



Sleight of Hand: Identifying Concealed Information by Monitoring Mouse-Cursor Movements

Jeffrey L. Jenkins¹, Jeffrey G. Proudfoot², Joseph S. Valacich³, G. Mark Grimes⁴,
Jay F. Nunamaker, Jr.⁵

¹Brigham Young University, U.S.A., jeffrey_jenkins@byu.edu

²Bentley University, U.S.A., jproudfoot@bentley.edu

³University of Arizona, U.S.A., valacich@arizona.edu

⁴University of Houston, U.S.A., gmgrimes@bauer.uh.edu

⁵University of Arizona, U.S.A., jnunamaker@cmi.arizona.edu

Abstract

Organizational members who conceal information about adverse behaviors present a substantial risk to that organization. Yet the task of identifying who is concealing information is extremely difficult, expensive, error-prone, and time-consuming. We propose a unique methodology for identifying concealed information: measuring people's mouse-cursor movements in online screening questionnaires. We theoretically explain how mouse-cursor movements captured during a screening questionnaire differ between people concealing information and truth tellers. We empirically evaluate our hypotheses using an experiment during which people conceal information about a questionable act. While people completed the screening questionnaire, we simultaneously collected mouse-cursor movements and electrodermal activity—the primary sensor used for polygraph examinations—as an additional validation of our methodology. We found that mouse-cursor movements can significantly differentiate between people concealing information and people telling the truth. Mouse-cursor movements can also differentiate between people concealing information and truth tellers on a broader set of comparisons relative to electrodermal activity. Both mouse-cursor movements and electrodermal activity have the potential to identify concealed information, yet mouse-cursor movements yielded significantly fewer false positives. Our results demonstrate that analyzing mouse-cursor movements has promise for identifying concealed information. This methodology can be automated and deployed online for mass screening of individuals in a natural setting without the need for human facilitators. Our approach further demonstrates that mouse-cursor movements can provide insight into the cognitive state of computer users.

Keywords: Concealed Information, Mouse-Cursor Movement, Graded-Motor Response Analysis, Electrodermal Activity, Deception Detection, Video Emotion Analysis

France Belanger was the accepting senior editor. This research article was submitted on January 31, 2017 and went through two revisions.

1 Introduction

Organizational members who conceal information about adverse behaviors present a substantial risk to their organization. For example, insider threats—i.e., adversaries posing as trusted members of an organization—may conceal malicious acts, such as espionage or sabotage, resulting in significant danger to both the private and public sectors (Upton & Creese, 2014). Even a nonmalicious employee may conceal information about noncompliance with organizational policies (e.g., security policies, acceptable-use policies), which can render organizations vulnerable to attacks. Security incidents facilitated by information concealment are prevalent (PWC, 2016; Schulze, 2016), costing organizations hundreds of thousands of dollars on average per incident (Raytheon, 2015) and costing society tens of billions of dollars per year (Figliuzzi, 2012).

Being able to identify when people are concealing information about adverse behaviors is an extremely difficult, expensive, error-prone, and time-consuming task. For example, concealed information of malicious acts takes, on average, 256 days to detect (Gordover, 2016). Most organizations report not having appropriate controls in place to detect when a concealed attack is occurring (Schulze, 2016), and detection systems are plagued with high numbers of false positives (Monahan, 2015). Even simple violations to organizational policies (e.g., storing confidential information on portable devices) are difficult to detect, resulting in deterrence programs that are often inadequate (Park, Ruighaver, Maynard, & Ahmad, 2012). Thus, there is a need to create systems that supplement existing techniques to improve deception detection.

To address this challenge, we propose a novel approach to help identify concealed information: the monitoring of mouse-cursor movements in online screening questionnaires. Mouse-cursor movements can be monitored online in people's natural environments without any specialized hardware or software installed on their computers. Additionally, this approach can be mass-deployed online to screen individuals for concealed information and can trigger follow-up evaluations as needed. Alternatively, this approach can be used to further screen individuals who are already flagged as potential threats by existing systems, decreasing the number of false positives.

In this paper, we first present a specialized screening questionnaire—based on the concealed information test (CIT)¹—as a robust technique to screen for concealed information online. We then theoretically explain how mouse-cursor movements differ between people concealing information and people telling the

truth using this test. In doing so, we address the following research question: *How do mouse-cursor movements differ for people concealing information and people telling the truth in an online CIT-based questionnaire?*

Second, in an exploratory analysis to further validate our methodology, we compare people's mouse-movement responses to their electrodermal activity while they complete the online questionnaire. Electrodermal activity is the primary response mechanism of interest used in the polygraph-based CIT (Krapohl, McCloughan, & Senter, 2009). An electrodermal response refers to a change in the electrical properties of the skin, which vary with the skin's moisture level (Martini & Bartholomew, 2003). When a person conceals information while responding to a question (in our case, the online questionnaire), it causes arousal, thereby increasing the rate of sweat secretion on the skin, which increases the skin's ability to conduct an electrical current (i.e., increased electrodermal activity) (Fowles, 2007). As our screening questionnaire is based on the CIT, we compare whether changes in mouse-cursor movements correspond to changes in electrodermal activity. In doing so, we answer the following exploratory research question: *Do mouse-cursor movements correspond with changes in electrodermal activity during an online CIT-based questionnaire?*

We tested our hypotheses using an experiment during which participants concealed information in our CIT-based test after completing a questionable task: stealing credit card numbers in a mock scenario. In the experiment, we simultaneously measured the mouse-cursor movements and electrodermal activity of each participant. We found that mouse-cursor movements can significantly differentiate between people concealing information and people telling the truth in our online questionnaire. We also found that mouse-cursor movements can differentiate between concealed information and truth on a broader set of comparisons relative to electrodermal activity. Both mouse-cursor movements and electrodermal activity demonstrated the potential to be used for identifying concealed information with a similar accuracy rate. Mouse-cursor movements, however, yielded significantly fewer false positives than electrodermal readings. Our results demonstrate that the use of mouse-cursor monitoring shows promise for identifying concealed information. The methodology can be implemented online and automated to mass-screen individuals in their natural environments to facilitate existing detection systems without the bias of human facilitators. Furthermore, this approach demonstrates that mouse-cursor movements can provide insight into the cognitive state of computer users.

¹The CIT is a scientifically validated criminal interviewing technique that can be used in polygraph examinations.

2 Background

Developing systems to detect concealed information has been the focus of much research. In general, the research on detecting concealed information can be split into two complementary areas. First, several systems have been developed that look for cues indicating that information is being concealed, and other adverse behaviors, by monitoring information in a person's environment. For example, studies have provided solutions that assess system calls (Liu, Martin, Hetherington, & Matzner, 2005), social media (Kandias, Stavrou, Bozovic, & Gritzalis, 2013), weblogs (blogs) (Myers, Grimaila, & Mills, 2009), activity logs (Legg, Buckley, Goldsmith, & Creese, 2015), active directory logs (Hsieh, Lai, Mao, Kao, & Lee, 2015), and a variety of individual and personality characteristics (Agrafiotis et al., 2015) to detect concealed adverse behaviors. Sanzgiri & Dasgupta, (2016) group these techniques into several categories, including anomaly-based approaches, role-based access control, scenario-based approaches, using decoys and honeypots, risk analysis using psychological factors, and risk analysis using workflows.

Second, several systems have been developed that question people directly about concealed information and other adverse behaviors. These systems introduce stimuli into a person's environment (e.g., a screening questionnaire), then monitor the person's responses to identify indicators of concealed information associated with those stimuli (Nunamaker, Derrick, Elkins, Burgoon, & Patton, 2011; Twyman, Lowry, Burgoon, & Nunamaker, et al., 2014). Researchers working in this area have investigated several topics, including system-design principles (Derrick, Jenkins, & Nunamaker, 2011), system use and possible applications (Jensen, Lowry, Burgoon, & Nunamaker, 2010), various sensors to detect deception indicators (Proudfoot, Jenkins, Burgoon, & Nunamaker, 2016; Twyman, Elkins, Burgoon, & Nunamaker, 2014), the fusion of sensors designed to detect deception indicators (Derrick et al., 2010), people's perceptions and reactions to system adoption (Elkins, Dunbar, Adame, & Nunamaker, 2013), and understanding countermeasures against automated credibility assessment systems (Proudfoot et al., 2016a).

Our research specifically builds on and extends the second area of research by developing a theoretically sound, mass-deployable technique for detecting concealed information based on the CIT and mouse-cursor tracking. As opposed to other sensors typically used to detect concealed information (e.g., electrodermal activity), mouse-cursor movements can be monitored in the course of an online questionnaire using JavaScript without any special hardware or software required on the respondent's computer. Mouse-cursor movements can provide "high-fidelity, real-time motor traces of the mind (and) can reveal

'hidden' cognitive states that are otherwise not detectable by traditional measures" (Freeman & Ambady, 2011).

Researchers once believed that the mind's cognitive and motor systems were functionally independent. However, recent research is unequivocally demonstrating that hand movements can show powerful traces of internal cognitive processes (Anderson et al., 2015; Freeman, Dale, & Farmer, 2011; Hibbeln et al., 2017). For example, primate studies have shown that hand movements and mental dynamics are closely intertwined; the processing of perceptual information continually informs motor-cortical population codes *during* a decision-making process, rather than waiting until the end of a decision-making process (Cisek & Kalaska, 2005; Paninski, Fellows, Hatsopoulos, & Donoghue, 2004).

In human studies, neurophysiological findings have shown that the brain immediately shares its ongoing results with the motor cortex when categorizing visual stimuli (Freeman, Ambady, Midgley, & Holcomb, 2011). As information is shared with the motor cortex, the mind programs multiple movements concurrently in response to competing stimuli with action potential (Song & Nakayama, 2006; Song & Nakayama, 2008). These competing movement responses continuously influence subsequent behavior (Freeman, Ambady, Midgley et al., 2011). For example, hand movements have been shown to be predictive of cognitive processing, including decision conflict, difficulty judging the truthfulness of statements (McKinstry, Dale, & Spivey, 2008), deception (Duran, Dale, & McNamara, 2010; Monaro, Gamberini, Sartori, 2017), user identification (Ikehara et al., 2003), increased cognitive processing (Dale & Duran, 2011), emotion (Grimes, Jenkins, & Valacich, 2013; Hibbeln, Jenkins, Schneider, Valacich, & Weinmann, 2017), attention (Anderson et al., 2015), attraction toward distraction stimuli (Song et al., 2006; Song et al., 2008), language processing (Spivey, Grosjean, & Knoblich, 2005), interpretation of ambiguous sentences (Farmer, Cargill, Hindy, Dale, & Spivey, 2007), learning (Dale, Roche, Snyder, & McCall, 2008), attitude formation, concealment of racial prejudices (Wojnowicz, Ferguson, Dale, & Spivey, 2009), and dynamic competition in classification tasks (Dale, Kehoe, & Spivey, 2007; Freeman & Ambady, 2009; Freeman & Ambady, 2011; Freeman, Ambady, Rule, & Johnson, 2008), to name a few.

Three specific studies relevant to identifying concealed information include that of McKinstry et al. (2008), who had participants in a controlled study judge the truthfulness of statements using a mouse cursor on a computer screen to select "yes" for true statements and "no" for false statements. The results revealed that when participants answered questions with a greater uncertainty of truthfulness, their mouse-cursor movements showed greater fluctuations. Similarly,

Duran et al. (2010) used a Nintendo Wii remote to capture participants' hand movements while answering autobiographical questions either truthfully or falsely. Participants aimed the Wii controller at a wall that had the words "yes" or "no" projected onto the surface. When responding falsely, the responses had greater entropy. People's hand trajectories also reached peak velocity later in the movement, with a steeper curve toward the false option. Finally, a third study reported on the use of mouse-movement analysis to detect fake identities (Monaro et al., 2017). Participants in this study had to answer expected, unexpected, and baseline questions by moving a mouse. The researchers found that the observed mouse trajectories and participants' error rates could be used to accurately distinguish between liars and truth tellers. Clearly, a growing body of recent cognitive psychology and neuroscience research demonstrates a strong linkage between variations in hand movements and different types of cognitive activity, including deception.

We add to these studies in several ways. First, we pair mouse-cursor tracking with a theoretically sound questionnaire format—the concealed information test (CIT)—to robustly detect concealed information. We adjust the CIT to allow it to be deployed online to capture mouse-cursor movements. Second, we theoretically explain and empirically test how mouse-cursor movements can predict concealed information in both within-subject comparisons while answering baseline vs. key questions, as well as in between-subject comparisons while answering key questions (baseline and key questions are explained in the next section). Third, we validate our approach for detecting concealed information by comparing it with the primary sensor used in polygraph examinations: namely, electrodermal activity.

2.1 Concealed Information Test (CIT)

In this study, we pair mouse-cursor tracking with a theoretically sound questionnaire format—the concealed information test—to detect concealed information. The CIT is the most scientifically validated polygraph-based questioning technique (Ben-Shakhar & Elaad, 2003; Council, 2003; Fiedler, Schmid, & Stahl, 2002). The objective of the CIT is to detect whether a person has "inside", or "concealed", knowledge of an activity (e.g., stealing intellectual property) (Ben-Shakhar et al., 2003). In a standard CIT, the person being interviewed is asked several questions about specific key pieces of information (e.g., someone accessing and stealing sensitive data).

For example, in a context in which sharing sensitive information is prohibited, the interviewer may state, "We detected that one of our sensitive databases was accessed. If you accessed the data, you would know which database was breached". The interviewer then provides approximately six plausible answers, with one of the six being the database that was breached, to

which the interviewee responds "yes" or "no" as to their culpability (the answer associated with the incident of interest is referred to as the *key* item or question). The other five items should be plausible answers, yet unrelated to the adverse activity. These questions are termed *baseline* questions. When a truthful person completes the CIT, he or she will respond similarly to both the baseline and key questions. When a person concealing information is presented with a key question, however, he or she will have a detectable psychophysiological change as compared with the baseline questions (Krapohl et al., 2009). This reaction, referred to as an *orienting response*, is traditionally measured as variations in electrodermal activity. However, the CIT has been extended to include other responses in information systems research, including eye tracking (Proudfoot, Jenkins et al., 2016) and postural rigidity (Twyman, Elkins, et al., 2014).

We adapt the CIT format to allow us to implement it online and use it to capture mouse-cursor movements. First, whereas the traditional CIT is presented vocally to the respondent, we present stimuli (key items and baseline items) on a computer screen. Second, whereas people vocally answer "yes" or "no" during a traditional CIT, we have people answer each question using a computer mouse. Respondents are required to move the mouse from the bottom middle of the screen to one of the two upper corners of the screen, each of which contains a possible answer. For instance, if the computer screen displays the question, "Have you stolen any classified information?" the respondent must move the mouse from the lower middle of the screen to either "no" (to deny stealing classified information) or "yes" (if they wish to confess). Mouse-cursor movements are captured while the respondent is answering each question. An example is shown in Figure 1. This specialized protocol for responding to questions allows us to measure specific movement characteristics to identify concealed information.

