .5$ were classified as truthful and $p|T$ values $< .5$ were deceptive, 70% of the malintent and 67% of the innocent individuals were classified correctly. That classification was significantly above chance, $\chi^2 = 8.01$ (1), $p = .004$, Kendall's *tau-b* = .37, $p = .002$, and was again similar to the performance of the TES in Honts and Alloway's (2007) forensic paradigm.

Discussion

The present results provide a proof of concept for a new paradigm to assess malintent. Malintent participants approached a screening task not having committed a transgression in the past, but with knowledge and intent to commit a transgression if they were able to pass the screening. Innocent participants approached the screening task without malintent or malintent related information and were motivated to pass the screening to avoid delay. A modified version of the U. S. Government's Test for Espionage and Sabotage, a psychophysiological deception detection test, was used as the credibility assessment tool. The TES was able to discriminate malintent from innocent participants at better than chance levels. The performance of the TES in this malintent paradigm was much better than that reported for unassisted individuals (Hartwig, Granhag, & Luke, 2014) and was comparable to the performance of the TES in a forensic laboratory paradigm (Honts & Alloway, 2007). Unfortunately, the nature of the equipment and the time necessary for administration of the TES make it an unreasonable candidate for use a high volume portals, although it is currently used for employment screening in national security screening settings in the United States (Department of Defense Polygraph Institute Research Division Staff, 1998).

Nevertheless, these results validate this paradigm as a way to establish a basic malintent paradigm. The paradigm is easy to implement and should be easily adaptable to a variety of manipulations that would allow for the explication of the malintent construct. Research is urgently needed to define the limits and nature of the malintent concept. Although already being widely attempted in the field (Honts & Hartwig, 2014), such basic research would seem to be absolutely necessary before legitimately applying techniques to detect malintent in the field.

References

Department of Defense Polygraph Institute Research Division Staff. (1998). Psychophysiological detection of deception accuracy rates obtained using the test for espionage and sabotage. *Polygraph, 27*, 68–73.

Granhag, P. A. (2010). On the psycho-legal study of true and false intentions: Dangerous waters and some stepping stones. *Open Criminology Journal, 3*(2), 3743. doi:10.2174/1874917801003020037

Hartwig, M., & Bond, C.F. (2011). Why do lie-catchers fail? A lens model meta-analysis of human lie judgments. *Psychological Bulletin, 137*, 643–659.

Hartwig, M., Granhag, P. A., & Luke, T. (2014). Strategic use of evidence during investigative interviews: The state of the science. In, Raskin, D. C., Honts, C. R., & Kircher, J. C. *Credibility assessment: Scientific research and applications:.* (pp. 1-36). Oxford, UK: Academic Press. http://dx.doi.org/10.1016/B978-0-12-394433-7.00001-4

Honts, C. R. & Alloway, W. (2007). Information does not affect the validity of a comparison question test. *Legal And Criminological Psychology, 12,* 311-312. (Available online in 2006)

Honts, C. R. & Hartwig, M. (2014). Credibility assessment at portals. In, Raskin, D. C., Honts, C. R., & Kircher, J. C. *Credibility assessment: Scientific research and applications:.* (pp. 37-61). Oxford, UK: Academic Press. http://dx.doi.org/10.1016/B978-0-12-394433-7.00002-6

Honts, C. R., & Reavy, R., (2015). The comparison question polygraph test: A contrast of methods and scoring. *Physiology and Behavior, 143*, 15-26. Published online 24 February 2015, doi:10.1016/j.physbeh.2015.02.028

Honts, C. R., & Schweinle, W. (2009). Information gain of psychophysiological detection of deception in forensic and screening settings. *Applied Psychophysiology and Biofeedback, 34,* 161-172. (Available online July 2009)

Kircher, J.C., Horowitz, S.W., Raskin, D.C., 1988. Meta-analysis of mock crime studies of the control question polygraph technique. *Law and Human Behavior, 12*, 79–90

Kircher, J. C., & Raskin, D. C. (1988). Human versus computerized evaluations of polygraph data in a laboratory setting. *Journal of Applied Psychology, 73*, 291-302.

Meijer, E. H., Verschuere, B., & Merckelbach, H. (2010). Detecting criminal intent with the concealed information test. *The Open Criminology Journal*, *3*, 44-47.

Raskin, D. C., & Kircher, J. C. (2014). Validity of polygraph techniques and decision methods. In, Raskin, D. C., Honts, C. R., & Kircher, J. C. *Credibility assessment: Scientific research and applications:.* (pp. 63-129). Oxford, UK: Academic Press. http://dx.doi.org/10.1016/B978-0-12-394433-7.00003-8

Sooniste, T., Granhag, P. A., Knieps, M., & Vrij, A. (2013). True and false intentions: asking about the past to detect lies about the future. *Psychology, Crime & Law*, *19*, 673-685.

TV Eye (1983). Telling the truth. Episode in TV Eye series, London, UK: Thames Color Productions.

Vrij, A., & Gannis, G. (2014). Theories in deception and lie detection. In, Raskin, D. C., Honts, C. R., & Kircher, J. C. *Credibility assessment: Scientific research and applications:.* (pp. 301-374). Oxford, UK: Academic Press. http://dx.doi.org/10.1016/B978-0-12-394433-7.00007-5

Vrij, A., Granhag, P. A., Mann, S. A., & Leal, S. (2011). Lying about flying: The first experiment to detect false intent. *Psychology, Crime & Law*, *17*, 611-620.

Vrij, A., Leal, S., Mann, S. A., & Granhag, P. A. (2011). A comparison between lying about intentions and past activities: Verbal cues and detection accuracy. *Applied Cognitive Psychology*, *25*, 212–218. http://dx.doi.org/10.1002/acp. 1665.

Author Note

The author would like to thank the following individuals for their work in collecting the data in this study: Scott McBride, Flavia Pittman, James Pittman, Adela Anderson, and Ashley Christiansen. Correspondence concerning this paper should be sent to the author at: Psychology Department, Boise State University, 1910 University Drive, Boise, ID 83725-1715 or chonts@boisestate.edu

Some of the results presented here were also given as a poster presented at the annual meeting of the Association for Psychological Science in Chicago: Honts, C. R., Pittman, F. A., Pittman, J. V., McBride, S. T., Anderson, A. B., & Christiansen, A. K., (2008, May). *A New Paradigm for the Study of Deception Detection at Portals*.