3 Hypotheses

We now explain how concealing information influences mouse-cursor movements captured using our specialized CIT-based questionnaire. Based on the response activation model (Welsh & Elliott, 2004), we predict that people concealing information will indicate an attraction toward the truthful answer before committing to the deceptive answer. The response activation model explains the process through which competing responses (e.g., answering "yes" or "no") influence hand movements. As noted, the possible responses, in the context of a screening questionnaire, include "yes" to admit to an activity or "no" to deny an activity. The answer that the respondent ultimately chooses (e.g., "no" to deny the activity) is termed the *target stimulus*. The answer that is not chosen ("yes" to confess to the activity) is termed the *distraction stimulus*.

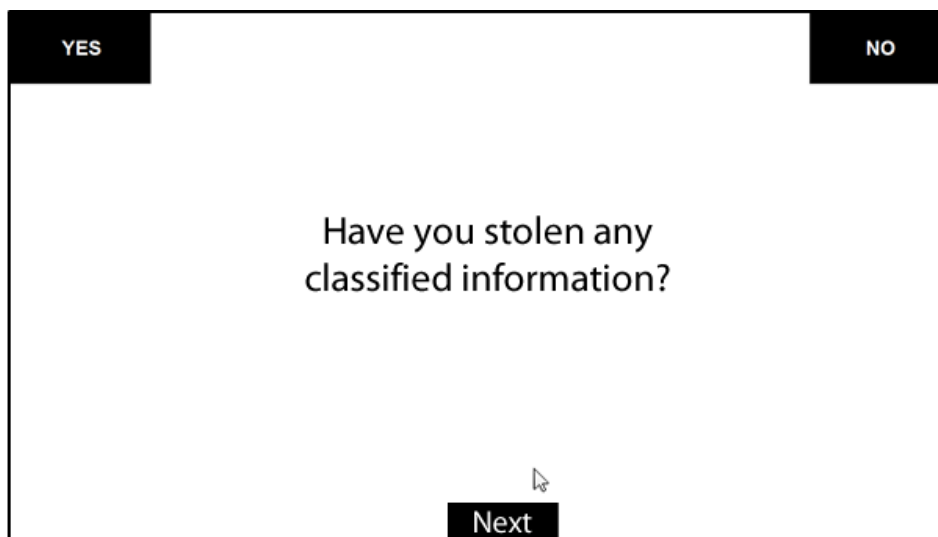


Figure 1. Example of a CIT Question

The response activation model posits that when a person considers both a target stimulus and a distraction stimulus as potential answers, the mind automatically starts to program motor movements toward each stimulus concurrently. Programming motor movements refers to sending nerve impulses to the hand to stimulate movement to possible destinations. This stimulus occurs even before the mind has fully determined which answer to choose, enabling more efficient movements for when the respondent actually does make a final decision (Georgopoulos, 1990; Song et al., 2006; Song et al., 2008; Tipper, Howard, & Jackson, 1997). For example, in the context of a person concealing information when answering a question, the mind will start programming movement to both the “yes” and “no” answers for a short period.

As the brain determines which answer the mouse cursor should be moved toward, it begins to inhibit programming to the distraction stimulus so that the final movement to the target stimulus can emerge (e.g., by eliminating the movement path toward confessing to an adverse activity) (Tipper et al., 1997; Welsh et al., 2004). Inhibition is not immediate, but rather occurs over a short period depending on the salience of the distraction stimulus. If a distraction stimulus is not salient (i.e., if it does not have personal significance to the respondent), then inhibition will occur very quickly (i.e., in less than a few hundred milliseconds). However, if the distraction stimulus is salient and thereby captures the respondent’s attention (e.g., the stimulus has personal significance to an individual because of concealed information), inhibition will occur more slowly (up to ~750 milliseconds or more) (Welsh et al., 2004).

When moving the hand before the inhibition is complete, the end result is a movement that is

somewhere in the middle of both stimuli (Welsh et al., 2004). For example, if the key stimulus (e.g., the “no” answer) is to the right, and the distraction stimulus (e.g., the “yes” answer) is to the left, the mind will start programming movements to both stimuli when they are shown. If the hand starts to move before the programming to the distraction stimulus is inhibited, the movement will consist of a combination of the two movements, resulting in a mouse trajectory that is closer to the middle of the two options until inhibition is complete. Figure 2 visualizes this outcome.

In the context of responding to a screening questionnaire, concealing information on a key question is a catalyst for creating a salient distraction stimulus. When people see a question regarding an adverse behavior they are guilty of committing, their attention briefly turns to the truthful answer, which, if chosen, would signify their guilt. The individual’s response to this salient question is exhibited as an orienting response (Krapohl et al., 2009; Lykken, 1959) and has been shown to cause detectable behavioral and physiological changes (King, 2002; Sokolov, 1963; Williams et al., 2000). For example, if someone is asked “Have you stolen any classified information?” and he or she is guilty, the truthful answer (“yes”) will be strongly salient and will catch the respondent’s attention. The respondent may even consider answering truthfully for a fraction of a second or longer before moving the mouse to the deceptive answer (“no”).

These factors slow down the inhibition process. Movements that occur during these times will be a product of the person’s inclination toward both truthful and deceptive answers (mouse-cursor movements will be biased toward the truthful answer but will ultimately move to the deceptive answer). However, when the same person is answering another question truthfully, one that is not about adverse activity, it is likely that

the person will perceive the “yes” answer to be marginally salient. In this case, the person is less likely to pay much attention to that option, if any attention at all. Thus, inhibition occurs more quickly (if at all) and is likely finished before the person’s hand starts moving. Hence, the subsequent mouse trajectory is not as biased toward the opposite answer. In summary, when answering baseline and key questions on our screening questionnaire, the response-activation time for people concealing information will be slower on

key questions than on baseline questions. The movement response subsequently will be more biased toward the opposite answer (see Figure 3). Thus, we propose the following hypothesis:

H1: Mouse trajectories of people concealing information will show greater attraction toward the opposite response on key questions than on baseline questions.

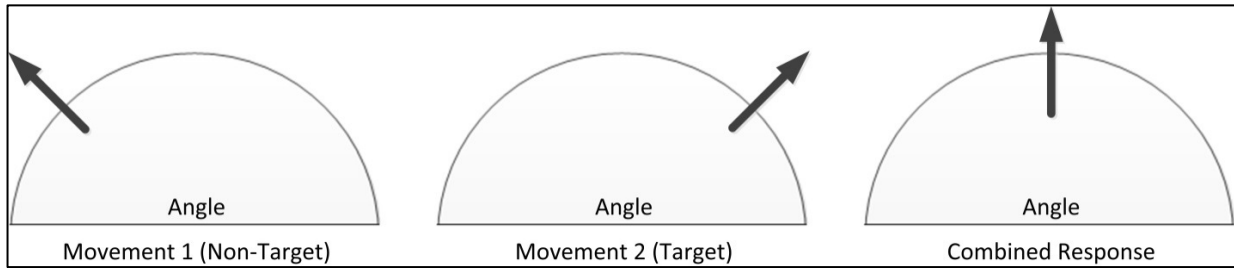


Figure 2. Combined Movement Resulting From Competing Motor Movements

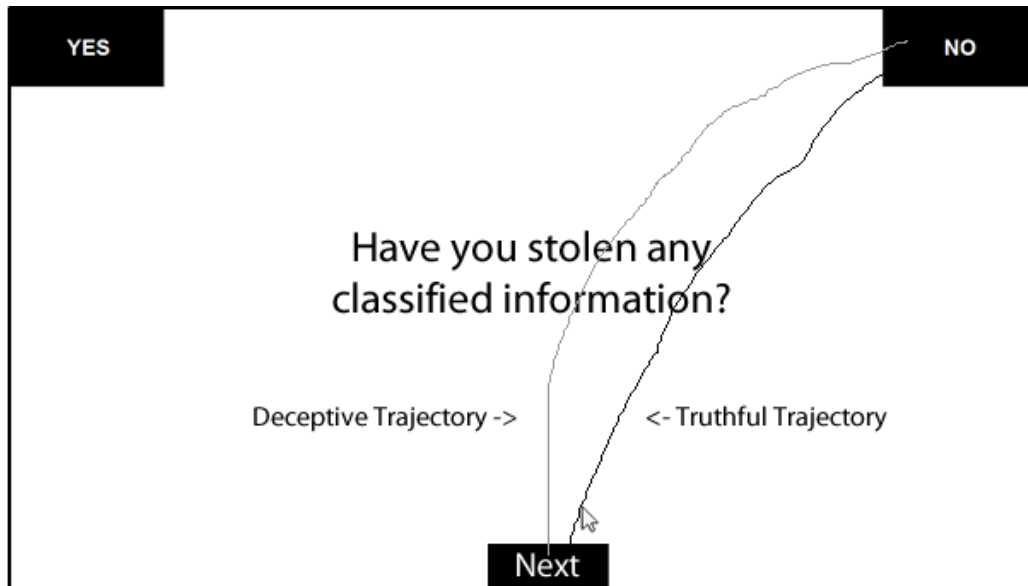


Figure 3. Example Trajectories of Truthful and Deceptive Responses

H1 compares how people concealing information answer key and baseline questions. We now predict how people concealing information differ from truthful people when answering key questions. When answering key questions, the opposite answer should be more salient for people concealing information than for truthful people. Truthful people are not anticipating any questions that will incriminate them, so they habitually may answer each question truthfully (with the “no” answer) without paying any attention to the alternative answer (Krapohl et al., 2009). Thus, the inhibition period will be very short. In such situations, trajectories may not be biased at all, even on key questions (Welsh et al., 2004). However, the inhibition

period for people concealing information will be longer, as they notice the truthful answer and must decide whether to deceive. This will cause a biased trajectory toward the opposite (truthful) answer. Accordingly, the mouse trajectories of people concealing information will be systematically biased toward the opposite answer, while truthful respondents’ mouse trajectories will not be biased toward the opposite answer to the same extent. Thus, we predict:

H2: Mouse trajectories of people concealing information will show greater attraction toward the opposite response on key questions than the mouse trajectories of truthful people.

Being deceptive requires heightened cognitive resources (Carrión, Keenan, & Sebanz, 2010). When being deceptive, people must first decide whether to tell the truth or be deceptive. During this process, deceivers weigh the risks and advantages of being deceptive. Once they decide to be deceptive, they must compose the deception. This often includes fabricating details and ensuring consistency in a face-to-face setting (Buller & Burgoon, 1996). Although an online setting may be a less-salient medium, people still often develop a cover story, just in case they are later confronted. Furthermore, people often take additional precautions online to ensure that their responses are deliberate (Derrick et al., 2011). As a result, people exert more cognitive effort when concealing information on key questions compared with answering benign baseline questions. Due to this increased cognitive effort, there is less working memory available for other tasks while concealers answer key questions.

When the consumption of cognitive resources increases, people's reaction times become slower (Unsworth & Engle, 2005). Slower reaction times lead to slower hand movements (Meyer, Abrams, Kornblum, Wright, & Smith, 1988; Meyer, Smith, Kornblum, Abrams, & Wright, 1990). Namely, when cognitive load is high and reaction time is slow, the brain has less cognitive ability to program movement. The brain is also slower in programming corrections to the movement trajectory when visually guiding the hand to its destination. One way the brain automatically compensates for this decrease in free cognitive resources is to spread the movement across a larger time span, which decreases the speed of movement (Meyer et al., 1988; Meyer et al., 1990). Allowing more time for movement allows the brain to program a comparable movement that could have occurred in a shorter time, given greater available resources (Hibbeln et al., 2017). As a result, people concealing information should move more slowly while responding to key questions relative to baseline questions, as cognitive resources are more constrained compared with when they are telling the truth on baseline questions. In summary, we hypothesize:

H3: People concealing information will move the mouse more slowly while responding to key questions, compared with responses to baseline questions.

Hypothesis 3 predicts that people who are concealing information will have a slower response speed on key questions, compared with their response time on baseline questions. We also predict that people who conceal information will differ from truthful people when answering key questions in terms of speed. Concealing information expends more cognitive resources to answer key questions than telling the

truth, since truthful people do not have to decide whether to tell the truth. As such, we predict that truthful people will answer key questions like they answer baseline questions, and since they have more free cognitive resources, they will move more quickly as a result (Meyer et al., 1988; Meyer et al., 1990). In addition, we predict that truthful people's mouse-movement speeds will be faster because they habituate to answering such questions. Neither baseline nor key questions are novel for truthful people (i.e., they are all viewed the same), so they can allow themselves to habituate to stimuli. This has been shown to increase the speed of people's mouse-cursor movements (Anderson et al., 2015). In summary, we predict:

H4: People concealing information will move the mouse more slowly when answering key questions, compared with truthful people.

4 Methodology

To test our hypotheses, we conducted an experiment in which people committed a questionably adverse act (a mock theft), then concealed information about this act while completing a screening questionnaire. Half of the participants were randomly assigned to commit the mock theft and conceal their involvement in the activity; the other half were asked to perform a benign activity. All participants—both in the concealed-information and truthful conditions—then completed a screening questionnaire using a computer, during which we tracked their mouse-cursor movements and electrodermal activity.

4.1 Procedures

A task was designed to mimic a realistic scenario in which half of the participants randomly committed a mock theft and concealed their involvement in the theft. Similar mock-crime experiments have been used widely in research to successfully mimic real-world deception scenarios (Burgoon, Blair, & Strom, 2008; Twyman, Lowry, et al., 2014; Twyman, Proudfoot, Schuetzler, Elkins, & Derrick, 2015; Valacich, Jenkins, Nunamaker, Hariri, & Howie, 2013). Although the task was sanctioned (i.e., participants were told to perform the illicit act and to appear innocent), the sanctioning was done indirectly, as a means of heightening both suspicion and anxiety. Participants registered for an appointment online and were randomly assigned to a concealed-information or truthful condition. Upon arriving at the experiment site, participants were given an envelope with instructions. They were instructed to enter the elevator (on the first floor), press a button to get to the fourth floor, and only then open the envelope and read the instructions.

Table 1. Guilty Participant Instructions

Your task is to commit a theft. You will go into the MIS department front office and steal a computer file that contains department credit card numbers. You will then go to room 109 for further instructions. **During the entire experiment, please try your best to appear innocent, do not raise any suspicion, and do not confess to committing the theft. If you are asked any questions about the theft, LIE.**

Below are the steps of your task:

1. Go to the MIS Department front office (see the first picture).
2. Go to the back-right corner of the reception area (circled in the lower picture; under the TV). Be confident. Don't talk with anyone unless talked to. If anyone asks what you are doing, say you are a TA, and you need to get a file.
3. Log in to the computer on the desk. Use the following credentials:
4. Username: **CHROME13admin**
5. Password: **manager**
6. You should see a picture of a red sports car as the desktop background and a file called "department credit card numbers"
7. Open the file to make sure it contains the department credit card numbers
8. Copy the entire file to the flash drive we gave you. You can plug the flash drive into the monitor or into the computer to the left side of the desk. **DO NOT REMOVE THE FILE, JUST COPY IT.**
9. Log out of the computer.
10. Go to room 109 with the flash drive when you are finished.

To make sure you remember the details of this theft, please answer the following questions:

What picture was on the desktop of the computer? _____

What information was in the file you stole? _____

Where did you copy the file to? _____

What password did you use to log in to the computer? _____

4.2 Concealed-Information Condition

The envelope for the concealed-information condition contained a set of instructions and a jump drive (see Table 1). Participants were instructed to go to the Management Information Systems department, log in to a computer in the front office using a set of credentials, and steal a file containing department credit card numbers. Participants were instructed to lie if confronted about the theft. Upon completing the tasks listed in Table 1, participants were then instructed to go to a room on the first floor. When they arrived at the room, an experiment facilitator explained that a theft had occurred and that the participant had been identified as a suspect in the theft. The participant was then asked to answer questions in a screening questionnaire.

4.3 Truthful Condition

Participants in the truthful condition were also given a folded piece of paper. They were instructed to enter the elevator (on the first floor), press the button to get to the fourth floor, then read the paper. Like the guilty

participants, the paper asked the truthful participants to go to the Management Information Systems department. However, rather than stealing information, innocent participants were asked to pick up a piece of paper (a free news article) at the front desk, then go back to the room on the first floor. Upon arriving at the room, an experiment facilitator explained that a theft had occurred and that the participant was a suspect in the theft. The participant was then asked to complete a screening questionnaire.

4.4 CIT-Based Screening Questionnaire

All participants completed a customized screening questionnaire based on the CIT. In designing the CIT-based test, we pilot-tested all of the items (key and baseline) to ensure that an innocent person would respond similarly to each item without unintended responses (e.g., to ensure some questions do not inherently elicit slower responses). We familiarized each participant with the format of the CIT through a practice test, in which the program required the respondent to move the mouse within the first second or the system would display an error. This helped

ensure that inhibition was not complete before movement occurred. Completing the practice test also reduced the likelihood that an orienting response would occur, due to the novel format of the test, and therefore confound our results (Krapohl et al., 2009). Screenshots and explanations of the CIT-based screening questionnaire are shown in Table 2.

4.5 Debrief

After completing the screening questionnaire, participants were debriefed on the true purpose of the study. In addition, participants completed a short questionnaire to report select demographic information.

4.6 Measures

We collected mouse-movement data, electrodermal data, and video during the screening questionnaire. Mouse-movement behavior collected during the administration of the CIT was captured using MouseTracker software (Freeman & Ambady, 2010; Freeman, Ambady, Midgley et al., 2011). This software captures mouse-cursor movements in terms of raw time, x-coordinate, and y-coordinate at approximately 70 hz (70 times a second). In addition, it performs transformations that allow for the comparison of trajectories across different screen resolutions and sizes. First, it rescales all mouse-trajectory data to a standard coordinate space (a 2 x 1.5 rectangle that is compatible with the aspect ratio of the computer screen). The top-left corner of the screen corresponds to -1, 1.5, and the bottom-right corner of the screen corresponds to 1,0. Thus, the starting position is at position 0,0. Second, it remaps all data so the mouse starts at position 0,0. Although the person must click a button at the middle-bottom of the screen to see the next item, the button's size allows for variations to exist (e.g., someone might actually click on the right side of the button). Thus, the trajectories are remapped for comparison. In our scenario, all participants used the same computer, which reduced the need to transform the data. However, to be consistent with past and future research, we also performed these transformations.

Using a polygraph machine, we also captured electrodermal responses using two sensors on the

pointer and ring fingers of the participants' nondominant hands (the hand not used to move the mouse). We allowed 12 seconds to transpire between the onset and offset of each question in the CIT to allow the individual's electrodermal activity to renormalize after reacting, before the onset of the next question (Gamer, Rill, Vossel, & Gödert, 2006).

Finally, using a high-definition web camera, we captured video of each participant's face during the interaction. We analyzed the video for emotion (fear) using computer-vision analyses as a check of validity (this will be explained in more detail later in the paper).

4.7 Participants

A total of 75 students were recruited for the experiment from an undergraduate business course; participants were incentivized with extra credit in the course. Of these, five participants in the guilty treatment refused to perform the mock-theft activity and four others confessed to committing the theft during the screening. This resulted in usable data from 66 participants (30 in the concealed-information treatment and 36 in the truthful condition). Fifty-nine percent of the participants were female, and the average age of participants was 21.8. The average number of years of college education per participant was 3.1. The most-represented nationalities were American (69%), Chinese (11%), and Mexican (9%). Twenty-nine percent of students were business-management majors, 27% were majoring in accounting, 20% in marketing, 15% in finance, and 9% in management information systems.

4.8 Evidence of Realism

We designed the experiment to mimic a real scenario in which someone would be deceptive. Field-based deception research reports that sanctioned laboratory work is indeed generalizable to real-world deception (Kircher & Raskin, 1988; Pollina, Dollins, Senter, Krapohl, & Ryan, 2004). The participants in the deceptive condition of our experiment concealed information during the automated screening questionnaire. Thus, our experiment represents a scenario in which deception was present.

Table 2. CIT Experiment

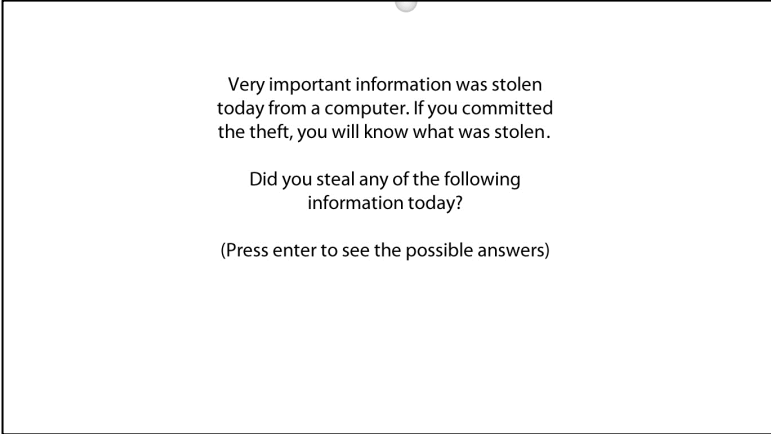
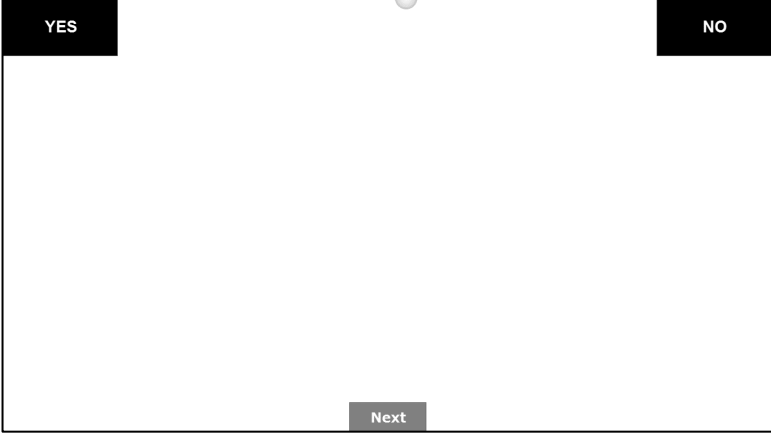
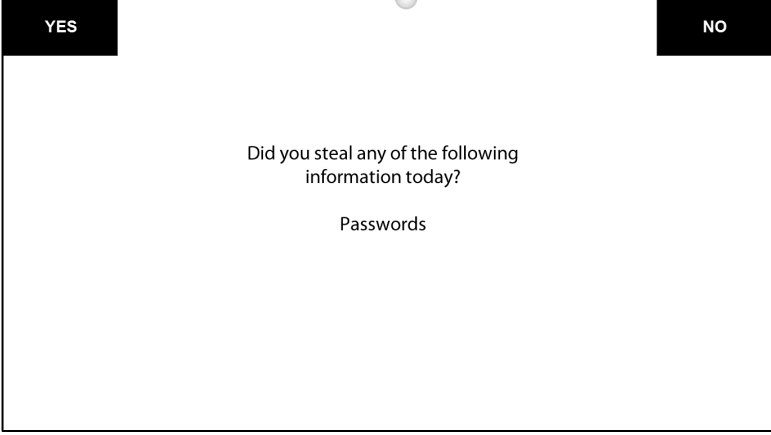
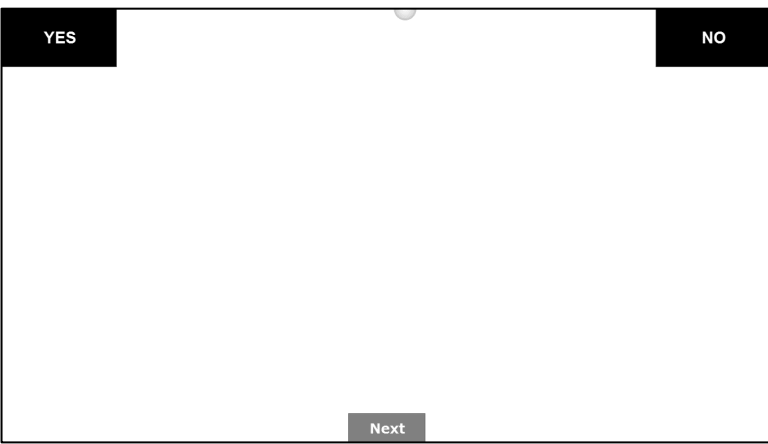
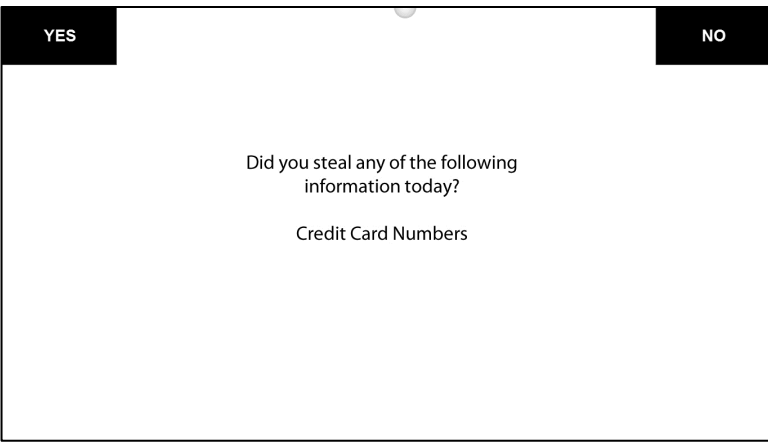
Screenshot	Explanation
 <p>Very important information was stolen today from a computer. If you committed the theft, you will know what was stolen.</p> <p>Did you steal any of the following information today?</p> <p>(Press enter to see the possible answers)</p>	<p>Beginning of the CIT explaining the purpose of the session.</p>
 <p>Next</p>	<p>After clicking on “enter”, the person must move the mouse to the bottom-middle of the screen to click on “next” before seeing the first item. This anchors the mouse in the same location for each item.</p>
 <p>Did you steal any of the following information today?</p> <p>Passwords</p>	<p>The first item (“passwords”) is shown. The person must move the mouse from the bottom-middle of the screen to the upper-right or upper-left corners to answer the question. The program requires the respondent to move the mouse within the first second, or it displays an error (the respondent becomes accustomed to this in the practice test preceding the CIT).</p>

Table 2. CIT Experiment

	<p>The mouse is anchored at the bottom of the screen, prior to displaying the next item.</p>
	<p>The respondent then sees the next stimulus. The process is repeated for the following items:</p> <ul style="list-style-type: none"> • Credit card numbers • Exam key • Social security numbers • Health records • Encryption codes <p>In this test, “credit card numbers” was the key answer, and the other items were baseline answers.</p>

However, we also examined qualitative and quantitative evidence to assess the extent to which our experiment exhibited outcomes resembling real-world deception scenarios. First, from a qualitative perspective, five of the participants in the concealment treatment refused to perform the mock-theft activity. When asked why they would not complete the task, they said stealing the information felt too unethical or immoral. Four other people admitted to committing the theft during the screening process, citing the same reasons for not lying. These refusals provide anecdotal evidence regarding the realism of the scenario and provide proof that it elicited feelings comparable to real-world deception.

As a means of gathering more objective evidence, we recorded video of participants’ facial expressions as they completed the online CIT using a high-definition web camera. We then used Microsoft’s Cognitive Service Emotion API to analyze microfacial movements indicative of fear. The assumption is that people who committed the theft should exhibit greater fear of being caught (because they were guilty) vs. the innocent participants. Each video was entered into the API and, in return, we received fear scores for each

frame of the video. To account for the multiple observations per participant, we used a linear mixed-model analysis. In the model, we specified the fear score as the dependent variable, the treatment as the fixed effect, and the participant ID as the random effect. The results demonstrated that people who were deceiving exhibited a higher level of fear than people who were telling the truth ($\beta = 0.020$; $t\text{-value} = 1.937$; $p < .05$; $R^2 = 0.361$), suggesting that the mock-theft scenario was realistic enough to cause a reaction that resembled real-life deception (i.e., increased fear).

As a final validation, we examined the electrodermal activity of participants who concealed information vs. truthful participants. In the real world, electrodermal activity increases when an individual is being deceptive. We found this pattern to hold in our experiment, further validating that we induced deception indicators resembling those exhibited in the real world (see the Section 5.7, “Exploratory Comparison to Electrodermal Activity Part A: Concealed-Information Key vs. Baseline Question”, for detailed statistical information).

5 Analysis

Each hypothesis was analyzed separately. Hypotheses 1 and 2 (which hypothesize greater attraction when concealing information) were analyzed using a graded motor-response analysis, a standard technique for comparing mouse-cursor trajectories (Dale et al., 2007). Hypotheses 3 and 4 (which hypothesize slower response speed when concealing information) were analyzed by comparing the mean-response speed for treatments and question types using linear mixed-effects modeling for Hypothesis 3 (as this comparison is within subjects) and a t-test for Hypothesis 4 (as this comparison is between subjects). Finally, we examined whether differences were also observed in electrodermal activity to address the second research question and to evaluate how mouse-cursor indicators compare with electrodermal-activity indicators in a simple decision-tree prediction model.

5.1 Graded Motor Response Analysis Description

The graded motor-response analysis is a well-established technique to test whether two mouse-movement trajectories are different from each other (Dale et al., 2007). In our analysis, we used the graded motor-response technique to see whether participants in the concealed-information condition showed significantly more attraction toward the opposite answer (which is the truthful answer for the concealed-information condition) on key questions, as compared with (1) their own responses to baseline questions, and (2) to truthful participants' responses to key questions.

As a prerequisite to the graded-motor response analysis, we first time-normalized the data. Time-normalized data provide information regarding the overall shape of the trajectories, which can be compared across conditions and people (Dale et al., 2007). The rationale for time normalization is that recorded trajectories tend to have different durations (i.e., some people simply move a mouse faster than other people). For example, consider a response from one person that lasts 800 milliseconds and a response from another person, who naturally moves slower, that lasts 1,600 milliseconds. If you try to compare the trajectories at 800 milliseconds for each response, you may not be comparing the same part of the trajectory—one respondent is finishing the movement while the other is still in the middle of the movement. Furthermore, it is impossible to compare trajectories at 1,600 milliseconds because the first did not last that long. Time normalization addresses this limitation by dividing the x,y coordinate pairs into 101 equal segments using linear interpolation. For each segment, the average x,y coordinate is computed based on the x,y coordinate pairs in that segment. For example, you can compare the end of one movement to the end of

another movement by running a statistical test on the average x or y coordinate in segment 101, or you can compare the middle of competing trajectories by analyzing segment 50.

In a typical graded motor-response analysis, differences between segments are tested using an appropriate statistical test (e.g., t-test, linear mixed-effects model). To avoid a possible increase in Type I error (alpha slippage) with running 101 tests when comparing the entire trajectory, overall trajectories are only deemed significantly different if eight segments in a row are significantly different from each other. This cutoff was determined through bootstrapping simulations to provide a conservative criterion that accounts for alpha slippage (Dale et al., 2007). This equates to a critical value of $.05^{.8}$, or $p < .00000000039$, to conclude that two trajectories are different from each other. To measure attraction between two horizontally aligned stimuli (e.g., the answers in our screening questionnaire), you would test whether there is a significant difference in the average x-coordinate for eight consecutive segments. For vertically aligned stimuli, you would test whether there is a significant difference in the average y-coordinate to measure attraction.

5.2 Baseline-Robustness Test

Prior to analyzing our hypotheses, we ran a robustness check to ensure that the baseline questions did not induce any abnormal responses. Again, an assumption of the CIT is that participants would respond similarly to the baseline questions and abnormally only to the key question if they are concealing information. Therefore, baseline questions should not, by themselves, elicit any abnormal behaviors. To test whether people responded similarly to all of the baseline questions, we examined whether each baseline question had (a) significant attraction compared with the opposite answer as compared with the rest of the baseline questions, and (b) slower speed compared with the rest of the baseline questions using linear mixed-effects modeling.

To test for attraction, we used graded-motor response analysis to predict the average x-position in each of the 101 segments. We included $n-1$ (n = the number of baseline questions) binary dummy variables as fixed effects in the model to examine whether any of the baseline questions caused a significant difference for eight consecutive time slots (if all dummy variables were false, this singled out the last baseline question). We also included a random effect for each participant to control for the repeated nature of the data. None of the baseline questions had a significant effect for eight consecutive time slots. We then used the same model to test whether any of the baseline questions had a significant effect on speed (replacing the x-position dependent variable with the speed variable). Again, none

of the baseline questions significantly influenced speed. Thus, the results were consistent with our pilot testing, and the baseline questions were found to be appropriate.

5.3 Hypothesis 1 Results: Concealed-Information Key vs. Baseline Attraction

Using the graded-motor response analysis, we analyzed the average x-coordinate in each of the 101 segments to examine whether participants in the concealed-information condition ($n = 30$) showed more attraction toward the opposite answer for key questions vs. baseline questions. We tested for a difference in the x-position for each segment, as the answers were horizontally aligned (the answers “yes” and “no” were in the upper two corners of the page). As each participant responded to one target item, plus

several baseline items (a within-subject comparison), we specified a linear mixed-effects model predicting the x-position for each segment (the dependent variable) based on whether the participant was viewing the key or baseline items (binary fixed effect) nested within each participant (random effect). This allowed us to examine whether there were differences in the x-position within each participant’s responses to key and baseline items. The analysis revealed 28 sequential segments that were significantly different ($p < .05$)—segments 43-70 and again for 11 sequential segments from 91-101. Thus, H1 is supported. As a reference regarding our control for alpha slippage, the probability of having 28 significant segments in a row is $.05^{28}$. Figure 4 graphs the average x position for each segment. The detailed statistics for the graded-motor response analysis are shown in Appendix A, Table A1.

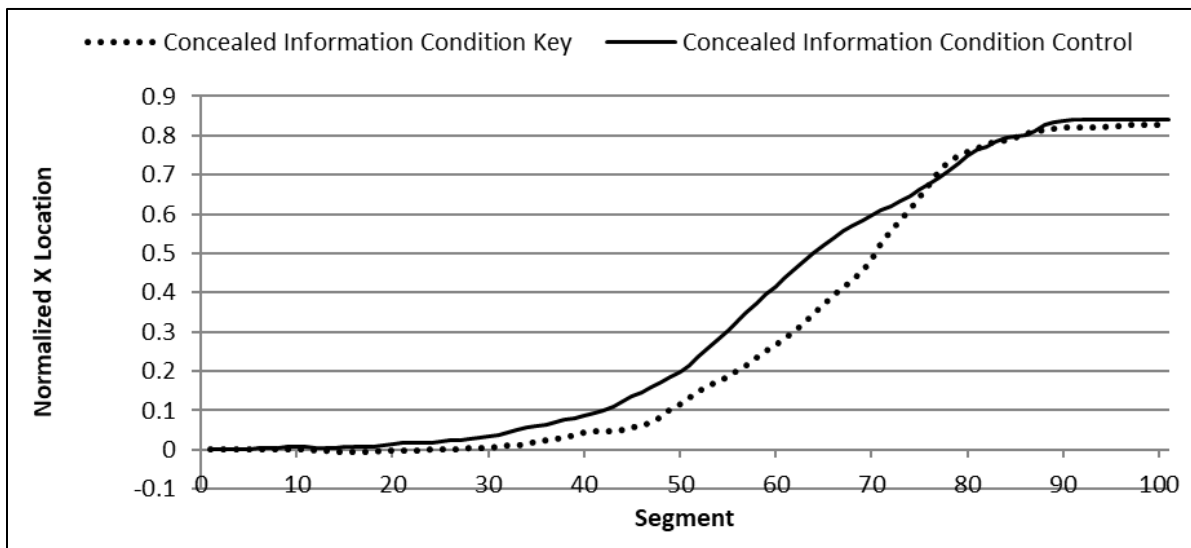


Figure 4. X-Locations by Normalized Time for Participants Concealing Information

5.4 Hypothesis 2 Results: Concealed-Information Key vs. Truthful Key Attraction

Using the graded-motor response analysis, we then analyzed the average x-coordinate for each of the 101 segments to examine whether participants in the concealed-information condition ($n = 30$) showed more attraction toward the opposite answer on key questions (based on x-values), compared with participants in the truthful condition ($n = 36$). Because

each participant only saw one key item regardless of treatment, we used a one-tailed t-test to examine whether segments for the concealment and truthful groups differed. We found that the trajectories of truthful participants and participants who concealed information were significantly different ($p < .05$) for segments 1-9 (nine sequential segments), 25-39 (15 sequential segments), and 72-101 (30 sequential segments)². Thus, H2 is supported. Figure 5 graphs the average normalized x position for each segment. The detailed statistics for the graded-motor response analysis are shown in Appendix A, Table A2.

² The mean differences for segments 1-9 are small and difficult to see visually in **Error! Reference source not found.5**. They are significant, however, because the standard

deviations are also very small. See Appendix A, Table A2 for more details.

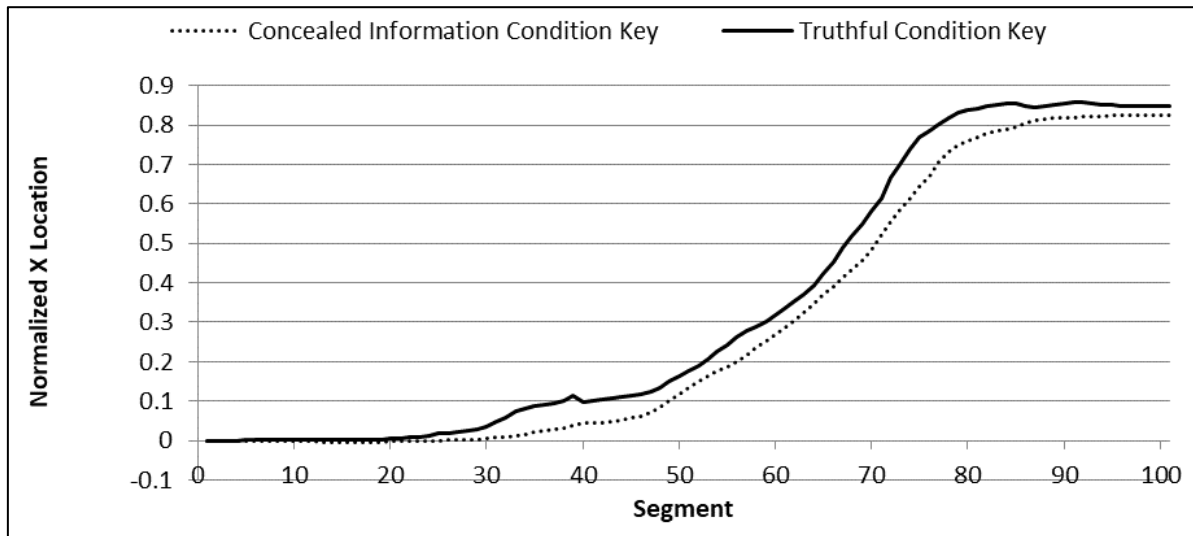


Figure 5. X-Locations by Normalized Time for Key Items

5.5 Hypothesis 3 Results: Concealed-Information Key vs. Baseline Speed

To test Hypothesis 3, we analyzed whether people in the concealed-information condition responded more slowly to key questions compared with baseline questions. As each participant responded to one target item, plus several baseline items, we specified a linear mixed-effects model predicting average speed based on treatment group (0 = baseline; 1 = concealment

group) nested within each participant. This allowed us to examine differences in speed when viewing key vs. baseline items within each participant’s responses. Thus, the analysis supports H3. Participants in the concealed-information condition registered significantly lower speed on key questions ($\beta = -0.028$, $t\text{-value} = -4.033$; $p < .001$; $R^2 = 0.169$). Speed on key questions was nearly twice as slow as speed on baseline questions. See Table 3 for summary statistics on speed for each treatment.

Table 3. Summary statistics for treatment groups for speed (normalized pixel/millisecond)

	Mean	Median	SD	Min	Max
Concealed-information key	0.0345	0.0250	0.0296	0.0011	0.0828
Concealed-information baseline	0.0616	0.0707	0.0459	0.0003	0.1935
Truthful key	0.0627	0.0752	0.0371	0.0001	0.1285
Truthful baseline	0.0622	0.0778	0.0362	0.0005	0.1322

5.6 Hypothesis 4 Results: Concealed-Information Key vs. Truthful Condition Key Speed

To test Hypothesis 4, we analyzed whether people in the concealed-information condition responded more slowly to the key question when compared with people in the truthful condition. As each participant responded to only one key question, we analyzed the data using a one-tailed t-test rather than a linear mixed-effects model. The analysis supported H4. Participants in the concealed-information condition had a slower average speed than did participants in the truthful condition: $t(64) = -2.75$; $p < .01$; $d = 0.138$. The speed

of participants who concealed information on key questions was nearly twice as slow as truthful people’s speed on key questions.

5.7 Exploratory Comparison to Electrodermal Activity Part A: Concealed-Information Key vs. Baseline Question

To help answer Research Question 2—*Do mouse-cursor movements correspond to changes in electrodermal activity in an online CIT-based questionnaire?*—we also explored whether participants in the concealed-information condition

exhibited a difference in electrodermal activity between the presentation of key and baseline items (similar to H1 and H3). The polygraph is based on the assumption that a person concealing information will experience a heightened electrodermal response (caused by arousal and stress) when answering key questions deceptively, compared with answering baseline questions truthfully (Krapohl et al., 2009). Our results confirmed that this effect was present in our experiment. We specified a linear mixed-effects model predicting electrodermal responses using the treatment group (0 = baseline; 041 = concealment group) nested within each participant. We found that the peak electrodermal response was a significant predictor of key items for people concealing information ($\beta = 195.71y$; $t\text{-value} = 2.056$; $p < .05$, $R^2 = 0.434$). In other words, after controlling for individual differences, people concealing information were significantly more likely to experience a higher electrodermal response on key items than on baseline items. This also helps verify the validity and realism of our experiment, as this physiological result matches the pattern of electrodermal responses observed in real-life deception scenarios (Krapohl et al., 2009).

5.8 Exploratory Comparison to Electrodermal Activity Part B: Concealed-Information Key vs. Truthful Key

Similarly, we conducted a t-test to examine whether there was a difference in electrodermal activity between how participants in the concealed-information condition answered key questions, compared with participants in the truthful condition (similar to H2 and H4). There was no significant difference between the two treatment groups on concealment-group key questions: $t(64) = -1.093$; $p > .05$; $d = 0.274$: mean truthful group key questions = 4946 (sd = 2723); mean key items = 5385 (sd = 2501).

5.9 Exploratory Comparison to Electrodermal Activity Part C: Prediction Capability

As a final analysis to explore Research Question 2, we compared mouse-cursor tracking to electrodermal activity in a simple proof-of-concept prediction model. This allowed us to explore whether mouse-cursor tracking has the potential to be used for classifying who is concealing information, as well as how it indirectly compares with electrodermal activity. While the intent of this analysis was not to create an optimal

model, nor to determine which indicator (mouse-cursor movements vs. electrodermal activity) is better, it shows that mouse-cursor movements can be used in a simple model to predict deception.

To do this, we implemented a theory-driven decision-tree (i.e., rule-based) model for electrodermal activity and mouse-cursor movements separately. We did not use machine learning to train the model. Rather, the model used a theory based on our hypotheses and past methodologies to generate the decision-tree rules, thereby increasing its generalizability and reducing the likelihood of overfitting. The decision-tree models for electrodermal activity and mouse movements are shown in Figure 6 and are summarized below.

The decision-tree model for electrodermal activity is based on how the polygraph CIT examination is scored (Krapohl et al., 2009), albeit simplified. Thus, the results should not be interpreted as the ultimate potential for electrodermal activity, nor as a direct comparison with the mouse-movement model.³ The model only focuses on comparing responses to key items with responses to baseline items within subjects, as these differences were significant in our experiment and have been shown to be predictive in real-life CIT polygraph scenarios (Krapohl et al., 2009). We classified someone as concealing information if his or her response to the key item showed higher electrodermal activity relative to the participant's responses to all baseline questions. Otherwise, the person was classified as truthful.

The mouse-movement model was based on our hypotheses that deceivers would show a significant attraction toward the opposite response on key questions compared with baseline questions, and that they would also exhibit slower speeds. Note that we only used the comparison between baseline and key questions (Hypotheses 1 and 3) because this was commonly significant between electrodermal activity and mouse-cursor movement analyses. Thus, we classified someone as deceptive if (a) the movement trajectory on the key item showed significantly more attraction toward the opposite answer than did the person's trajectories to the baseline questions, and (b) if the response to the key item was slower than the person's responses to all baseline questions.

We ran each participant's data individually through the decision-tree rules and produced a prediction of truthful or deceptive. We then compared the prediction with ground truth (the treatment group) to generate aggregate statistics. The true- and false-positive rates are shown in Table 4.

³ For example, the polygraph has been shown to have accuracy ranging from 70-90% in research (APA, 2014).

Table 4. True and False Positives for Mouse-Movement Model

Mouse-movement model		
	True-positive rate	False-positive rate
Concealed information	.733	.167
Truthful	.833	.267
Average	.783	.217
Electrodermal activity model		
	True-positive rate	False-positive rate
Concealed information	.733	.389
Truthful	.611	.267
Average	.672	.328

The results suggest that mouse-cursor movements can help differentiate between people concealing information and truthful people. The average accuracy of the mouse-movement model was 78.3%, and the average accuracy of the electrodermal activity model was 62.7%.

After tabulating the prediction models, we ran a statistical test of proportions to examine whether these two accuracy rates were significantly different from each other. This test is informational only and should not be used to conclude that mouse-cursor movements are a better indicator of deception than electrodermal activity (because the models are neither necessarily comparable nor optimized). The test of proportions showed a marginally significant difference between the two overall accuracy rates for the given model specification: $\chi^2(1) = 2.035$; $p < .10$. The biggest difference between the two models was the false-positive rate for detecting truthful people. The difference between the mouse-movement model and the electrodermal activity model was 22.2%, which is significantly different: $\chi^2(1) = 8.041$; $p < .01$.

6 Discussion

This research introduces a novel, mass-deployable approach for identifying concealed information using an online CIT-based screening questionnaire and the tracking/analysis of mouse-cursor movements. In developing this solution, we proposed two research questions to understand the efficacy of using mouse-cursor movements to identify concealed information.

Our first research question asked: *How do mouse-cursor movements differ for people concealing information and people telling the truth in an online CIT-based questionnaire?* We developed hypotheses to explain how (1) attraction toward the opposite response and (2) speed differs for people concealing information relative to truthful people across key and baseline questions. Table 5 summarizes the results; all hypotheses were supported.

As electrodermal activity is the standard response used in CIT-based polygraph tests, our second research question asked: *Do mouse-cursor movements correspond with changes in electrodermal activity during an online CIT-based questionnaire?* To address this question, we simultaneously captured mouse-cursor movements and electrodermal activity from our experiment participants. We then conducted three exploratory analyses. We found that both mouse-cursor tracking and electrodermal activity differentiated between how people concealing information answered baseline and key questions. In our second analysis, the trajectory analysis differentiated between how people concealing information and truthful people answered key questions, but electrodermal activity did not. Finally, in our third analysis, we found that mouse-cursor tracking and electrodermal activity identified concealed information with similar accuracy; however, mouse-cursor movements had fewer false positives. Below, we discuss the implications for research and practice.

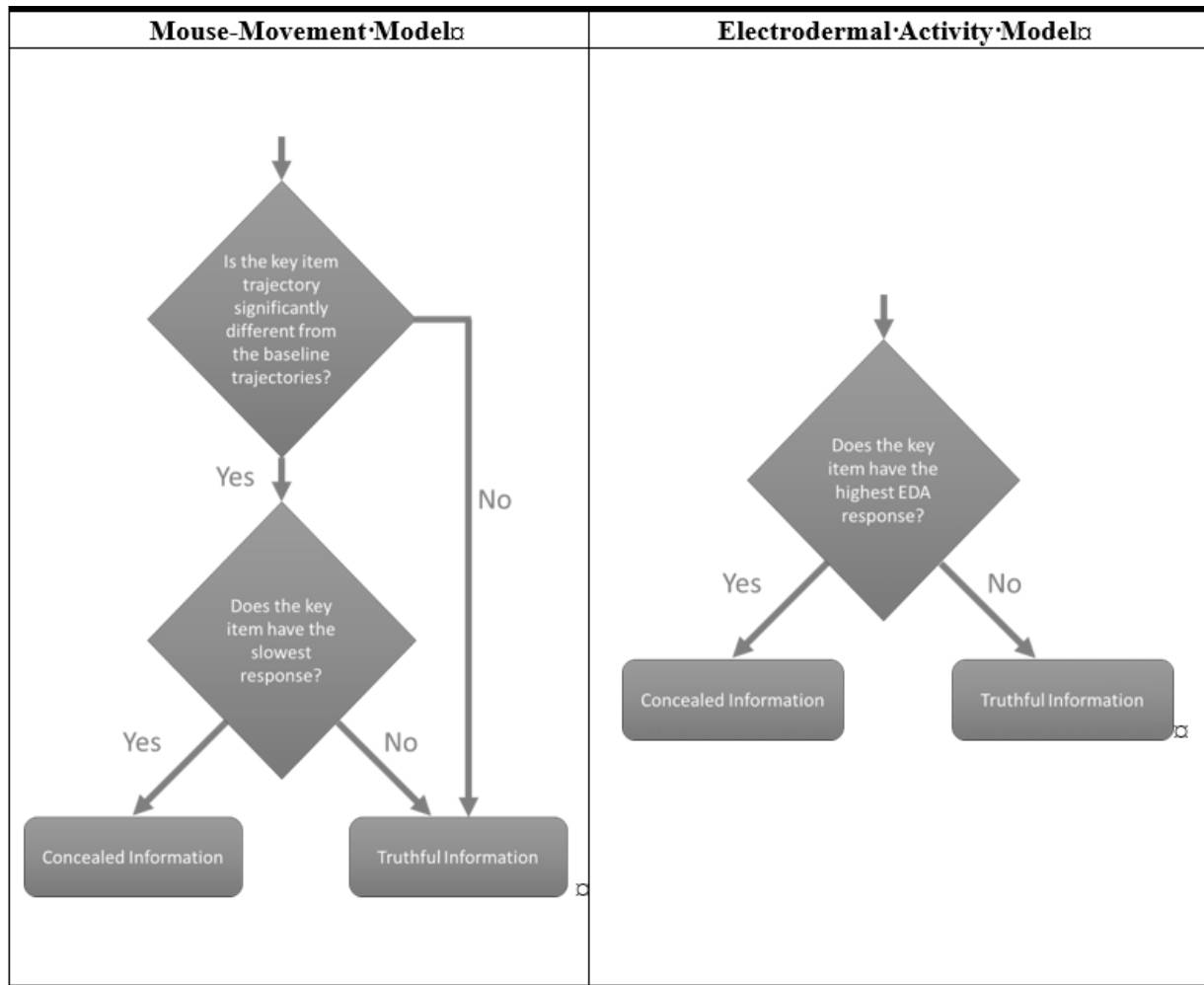


Figure 6. Simple Theory-Driven Decision-Tree Models for Prediction

Table 5. Summary of Hypotheses

Hypothesis	Result
H1: Mouse trajectories of people concealing information will show greater attraction toward the opposite response on key questions than on baseline questions.	Supported
H2: Mouse trajectories of people concealing information will show greater attraction toward the opposite response on key questions than the mouse trajectories of truthful people.	Supported
H3: People concealing information will move the mouse more slowly while responding to key questions, compared with responses to baseline questions.	Supported
H4: People concealing information will move the mouse more slowly when answering key questions, compared with truthful people.	Supported

6.1 Implications for Research

Our research provides a rigorous, theory-driven approach for identifying concealed information by monitoring mouse-cursor movements. Past research started to recognize the potential for identifying

deception by monitoring mouse-cursor movements (e.g., Duran et al., 2010; McKinstry et al., 2008; Monaro et al., 2017). A current gap in this literature, however, is the need to construct a standardized questioning technique and explain how mouse-cursor movements differentiate between concealed

information and truth through theory-driven hypotheses. To address this need, we first draw on the concealed information test (CIT)—the most scientifically-validated polygraph-based questioning technique (Ben-Shakhar et al., 2003; Council, 2003; Fiedler et al., 2002)—as a basis for a mouse-cursor movement-screening questionnaire. We made several adaptations to the CIT to make our approach amenable to rapid scalability, including the presentation format and mode of answers (i.e., online format, answers in upper corners, movement starting position in bottom middle, requirement to start moving the mouse soon after the question appears). These adaptations extend the CIT to a mass-screening scenario that can be conducted online, enabling mouse-cursor tracking to be used as a granular sensor of concealed information. Importantly, our research empirically demonstrates that this format has efficacy for predicting concealed information in a computerized setting using mouse-cursor movements.

Second, we provide theory-driven hypotheses of why mouse-cursor movements differentiate between people concealing information and truthful people on this specialized screening questionnaire. Past research has suggested that mouse-cursor movements may provide important information about people's cognitive and emotional processes (e.g., Dale et al., 2011; Freeman, Dale, & Farmer, 2011; Grimes et al., 2013; Hibbeln et al., 2017). However, little research has explained theoretically why mouse-cursor movements differ between people concealing information and truthful people. To address this need, we drew on the response activation model (Welsh et al., 2004) to explain how concealing information causes people to show attraction toward the opposition response. We also drew on theory relating to cognitive load and response times to explain how concealing information causes people to move the mouse more slowly. Our hypotheses were supported. These findings provide theoretical insight into past empirical observations (e.g., Duran et al., 2010; McKinstry et al., 2008; Monaro et al., 2017) that mouse-cursor movements provide valuable input concerning the veracity of information.

Third, we are among the first to measure mouse-cursor movements and electrodermal activity simultaneously while participants complete a computerized task. This responds to calls for the use of multimethod research to cross-validate results (Venkatesh, Brown, & Sullivan, 2016). Past research has largely found that meaningful electrodermal-activity indicators of deception occur when doing within-subject comparison—i.e., comparing a person's key questions to how that same person responded to baseline questions (Krapohl et al., 2009). Confirming this finding, we found that electrodermal activity differentiated between how people answered baseline vs. key questions when concealing information in our

experiment. Interestingly, these differences also corresponded to changes in the attraction and speed of people's mouse-cursor movements (H1 and H2). This is an important finding to support the validity of the research—that mouse-cursor movement attraction and speed correspond to validated psychophysiological measures of concealed information from past literature.

Interestingly, although past literature has found that electrodermal activity is higher in a within-subject comparison (when comparing baseline to key items when people are concealing information), it has typically not found support that electrodermal activity can significantly differentiate between subjects when comparing key items between truthful people and people concealing information (Fiedler et al., 2002; Krapohl et al., 2009). Our results support this conclusion; there was no difference between truthful people and people concealing information in terms of electrodermal activity. However, we also found a between-subject difference when comparing mouse-cursor movements between truthful and deceitful people on key items. Namely, when respondents concealed information, they showed greater attraction and slower speed on key questions than those who were being truthful (H3 and H4). This suggests that mouse-cursor movements may provide information about cognitive processes that is not easily accessible through traditional deception-measuring methods (e.g., electrodermal activity). One reason mouse-movement attraction and speed may be significant between participants (whereas electrodermal was not) is because levels of electrodermal activity vary immensely between people. Electrodermal activity may differ according to health conditions, fitness, temperature, and even the time of day (Poh, Swenson, & Picard, 2010; Turpin, Shine, & Lader, 1983). However, it may be that mouse-cursor movements are influenced by fewer external factors and are thus more robust to individual differences. This would explain why mouse-cursor speed and attraction are significant between subject indicators of concealed information whereas electrodermal activity was not. Future research should test these propositions and explore additional differences between electrodermal activity and mouse-cursor movements.

Finally, no single methodology for detecting deception is perfect. Rather, the best prediction of deception comes from multiple complementary sources. For example, prior information systems research has investigated the use of an automated interviewing platform to conduct credibility assessments (Derrick, Elkins, Nunamaker, Zeng, & Burgoon, 2010; Derrick et al., 2011). This system collects data on a variety of potential indicators, including eye movements and kinesic activity (Proudfoot, Jenkins et al., 2016; Twyman, Elkins, et al., 2014). In theory, as the number of reliable indicators that are analyzed by the system

increases, accuracy should also increase, false positives should be reduced, and the system should be more resistant to countermeasures (Proudfoot, Boyle, & Schuetzler, 2016; Twyman et al., 2015). Considering this related work, the results and contributions of the present study to existing research should be interpreted as a new layer in the defense-in-depth strategy for detecting deception. The ideal system for identifying concealed information should triangulate several sources of both passive and active indicators, including log analysis, mouse-trajectory analysis, mouse-speed analysis, communication analysis, personality assessments, and other behavioral information.

6.2 Implications for Practice

Researchers have long been interested in developing means to identify concealed information. For example, numerous studies have been conducted to develop integrity scales (and other criterion-focused occupational personality scales) that can predict problematic behaviors in the workplace (e.g., theft, disciplinary problems, absenteeism) (Jones, 1981; Ones & Viswesvaran, 2001; Ones, Viswesvaran, & Schmidt, 1993; Terris & Jones, 1982) and help organizations avoid hiring individuals who may pose a threat. While a meta-analysis of these tools found them to be effective (Ones et al., 1993), technology is permitting novel means of identifying past and future nefarious actions by organizational insiders concealing information. Our research has powerful implications for practice as it introduces a new way of detecting concealed information in organizations. People who conceal information about adverse behaviors in organizations present a significant danger to both the private and public sectors, and the detection of concealed information is traditionally a difficult, expensive, error-prone, and time-consuming task. We provide a solution that can supplement extant monitoring systems to improve deception detection. For example, this approach can be mass-deployed online to screen individuals for various types of concealed information (e.g., noncompliance with organizational policies), and thereby trigger follow-up evaluations. Alternatively, it can be used to screen individuals already flagged as potentially being non-compliant by existing systems (e.g., file-logging systems) to decrease the number of false positives. In response to an alert, our solution can be deployed easily through a variety of mechanisms (e.g., links in email, system interjections, embedding in applications or websites, etc.) and does not require any special hardware or software on the person's computer. Importantly, data analysis and the generation of results can be automated and computed in under a second.

One area in particular that our research can enhance is that of manual screening processes, such as background checks and polygraph examinations.

Traditional manual screening for threats is time-consuming and expensive. For example, polygraph examinations take multiple hours to administer, on average, and are often viewed as being subjective due to the variability present in the examiner's method of conducting the interview and interpreting the results. These screenings are also expensive and cannot be easily deployed en masse. As a result, government agencies that rely on polygraph examinations have overwhelming backlogs of people who need screening and never receive it (GAO, 2004; Serbu, 2016). Our proposed solution, on the other hand, can easily be deployed to thousands of individuals simultaneously within an organization using an online questionnaire. The approach is unbiased and based on theoretically driven cues of deception. People can complete the questionnaire in their natural environments (e.g., on their own computer). The marginal cost of deploying it to an additional person is minuscule. Thus, our approach can also be used for prescreening to reduce the subset of people who must receive manual screenings (e.g., the polygraph). In this way, our research can help organizations deploy limited manual resources more effectively.

6.3 Limitations and Future Research

Although our experiment was designed to mimic a realistic concealed-information scenario (see Section 4.8: "Evidence of Realism"), the experiment was sanctioned. Several differences exist between our experiment and real-world deception. First, participants were instructed to commit the theft and to lie if asked about committing the theft. Past research has shown that people are more willing to commit questionable activities if they are asked to do them by an authority figure (e.g., an experiment facilitator) (Milgram, 1963). Second, the stakes of being caught in the deception were low. If people got caught deceiving, there were no consequences. Thus, people's reactions (including mouse movements) may be different from what would happen in a real-world deception scenario. For example, in the real world, people may experience greater decision conflict and cognitive load when deceiving than they would in this experiment. As a result, we would expect that inhibition of competing motor responses would be slower because real-life experiences are more salient than simulated experiences. This would result in even greater attraction to the opposite response. Likewise, the increased cognitive load may cause people to move more slowly. Thus, real-world deception may cause more profound differences between people concealing information and people telling the truth. This supports prior deception research showing that laboratory deception experiments are indeed generalizable to real-world deception (Kircher et al., 1988; Pollina et al., 2004). Nevertheless, future research should

cross-validate the results of our study in a higher-stakes, more-realistic scenario.

Another potential difference between our experiment and real-world deception is the prevalence of countermeasures. A countermeasure refers to measures taken by a person to avoid being classified as deceptive. Prior information-systems research investigating other types of systems designed to identify deception have (1) also acknowledged the potential risk of countermeasures, and (2) evaluated the robustness of these systems to detect countermeasures (Twyman et al., 2016; Proudfoot et al., 2016). Because of the low stakes in our experiment, and because people did not know how we were detecting deception, participants likely did not engage in extensive countermeasure use. For example, H1 and H3 are contingent on the respondent moving the mouse very soon after seeing the question-and-answer options. If the respondent waits until the inhibition process is complete before answering, the movement trajectories will not be biased by the competing motor programming (Welsh et al., 2004). This could potentially be used as a countermeasure to avoid detection.

Future research should seek to develop strategies for mitigating countermeasure attempts. For example, a tool designed to implement our mouse-movement methodology for detecting concealed information must encourage participants to move the mouse quickly, ideally within the first second. In our experiment, participants were required to move the mouse within the first second, otherwise an error message was displayed. An alternative design for encouraging people to move the mouse during the decision-making process is to have people answer a question by dragging a ball from the lower middle of the screen to one of the answers in the upper-left or upper-right sections of the screen. The system withholds the question until the person starts dragging the ball upward, then registers an error if the person stops dragging the ball or releases the ball. In this way, the movement captures the dynamic nature of a person processing the question for the first time. Future research could test such a system.

Furthermore, this study focused largely on only one age demographic, as the average age of participants was just under 22 years. Participants were students, and, based on a self-reported questionnaire, were deemed to be computer savvy. In several of our pilot studies, we used Amazon's Mechanical Turk to recruit participants. The average age of these participants was roughly 35 years old, and the results were similar to those reported in this study. Furthermore, the cultural demographic was much richer in these pilot studies since most participants were not from the U.S. While this pilot process points to an increased generalizability of our findings, future work should evaluate our proposed methodology for identifying

concealed information in a more diverse population. Furthermore, future research should examine whether individual differences affect the diagnostic capability of using mouse-movement analysis for deception detection. For example, women tend to experience guilt more than men (Bybee, 1997), and narcissism, agreeableness, and self-esteem have been found to correlate negatively with guilt (Strelan, 2007). Future research could examine the extent to which these individual factors influence mouse-cursor movements when being deceptive.

In addition, we allowed 12 seconds to transpire between the onset and offset of each question in the CIT, thereby accommodating each individual's electrodermal activity to react to a question, then normalize, before the onset of the next question (Gamer et al., 2006). Theoretically, valid mouse-movement responses do not require this amount of time. Thus, future research should examine whether the mouse-movement results would change after removing this exaggerated latency between questions.

Future research could also present alternative questionnaire designs to see whether this improves the accuracy of mouse-cursor movements in identifying concealed information. For example, one could present a CIT in which every question is treated as a target question for screening purposes (e.g., replacing baseline questions with questions that ask about key organizational data assets). Each question could be set iteratively as the target and compared versus the rest to identify anomalies in a screening scenario.

Additionally, it is important to note that devising and conducting a CIT-based screening process inherently requires a certain amount of time (even in the most automated and rapid interactions). As security incidents are often extremely time-sensitive (i.e., it is critical to identify the person(s) who may be tampering with, destroying, or stealing important organizational data as quickly as possible), the approach presented in this paper may not be ideal for all circumstances, especially if the organization is unaware that an incident has occurred or is currently taking place and a new CIT interaction must first be developed (e.g., appropriate stimuli selection) before it can be deployed.

Finally, a practical limitation, and an opportunity for future research, is the constantly evolving landscape of human-computer interaction. The use of a computer mouse to interact with a computer clearly has been a ubiquitous standard for decades. However, with the introduction of handheld devices (e.g., smartphones and tablets), which permit people to accomplish many similar and overlapping tasks without the use of a mouse (or keyboard), it is worth acknowledging that the utility of this exact approach may be reduced over time as other interaction mediums, such as touchscreens, proliferate further. However, the

technique presented in this paper can be adapted for use on other types of devices. For example, on a touchscreen, a highly similar CIT-based task could be utilized in which people drag an object across a screen using their fingers. The theoretical underpinnings discussed in this paper still would apply to this type of interaction, and the indicators that could be measured using this approach would be highly similar to the present research. In short, the way in which people interact with a system may change over time, but it is probable that a mouse-based approach could be modified to be both applicable, and effective, in any number of contexts and interaction formats. Future research should seek to evaluate the potential applicability of this study as new interaction formats are introduced and become widespread.

7 Conclusion

Identifying people who are concealing information is critical for protecting individuals, organizations, and

society. We propose that measuring people's mouse-cursor movements in an online CIT-based questionnaire can help improve the detection of information concealment. We empirically tested our theory-derived hypotheses in a mock-theft experiment, in which mouse-cursor movements and electrodermal activity were measured simultaneously. We found that mouse-cursor movements can significantly differentiate between people who are concealing information and truthful people using an online CIT-based questionnaire. We also found that mouse-cursor movements can differentiate between people who conceal information and truthful people using a broader set of comparisons relative to electrodermal activity. Mouse-cursor movements also yielded significantly fewer false positives than electrodermal activity. Our results demonstrate that the use of mouse-cursor monitoring holds promise for identifying information concealment and can be used to supplement existing systems to improve deception detection.

References

- Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security*, 2015(7), 9-17.
- Anderson, B. B., Kirwan, C. B., Jenkins, J. L., Eargle, D., Howard, S., & Vance, A. (2015). How polymorphic warnings reduce habituation in the brain: Insights From an fMRI study. *Proceedings of the ACM Conference on Human Factors in Computing Systems* (pp. 2883-2892). ACM.
- APA (2014). The truth about lie detectors (aka polygraph tests). Retrieved from <https://www.apa.org/research/action/polygraph.aspx>
- Ben-Shakhar, G. & Eyal, E. (2003). The validity of psychophysiological detection of information with the guilty knowledge test: A meta-analytic review. *Journal of Applied Psychology*, 88(1), 131-151.
- Buller, D. B. & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, 6(3), 203-242.
- Burgoon, J. K., Blair, J. P., & Strom, R. E. (2008). Cognitive biases and nonverbal cue availability in detecting deception. *Human Communication Research*, 34(4), 572-599.
- Bybee, J. (1997). The emergence of gender differences in guilt during adolescence. In J. Bybee (Ed.), *Guilt and Children* (pp. 113). San Diego, CA: Academic.
- Carrión, R. E., Keenan, J. P., & Sebanz, N. (2010). A truth that's told with bad intent: An ERP study of deception. *Cognition*, 114(1), 105-110.
- Cisek, P. & Kalaska, J. F. (2005). Neural correlates of reaching decisions in dorsal premotor cortex: specification of multiple direction choices and final selection of action. *Neuron*, 45(5), 801-814.
- Council, N. R. (2003). *The polygraph and lie detection*. Washington, DC: National Academies.
- Dale, R. & Duran, N. D. (2011). The cognitive dynamics of negated sentence verification. *Cognitive Science*, 35(5), 983-996.
- Dale, R., Kehoe, C., & Spivey, M. J. (2007). Graded motor responses in the time course of categorizing atypical exemplars. *Memory & Cognition*, 35(1), 15-28.
- Dale, R., Roche, J., Snyder, K., & McCall, R. (2008). Exploring action dynamics as an index of paired-associate learning. *PLoS One*, 3(3), e1728.
- Derrick, D. C., Elkins, A. C., Nunamaker, J. F., Jr. Zeng, D. D., & Burgoon, J. K. (2010). Border security credibility assessments via heterogeneous sensor fusion. *IEEE Intelligent Systems*, 25(3), 41-49.
- Derrick, D. C., Jenkins, J. L., & Nunamaker, J. F., Jr. (2011). Design principles for special purpose, embodied, conversational intelligence with environmental sensors (SPECIES) agents. *AIS Transactions on Human-Computer Interaction*, 3(2), 62-81.
- Duran, N. D., Dale, R., & McNamara, D. S. (2010). The action dynamics of overcoming the truth. *Psychonomic Bulletin & Review*, 17(4), 486-491.
- Elkins, A. C., Dunbar, N. E., Adame, B., & Nunamaker, J. F., Jr. (2013). Are users threatened by credibility assessment systems? *Journal of Management Information Systems*, 29(4), 249-262.
- Farmer, T. A., Cargill, S. A., Hindy, N. C., Dale, R., & Spivey, M. J. (2007). Tracking the continuity of language comprehension: Computer mouse trajectories suggest parallel syntactic processing. *Cognitive Science*, 31(5), 889-909.
- Fiedler, K., Schmid, J., & Stahl, T. (2002). What is the current truth about polygraph lie detection?. *Basic and Applied Social Psychology*, 24(4), 313-324.
- Figliuzzi, C. F. (2012). Statement before the house committee on homeland security, subcommittee on counterterrorism and intelligence. Retrieved from <https://www.dhs.gov/news/2011/09/13/statement-record-ussc-house-homeland-security-subcommittee-counterterrorism-and>
- Fowles, D. C. (2007). The three arousal model: Implications of gray's two-factor learning theory for heart rate, electrodermal activity, and psychopathy. *Psychophysiology*, 17(2), 87-104.
- Freeman, J., Dale, R., & Farmer, T. (2011). Hand in motion reveals mind in motion. *Frontiers in Psychology*, 2, Article 59.
- Freeman, J. B. & Ambady, N. (2009). Motions of the hand expose the partial and parallel activation of stereotypes. *Psychological Science*, 20(10), 1183-1188.
- Freeman, J. B. & Ambady, N. (2010). MouseTracker: software for studying real-time mental processing using a computer mouse-tracking method. *Behavior Research Methods*, 42(1), 226-241.

- Freeman, J. B. & Ambady, N. (2011). When two become one: Temporally dynamic integration of the face and voice. *Journal of Experimental Social Psychology, 47*(1), 259-263.
- Freeman, J. B., Ambady, N., Midgley, K. J., & Holcomb, P. J. (2011). The real-time link between person perception and action: Brain potential evidence for dynamic continuity. *Social Neuroscience, 6*(2), 139-155.
- Freeman, J. B., Ambady, N., Rule, N. O., & Johnson, K. L. (2008). Will a category cue attract you? Motor output reveals dynamic competition across person construal. *Journal of Experimental Psychology: General, 137*(4), 673-690.
- Gamer, M., Rill, H.-G., Vossel, G., & Gödert, H. W. (2006). Psychophysiological and vocal measures in the detection of guilty knowledge. *International Journal of Psychophysiology, 60*(1), 76-87.
- GAO (2004). GAO-04-344: DOD personnel clearances: DOD needs to overcome impediments to eliminating backlog and determining its size. Retrieved from <https://www.gao.gov/products/gao-04-344>
- Georgopoulos, A. P. (1990). Neurophysiology of reaching. In M. Jeannerod (Ed.), *Attention and Performance XIII*. Hillsdale, NJ: Erlbaum.
- Gordover, M. (2016). 5 things you should know about insider threats. Retrieved from <https://www.observeit.com/blog/5-things-you-should-know-about-insider-threats/>
- Grimes, M., Jenkins, J. L., & Valacich, J.S. (2013). Exploring the effect of arousal and valence on mouse interaction. In *Proceedings of the International Conference on Information Systems*.
- Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., & Weinmann, M. (2017). How is your user feeling? Inferring emotion through human-computer interaction devices. *MIS Quarterly, 41*(1), 1-21.
- Hsieh, C.-H., Lai, C.-M., Mao, C.-H., Kao, T.-C., & Lee, K.-C. (2015). AD2: Anomaly detection on active directory log data for insider threat monitoring. In *Proceedings of the Carnahan Conference on Security Technology (ICCST)* (287-292).
- Jensen, M. L., Lowry, P. B., Burgoon, J. K., & Nunamaker, J. F., Jr. (2010). Technology dominance in complex decision making: The case of aided credibility assessment. *Journal of Management Information Systems, 27*(1), 175-202.
- Jones, J. W. (1981). Attitudinal correlates of employee theft of drugs and hospital supplies among nursing personnel. *Nursing Research, 30*(6), 349-350.
- Kandias, M., Stavrou, V., Bozovic, N., & Gritzalis, D. (2013). Proactive insider threat detection through social media: The YouTube case. *Proceedings of the Workshop on Privacy in the Electronic Society* (261-266).
- King, J. S. (2002). An introduction to the orienting response (OR) and its habituation. Retrieved from www.radford.edu/~jksking/Orienting%20Response.doc.
- Kircher, J. C. & Raskin, D. C. (1988). Human versus computerized evaluations of polygraph data in a laboratory setting. *Journal of Applied Psychology, 73*(2), 291-302.
- Krapohl, D. J., McCloughan, J. B., & Senter, S. M. (2009). How to use the concealed information test. *Polygraph, 38*(1), 34-49.
- Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Automated insider threat detection system using user and role-based profile assessment. *IEEE Systems Journal, 11*(2), 1-10.
- Liu, A., Martin, C., Hetherington, T., & Matzner, S. (2005). A comparison of system call feature representations for insider threat detection. In *Proceedings of the SMC Information Assurance Workshop*.
- Lykken, D. T. (1959). The GSR in the detection of guilt. *Journal of Applied Psychology, 43*(6), 385-388.
- Martini, F., & Bartholomew, E. (2003). *Essentials of Anatomy & Physiology*. San Francisco, CA: Cummings.
- McKinstry, C., Dale, R., & Spivey, M. J. (2008). Action dynamics reveal parallel competition in decision making. *Psychological Science, 19*(1), 22-24.
- Meyer, D. E., Abrams, R. A., Kornblum, S., Wright, C. E., & Smith, K. J. (1988). Optimality in human motor performance: Ideal control of rapid aimed movements. *Psychological Review, 95*(3), 340-370.
- Meyer, D. E., Smith, J. E. K., Kornblum, S., Abrams, R. A., & Wright, C. E. (1990). Speed-accuracy tradeoffs in rapid aimed movements: Toward a theory of rapid voluntary action. In M. Jeannerod (Ed.), *Attention and Performance XIV* (pp. 173-226). Hillsdale, NJ: Erlbaum.

- Milgram, S. (1963). Behavioral study of obedience. *The Journal of Abnormal and Social Psychology*, 67(4), 371-378.
- Mnahan, D. (2015). Data-driven security reloaded: summary of research findings for endpoint threat detection, prevention, and response. Retrieved from https://cdn2.hubspot.net/hubfs/208516/Assets/EMA-Prelert-DataDrivenSecurityReloaded-Summary_Apr2015.pdf
- Monaro, M., Gamberini, L., & Sartori, G. (2017). The detection of faked identity using unexpected questions and mouse dynamics. *PLoS One*, 12(5), e0177851.
- Myers, J., Grimaila, M. R., & Mills, R. F. (2009). Towards insider threat detection using web server logs. In *Proceedings of the Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*.
- Nunamaker, J. F., Jr., Derrick, D. C., Elkins, A. C., Burgoon, J. K., & Patton, M. W. (2011). Embodied conversational agent-based kiosk for automated interviewing. *Journal of Management Information Systems*, 28(1), 17-48.
- Ones, D. S. & Viswesvaran, C. (2001). Integrity tests and other criterion-focused occupational personality scales (COPS) used in personnel selection. *International Journal of Selection and Assessment*, 9(1-2), 31-39.
- Ones, D. S., Viswesvaran, C., & Schmidt, F. L. (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology*, 78(4), 679-703.
- Paninski, L., Fellows, M. R., Hatsopoulos, N. G., & Donoghue, J. P. (2004). Spatiotemporal tuning of motor cortical neurons for hand position and velocity. *Journal of Neurophysiology*, 91(1), 515-532.
- Park, S., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2012). Towards understanding deterrence: information security managers' perspective. *Proceedings of the International Conference on IT Convergence and Security*.
- Poh, M.-Z., Swenson, N. C., & Picard, R. W. (2010). A wearable sensor for unobtrusive, long-term assessment of electrodermal activity. *IEEE Transactions on Biomedical Engineering*, 57(5), 1243-1252.
- Pollina, D. A., Dollins, A. B., Senter, S. M., Krapohl, D. J., & Ryan, A. H. (2004). Comparison of polygraph data obtained from individuals involved in mock crimes and actual criminal investigations. *Journal of Applied Psychology*, 89(6), 1099-1105.
- Proudfoot, J. G., Boyle, R., & 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, 23-33.
- Proudfoot, J. G., Jenkins, J. L., Burgoon, J. K., & Nunamaker, J. F., Jr. (2016). More than meets the eye: How oculometric behaviors evolve over the course of automated deception detection interactions. *Journal of Management Information Systems*, 33(2), 332-360.
- PWC (2016). The global state of information security® survey 2016. Retrieved from <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html>
- Raytheon (2015). The financial industry and the insider threat: Total awareness leads to secured enterprise. Retrieved from https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_244836.pdf
- Sanzgiri, A. & Dasgupta, D. (2016). Classification of insider threat detection techniques. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference*.
- Schulze, H. (2016). Insider threat. Retrieved from <http://www.veriato.com/docs/default-source/whitepapers/insider-threat-report-2016.pdf>
- Serbu, J. (2016). White house names first director of new security clearance bureau. Retrieved from <https://federalnewsradio.com/opm/2016/09/white-house-names-first-director-new-security-clearance-bureau/>
- Sokolov, E. N. (1963). Higher nervous functions - orienting reflex. *Annual Review of Physiology*, 25(1), 545-580.
- Song, J. H. & Nakayama, K. (2006). Role of focal attention on latencies and trajectories of visually guided manual pointing. *Journal of Vision*, 6(9), 982-995.
- Song, J. H. & Nakayama, K. (2008). Target selection in visual search as revealed by movement trajectories. *Vision Research*, 48(7), 853-861.
- Spivey, M. J., Grosjean, M., & Knoblich, G. (2005). Continuous attraction toward phonological competitors. *Proceedings of the National*

- Academy of Sciences of the United States of America*, 102(29), 10393-10398.
- Strelan, P. (2007). Who forgives others, themselves, and situations? The roles of narcissism, guilt, self-esteem, and agreeableness. *Personality and Individual Differences*, 42(2), 259-269.
- Terris, W. & Jones, J. (1982). Psychological factors related to employees' theft in the convenience store industry. *Psychological Reports*, 51(3), 1219-1238.
- Tipper, S. P., Howard, L. A., & Jackson, S. R. (1997). Selective reaching to grasp: Evidence for distractor interference effects. *Visual Cognition*, 4(1), 1-38.
- Turpin, G., Shine, P., & Lader, M. (1983). Ambulatory electrodermal monitoring: Effects of ambient temperature, general activity, electrolyte media, and length of recording. *Psychophysiology*, 20(2), 219-224.
- Twyman, N. W., Elkins, A. C., Burgoon, J. K., & Nunamaker, J. F., Jr. (2014). A rigidity detection system for automated credibility assessment. *Journal of Management Information Systems*, 31(1), 173-202.
- 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.
- Twyman, N. W., Proudfoot, J. G., Schuetzler, R. M., Elkins, A. C., & Derrick, D. C. (2015). Robustness of multiple indicators in automated screening systems for deception detection. *Journal of Management Information Systems*, 32(4), 215-245.
- Unsworth, N., & Engle, R. W. (2005). Individual differences in working memory capacity and learning: Evidence from the serial reaction time task. *Memory & Cognition*, 33(2), 213-220.
- Upton, D. M., & Creese, S. (2014). The danger from within. *Harvard Business Review*, 92(9), 94-101.
- Valacich, J. S., Jenkins, J. L., Nunamaker, J. F., Jr., Hariri, S., & Howie, J. (2013). Identifying insider threats through monitoring mouse movements in concealed information tests. In *Proceedings of the HICSS-46 Symposium on Credibility Assessment and Information Quality in Government and Business*.
- Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, 17(7), 435-494.
- Welsh, T. N. & Elliott, D. (2004). Movement trajectories in the presence of a distracting stimulus: Evidence for a response activation model of selective reaching. *The Quarterly Journal of Experimental Psychology Section A*, 57(6), 1031-1057.
- Williams, L. M., Brammer, M. J., Skerrett, D., Lagopolous, J., Rennie, C., Kozek, K., Olivieri, G., Peduto, T., & Gordon, E. (2000). The neural correlates of orienting: An integration of fMRI and skin conductance orienting. *Neuroreport*, 11(13), 3011-3015.
- Wojnowicz, M. T., Ferguson, M. J., Dale, R., & Spivey, M. J. (2009). The self-organization of explicit attitudes. *Psychological Science*, 20(11), 1428-1435.

Appendix A: Detailed Statistics for Hypothesis 1 And 2

Hypotheses 1 and 2 were analyzed using a graded motor-response analysis. In a graded motor response analysis, differences between segments are tested using an appropriate statistical test (e.g., t-test, linear mixed effects model). To avoid alpha slippage from running 101 tests when comparing the entire trajectory, overall trajectories are only deemed significantly different if eight segments in a row are significantly different from each other. This cutoff was determined through bootstrapping simulations to provide a conservative criterion that accounts for alpha slippage (Dale et al., 2007). This equates to a critical value of $.05^8$, or $p < .000000000039$ to conclude that two trajectories are different from each other. Measuring attraction between two horizontally aligned stimuli (e.g., the answers in our screening questionnaire) would require testing whether there is a significant difference in the average x-coordinate for eight consecutive segments. Below is the detailed means, standard deviations, and t-tests for each of the 101 segments for Hypothesis 1 and Hypothesis 2.

Note, that for both sets of results, we show effect sizes. However, because the graded motor-response analysis is not based on a single test, but rather a sequence of significant results, a better effect size can be obtained by referencing Section 5.9, “Exploratory Comparison to Electrodermal Activity Part C: Prediction Capability”, in the main paper.

Table A1. Detailed Results of Linear Mixed Effects Model for Hypothesis 1:

Variable	Estimate (the effect of concealment)	Std_Error	T_Value	R2	P-Value (one-tailed)
X_1	(0.0003)	0.0002	(1.8122)	0.0216	0.0350
X_2	(0.0006)	0.0003	(2.2209)	0.0691	0.0132
X_3	(0.0010)	0.0006	(1.6796)	0.1320	0.0465
X_4	(0.0016)	0.0010	(1.5884)	0.1748	0.0561
X_5	(0.0029)	0.0017	(1.7238)	0.2055	0.0424
X_6	(0.0043)	0.0028	(1.5472)	0.2228	0.0609
X_7	(0.0054)	0.0035	(1.5266)	0.2244	0.0634
X_8	(0.0063)	0.0049	(1.2851)	0.2185	0.0994
X_9	(0.0066)	0.0060	(1.0885)	0.2001	0.1382
X_10	(0.0067)	0.0074	(0.9083)	0.1836	0.1819
X_11	(0.0064)	0.0088	(0.7316)	0.1692	0.2322
X_12	(0.0078)	0.0099	(0.7836)	0.1268	0.2166
X_13	(0.0095)	0.0111	(0.8580)	0.1018	0.1955
X_14	(0.0104)	0.0120	(0.8696)	0.0989	0.1923
X_15	(0.0111)	0.0124	(0.8978)	0.0961	0.1846
X_16	(0.0104)	0.0132	(0.7917)	0.1011	0.2143
X_17	(0.0104)	0.0139	(0.7454)	0.0944	0.2280
X_18	(0.0127)	0.0147	(0.8649)	0.0550	0.1936
X_19	(0.0156)	0.0153	(1.0164)	0.0272	0.1547
X_20	(0.0177)	0.0148	(1.1962)	0.0391	0.1158
X_21	(0.0181)	0.0145	(1.2445)	0.0657	0.1067
X_22	(0.0176)	0.0146	(1.2069)	0.0973	0.1137
X_23	(0.0171)	0.0146	(1.1676)	0.1178	0.1215
X_24	(0.0182)	0.0150	(1.2123)	0.1149	0.1127
X_25	(0.0202)	0.0158	(1.2781)	0.1153	0.1006
X_26	(0.0216)	0.0170	(1.2727)	0.1131	0.1016
X_27	(0.0228)	0.0178	(1.2802)	0.1167	0.1002
X_28	(0.0243)	0.0186	(1.3087)	0.1246	0.0953

Table A1. Detailed Results of Linear Mixed Effects Model for Hypothesis 1:

X_29	(0.0268)	0.0192	(1.3999)	0.1425	0.0808
X_30	(0.0285)	0.0198	(1.4419)	0.1727	0.0747
X_31	(0.0309)	0.0209	(1.4766)	0.2034	0.0699
X_32	(0.0333)	0.0223	(1.4971)	0.2193	0.0672
X_33	(0.0387)	0.0240	(1.6126)	0.2049	0.0534
X_34	(0.0401)	0.0262	(1.5315)	0.1890	0.0628
X_35	(0.0394)	0.0278	(1.4175)	0.1748	0.0782
X_36	(0.0400)	0.0297	(1.3459)	0.1579	0.0892
X_37	(0.0424)	0.0312	(1.3594)	0.1359	0.0870
X_38	(0.0445)	0.0331	(1.3466)	0.1115	0.0891
X_39	(0.0433)	0.0342	(1.2662)	0.1017	0.1027
X_40	(0.0423)	0.0351	(1.2045)	0.1006	0.1142
X_41	(0.0467)	0.0355	(1.3140)	0.1024	0.0944
X_42	(0.0549)	0.0357	(1.5401)	0.1153	0.0618
X_43	(0.0626)	0.0365	(1.7158)	0.1152	0.0431
X_44	(0.0714)	0.0379	(1.8846)	0.1193	0.0297
X_45	(0.0783)	0.0394	(1.9887)	0.1229	0.0234
X_46	(0.0855)	0.0410	(2.0867)	0.1294	0.0185
X_47	(0.0893)	0.0427	(2.0908)	0.1320	0.0183
X_48	(0.0891)	0.0446	(1.9974)	0.1301	0.0229
X_49	(0.0828)	0.0464	(1.7837)	0.1278	0.0372
X_50	(0.0820)	0.0483	(1.6970)	0.1152	0.0449
X_51	(0.0819)	0.0500	(1.6397)	0.1167	0.0520
X_52	(0.0872)	0.0519	(1.6806)	0.1090	0.0464
X_53	(0.0969)	0.0537	(1.8040)	0.1165	0.0356
X_54	(0.1070)	0.0557	(1.9230)	0.1173	0.0272
X_55	(0.1168)	0.0579	(2.0170)	0.1189	0.0218
X_56	(0.1263)	0.0599	(2.1075)	0.1196	0.0175
X_57	(0.1359)	0.0609	(2.2326)	0.1305	0.0128
X_58	(0.1377)	0.0613	(2.2447)	0.1442	0.0124
X_59	(0.1435)	0.0610	(2.3515)	0.1724	0.0093
X_60	(0.1483)	0.0610	(2.4322)	0.1904	0.0075
X_61	(0.1530)	0.0607	(2.5196)	0.2165	0.0059
X_62	(0.1579)	0.0611	(2.5835)	0.2284	0.0049
X_63	(0.1579)	0.0617	(2.5598)	0.2279	0.0052
X_64	(0.1545)	0.0622	(2.4838)	0.2197	0.0065
X_65	(0.1524)	0.0620	(2.4569)	0.2156	0.0070
X_66	(0.1474)	0.0618	(2.3840)	0.2085	0.0086
X_67	(0.1441)	0.0616	(2.3380)	0.2049	0.0097
X_68	(0.1379)	0.0619	(2.2298)	0.1953	0.0129
X_69	(0.1298)	0.0619	(2.0969)	0.1838	0.0180
X_70	(0.1133)	0.0614	(1.8442)	0.1716	0.0326
X_71	(0.0864)	0.0600	(1.4394)	0.1649	0.0750
X_72	(0.0651)	0.0582	(1.1192)	0.1664	0.1315

Table A1. Detailed Results of Linear Mixed Effects Model for Hypothesis 1:

X_73	(0.0478)	0.0558	(0.8565)	0.1729	0.1959
X_74	(0.0331)	0.0532	(0.6229)	0.1714	0.2667
X_75	(0.0181)	0.0489	(0.3692)	0.1864	0.3560
X_76	(0.0053)	0.0453	(0.1169)	0.2076	0.4535
X_77	0.0143	0.0407	0.3508	0.2429	0.3629
X_78	0.0241	0.0373	0.6478	0.2576	0.2586
X_79	0.0212	0.0331	0.6410	0.2561	0.2608
X_80	0.0113	0.0308	0.3650	0.2010	0.3576
X_81	0.0053	0.0301	0.1774	0.1507	0.4296
X_82	0.0050	0.0289	0.1723	0.1393	0.4316
X_83	0.0006	0.0274	0.0208	0.1101	0.4917
X_84	(0.0054)	0.0270	(0.1989)	0.0369	0.4212
X_85	(0.0023)	0.0298	(0.0787)	0.0000	0.4686
X_86	0.0031	0.0287	0.1091	0.0001	0.4566
X_87	(0.0004)	0.0219	(0.0198)	0.0000	0.4921
X_88	(0.0111)	0.0126	(0.8759)	0.1519	0.1905
X_89	(0.0159)	0.0117	(1.3517)	0.2210	0.0882
X_90	(0.0173)	0.0106	(1.6299)	0.2593	0.0516
X_91	(0.0195)	0.0097	(2.0132)	0.3013	0.0220
X_92	(0.0202)	0.0089	(2.2765)	0.3368	0.0114
X_93	(0.0203)	0.0082	(2.4758)	0.3626	0.0066
X_94	(0.0190)	0.0079	(2.3968)	0.3698	0.0083
X_95	(0.0173)	0.0077	(2.2617)	0.3802	0.0119
X_96	(0.0152)	0.0074	(2.0476)	0.3899	0.0203
X_97	(0.0135)	0.0073	(1.8577)	0.3906	0.0316
X_98	(0.0135)	0.0073	(1.8567)	0.3884	0.0317
X_99	(0.0136)	0.0073	(1.8662)	0.3885	0.0310
X_100	(0.0136)	0.0073	(1.8651)	0.3886	0.0311
X_101	(0.0136)	0.0073	(1.8651)	0.3886	0.0311

TableA2. Detailed Results of T-Tests for Hypothesis 2

Variable	Mean Concealment Group	SD Concealment Group	Mean Truthful Group	SD Truthful Group	T-Value	DF	P-Value (one tailed)	Cohen's D
X_1	(0.0001)	0.0005	0.0002	0.0008	(1.8826)	65.0000	0.0321	0.5028
X_2	(0.0001)	0.0005	0.0003	0.0011	(1.8022)	65.0000	0.0381	0.5002
X_3	(0.0001)	0.0008	0.0004	0.0013	(1.7506)	65.0000	0.0424	0.4567
X_4	(0.0001)	0.0009	0.0004	0.0016	(1.6576)	65.0000	0.0511	0.4410
X_5	(0.0003)	0.0013	0.0005	0.0018	(2.0156)	65.0000	0.0240	0.5191
X_6	(0.0002)	0.0014	0.0006	0.0019	(1.9658)	65.0000	0.0268	0.5064
X_7	(0.0002)	0.0014	0.0007	0.0020	(2.0040)	65.0000	0.0246	0.5194
X_8	(0.0002)	0.0020	0.0007	0.0021	(1.8483)	65.0000	0.0346	0.4654
X_9	0.0000	0.0024	0.0013	0.0032	(1.8528)	65.0000	0.0342	0.4757
X_10	(0.0001)	0.0030	0.0005	0.0050	(0.5553)	65.0000	0.2903	0.1469
X_11	(0.0002)	0.0060	0.0011	0.0059	(0.8632)	65.0000	0.1956	0.2164
X_12	(0.0018)	0.0143	0.0019	0.0077	(1.3316)	65.0000	0.0938	0.3401
X_13	(0.0036)	0.0219	0.0017	0.0146	(1.1526)	65.0000	0.1267	0.2899
X_14	(0.0045)	0.0259	0.0020	0.0220	(1.0780)	65.0000	0.1425	0.2695
X_15	(0.0043)	0.0268	0.0024	0.0273	(0.9802)	65.0000	0.1653	0.2464
X_16	(0.0041)	0.0259	0.0017	0.0317	(0.7873)	65.0000	0.2170	0.2005
X_17	(0.0040)	0.0254	0.0021	0.0362	(0.7600)	65.0000	0.2250	0.1967
X_18	(0.0039)	0.0258	0.0023	0.0394	(0.7267)	65.0000	0.2350	0.1897
X_19	(0.0032)	0.0255	0.0030	0.0436	(0.6797)	65.0000	0.2496	0.1803
X_20	(0.0027)	0.0244	0.0045	0.0486	(0.7294)	65.0000	0.2342	0.1981
X_21	(0.0018)	0.0218	0.0055	0.0536	(0.6844)	65.0000	0.2481	0.1925
X_22	(0.0015)	0.0204	0.0072	0.0561	(0.7894)	65.0000	0.2164	0.2263
X_23	(0.0004)	0.0192	0.0096	0.0568	(0.9096)	65.0000	0.1832	0.2637
X_24	0.0002	0.0188	0.0124	0.0542	(1.1577)	65.0000	0.1256	0.3343
X_25	0.0000	0.0208	0.0186	0.0472	(1.9753)	65.0000	0.0262	0.5482
X_26	0.0016	0.0225	0.0191	0.0435	(1.9554)	65.0000	0.0274	0.5288
X_27	0.0027	0.0270	0.0210	0.0416	(2.0394)	65.0000	0.0227	0.5333
X_28	0.0034	0.0318	0.0241	0.0412	(2.2134)	65.0000	0.0152	0.5669
X_29	0.0032	0.0376	0.0274	0.0414	(2.4222)	65.0000	0.0091	0.6116
X_30	0.0048	0.0438	0.0360	0.0474	(2.7111)	65.0000	0.0043	0.6839
X_31	0.0071	0.0533	0.0479	0.0700	(2.5837)	65.0000	0.0060	0.6627
X_32	0.0098	0.0685	0.0585	0.0977	(2.2637)	65.0000	0.0135	0.5861
X_33	0.0116	0.0819	0.0729	0.1385	(2.1025)	65.0000	0.0197	0.5570
X_34	0.0156	0.0951	0.0818	0.1606	(1.9547)	65.0000	0.0275	0.5176
X_35	0.0204	0.1048	0.0877	0.1734	(1.8313)	65.0000	0.0358	0.4835
X_36	0.0246	0.1088	0.0905	0.1797	(1.7309)	65.0000	0.0441	0.4569
X_37	0.0284	0.1103	0.0932	0.1867	(1.6465)	65.0000	0.0522	0.4362
X_38	0.0322	0.1146	0.0999	0.1906	(1.6779)	65.0000	0.0491	0.4433
X_39	0.0378	0.1256	0.1135	0.2008	(1.7645)	65.0000	0.0412	0.4637
X_40	0.0440	0.1396	0.0987	0.2037	(1.2282)	65.0000	0.1119	0.3188
X_41	0.0462	0.1423	0.1011	0.2064	(1.2143)	65.0000	0.1145	0.3150
X_42	0.0465	0.1408	0.1041	0.2093	(1.2648)	65.0000	0.1052	0.3291

TableA2. Detailed Results of T-Tests for Hypothesis 2

X_43	0.0481	0.1370	0.1068	0.2113	(1.2881)	65.0000	0.1011	0.3367
X_44	0.0519	0.1377	0.1098	0.2123	(1.2644)	65.0000	0.1053	0.3305
X_45	0.0570	0.1404	0.1132	0.2120	(1.2219)	65.0000	0.1131	0.3186
X_46	0.0620	0.1418	0.1178	0.2119	(1.2128)	65.0000	0.1148	0.3158
X_47	0.0708	0.1438	0.1240	0.2117	(1.1516)	65.0000	0.1269	0.2993
X_48	0.0832	0.1494	0.1353	0.2147	(1.1038)	65.0000	0.1369	0.2860
X_49	0.1018	0.1652	0.1503	0.2228	(0.9732)	65.0000	0.1670	0.2503
X_50	0.1162	0.1809	0.1634	0.2317	(0.8938)	65.0000	0.1874	0.2286
X_51	0.1339	0.2043	0.1764	0.2402	(0.7530)	65.0000	0.2271	0.1911
X_52	0.1506	0.2230	0.1888	0.2458	(0.6457)	65.0000	0.2604	0.1630
X_53	0.1638	0.2325	0.2064	0.2519	(0.6966)	65.0000	0.2443	0.1757
X_54	0.1749	0.2370	0.2268	0.2640	(0.8189)	65.0000	0.2079	0.2069
X_55	0.1867	0.2420	0.2436	0.2791	(0.8620)	65.0000	0.1959	0.2184
X_56	0.2010	0.2511	0.2616	0.2991	(0.8677)	65.0000	0.1944	0.2204
X_57	0.2157	0.2632	0.2769	0.3146	(0.8344)	65.0000	0.2036	0.2120
X_58	0.2344	0.2786	0.2890	0.3215	(0.7186)	65.0000	0.2375	0.1820
X_59	0.2513	0.2910	0.3023	0.3267	(0.6532)	65.0000	0.2580	0.1651
X_60	0.2675	0.3021	0.3179	0.3326	(0.6291)	65.0000	0.2657	0.1588
X_61	0.2853	0.3079	0.3343	0.3380	(0.6010)	65.0000	0.2750	0.1517
X_62	0.3040	0.3085	0.3528	0.3400	(0.5970)	65.0000	0.2763	0.1507
X_63	0.3246	0.3059	0.3718	0.3387	(0.5801)	65.0000	0.2819	0.1465
X_64	0.3478	0.3020	0.3946	0.3352	(0.5824)	65.0000	0.2812	0.1471
X_65	0.3696	0.2986	0.4227	0.3325	(0.6660)	65.0000	0.2539	0.1683
X_66	0.3917	0.2980	0.4534	0.3318	(0.7760)	65.0000	0.2203	0.1960
X_67	0.4118	0.2995	0.4874	0.3327	(0.9470)	65.0000	0.1736	0.2392
X_68	0.4334	0.3014	0.5203	0.3319	(1.0870)	65.0000	0.1405	0.2744
X_69	0.4549	0.2966	0.5491	0.3255	(1.2004)	65.0000	0.1172	0.3030
X_70	0.4838	0.2858	0.5806	0.3143	(1.2782)	65.0000	0.1029	0.3227
X_71	0.5234	0.2648	0.6130	0.2955	(1.2650)	65.0000	0.1052	0.3197
X_72	0.5559	0.2504	0.6670	0.2603	(1.7291)	65.0000	0.0443	0.4350
X_73	0.5849	0.2342	0.6990	0.2331	(1.9444)	65.0000	0.0281	0.4881
X_74	0.6127	0.2171	0.7387	0.2183	(2.3037)	65.0000	0.0122	0.5787
X_75	0.6444	0.1904	0.7675	0.2128	(2.4150)	65.0000	0.0093	0.6105
X_76	0.6717	0.1691	0.7862	0.2039	(2.4147)	65.0000	0.0093	0.6142
X_77	0.7076	0.1324	0.8032	0.1899	(2.2876)	65.0000	0.0127	0.5927
X_78	0.7320	0.1127	0.8188	0.1761	(2.2941)	65.0000	0.0125	0.6010
X_79	0.7482	0.1035	0.8311	0.1632	(2.3708)	65.0000	0.0104	0.6218
X_80	0.7595	0.1008	0.8391	0.1486	(2.4542)	65.0000	0.0084	0.6380
X_81	0.7684	0.0995	0.8415	0.1344	(2.4286)	65.0000	0.0090	0.6248
X_82	0.7776	0.0979	0.8462	0.1227	(2.4369)	65.0000	0.0088	0.6220
X_83	0.7837	0.0948	0.8516	0.1134	(2.5648)	65.0000	0.0063	0.6519
X_84	0.7884	0.0902	0.8544	0.1042	(2.6792)	65.0000	0.0047	0.6791
X_85	0.7953	0.0813	0.8539	0.0893	(2.7176)	65.0000	0.0042	0.6863
X_86	0.8049	0.0719	0.8493	0.0685	(2.5223)	65.0000	0.0071	0.6322

TableA2. Detailed Results of T-Tests for Hypothesis 2

X_87	0.8108	0.0635	0.8460	0.0535	(2.4071)	65.0000	0.0095	0.6020
X_88	0.8148	0.0567	0.8480	0.0501	(2.4877)	65.0000	0.0077	0.6225
X_89	0.8179	0.0503	0.8511	0.0500	(2.6348)	65.0000	0.0053	0.6616
X_90	0.8196	0.0470	0.8543	0.0499	(2.8485)	65.0000	0.0029	0.7177
X_91	0.8195	0.0452	0.8563	0.0496	(3.0753)	65.0000	0.0015	0.7766
X_92	0.8199	0.0440	0.8576	0.0488	(3.2178)	65.0000	0.0010	0.8132
X_93	0.8203	0.0425	0.8554	0.0434	(3.2490)	65.0000	0.0009	0.8170
X_94	0.8217	0.0409	0.8523	0.0391	(3.0511)	65.0000	0.0016	0.7651
X_95	0.8231	0.0392	0.8500	0.0376	(2.7969)	65.0000	0.0034	0.7013
X_96	0.8247	0.0380	0.8483	0.0371	(2.4979)	65.0000	0.0075	0.6267
X_97	0.8258	0.0377	0.8473	0.0364	(2.3115)	65.0000	0.0120	0.5797
X_98	0.8259	0.0376	0.8470	0.0357	(2.2871)	65.0000	0.0127	0.5732
X_99	0.8259	0.0376	0.8470	0.0357	(2.2871)	65.0000	0.0127	0.5732
X_100	0.8259	0.0376	0.8470	0.0357	(2.2871)	65.0000	0.0127	0.5732
X_101	0.8259	0.0376	0.8470	0.0357	(2.2871)	65.0000	0.0127	0.5732

About the Authors

Jeffrey L. Jenkins is an assistant professor of information systems at Brigham Young University. He has developed, extensively validated, and patented algorithms to detect deception, cognitive conflict, uncertainty, and emotional reactions while people are using electronic input devices. Jeff's research also explores methodologies for detecting and mitigating insider security threats—i.e., a trusted member of an organization who poses an information security risk because of ignorance, negligence, or malicious intent. His work has been published in high-quality information systems and computer science outlets, including *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, and *CHI*.

Jeffrey G. Proudfoot is an assistant professor in the Information and Process Management Department at Bentley University. Before joining Bentley he completed a PhD in management information systems at the University of Arizona. Jeff's research centers on behavioral information security and insider threat detection. His work has been published or is forthcoming in a number of premier journals, including *MIS Quarterly*, *Journal of Management Information Systems*, *European Journal of Information Systems*, and *Decision Support Systems*. Jeff has also contributed to over \$1 million in Department of Homeland Security (DHS), Center for Identification Technology Research (CITeR), and National Science Foundation (NSF) grants, of which over \$500k was awarded with Jeff operating as a PI or a co-PI. His prior research affiliations include the Center for the Management of Information (CMI) and the National Center for Border Security and Immigration (BORDERS), a Department of Homeland Security Center of Excellence. He has also received several awards for teaching and service.

Joseph (Joe) S. Valacich is the Eller Professor of MIS in the Eller College of Management at the University of Arizona, a fellow of the Association for Information Systems (2009), and is a cofounder, chairman, and chief science officer (CSO) of Neuro-ID, Inc. His primary research interests include deception detection, human-computer interaction, data visualization, cyber security, and e-business. Dr. Valacich is a prolific scholar, publishing more than 100 scholarly articles in numerous prestigious journals. His scholarly work has had a tremendous impact not only on the IS field, but also on a number of other disciplines, including computer science, cognitive and social psychology, marketing, and management. As of January 2019, Google Scholar lists his citation counts at more than 23,800, with an H-index of 71. He was the general conference cochair for the 2003 International Conference on Information Systems (ICIS) and the 2012 Americas Conference on Information Systems (AMCIS); both were held in Seattle. He is the Honorary Chair for ICIS 2021 to be held in Austin, Texas.

G. Mark Grimes is an assistant professor of Decision and Information Sciences in the Bauer College of Business at the University of Houston. His research focuses on information systems security and analysis of HCI behaviors to detect changes in emotional and cognitive states. Mark's research has been published in journals including *Decision Support Systems* and *Information Technology for Development* and has been presented at the International Conference for Information Systems, the Americas Conference on Information Systems, as well as to various industry and government stakeholders. Mark received his PhD in management information systems from the University of Arizona.

Jay F. Nunamaker, Jr. is Regents and Soldwedel Professor of MIS, Computer Science and Communication and director of the Center for the Management of Information and the National Center for Border Security and Immigration at the University of Arizona. He received his PhD in operations research and systems engineering from Case Institute of Technology. He has held a professional engineer's license since 1965. He was inducted into the Design Science Hall of Fame and received the LEO Award for Lifetime Achievement from the Association for Information Systems. He was featured in the July 1997 issue of *Forbes* magazine on technology as one of eight key innovators in information technology. His specialization is in the fields of system analysis and design, collaboration technology, and deception detection. The commercial product GroupSystems ThinkTank, based on his research, is often referred to as the gold standard for structured collaboration systems. He founded the MIS Department at the University of Arizona in 1974 and served as department head for 18 years.

Copyright © 2019 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via email from publications@aisnet.org.